This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2020.2996615, IEEE Internet of Things Journal

A Survey and Tutorial on “Connection Exploding Meets Efficient Communication” in the Internet of Things

Huansheng Ning, *Senior Member, IEEE*, Fadi Farha *Student Member, IEEE*, Ziarmal Nazar Mohammad, and Mahmoud Daneshmand, *Life Senior Member, IEEE*

[1] ***Abstract*—IoT-enabled sensors and services have increased exponentially recently. Transmitting the massive generated data and control messages becomes an overhead on the communication system infrastructure. Many architectures and paradigms have been introduced to address the connection exploding, such as cloudlets, fog, and mist computing. Besides, software-related solutions such as mobile internet technologies and Software Defined Network also take part in mitigating the communication overhead. All of those new techniques have the same purposes summarized in achieving low latency, high throughput, and less storage and computing at the cloud level in addition to other objectives discussed through this survey. We listed the proposed solutions, showed their advantages and schemes, highlighted some of the newest IoT-enabled applications, and show how they benefit from applying the new paradigms.**

***Index Terms*—IoT Communications, Connection Exploding,**

I. INTRODUCTION

The Internet of Things (IoT), which was introduced by Kevin Ashton in 1999 [1], was used to express the technology of connecting the Radio-frequency identification (RFID) in the supply-chain [2]. Nowadays, IoT is a network of connected machines, physical objects, people, sensors, actuators, smartphones, tablets, vehicles, wearables devices, consumer electronics, and other devices that exchange data and control messages [3]. In recent years, the IoT devices have increased exponentially, and it is expected to exceed 28 billion connected devices by 2021 [4]. These devices belong to different categories including mobile devices (e.g., smartphones and tablets), sensors, and actuals. Besides, they are deployed in different IoT-enabled applications (e.g., smart logistics, transportation, grid, cities, building automation, smart manufacturing, homes, and agriculture) [5]. Most of the newly produced electronic devices have a connection to the internet, which makes the number of connected devices exceeds the people number on the internet [2]. The IoT applications with their end-devices are responsible for producing data, but for transmitting the data to their final destinations, network devices (such as routers, switches, gateways, etc.) are responsible for keeping connectivity between the whole IoT system components [6].

Cloud computing, as shown in *Fig. 1*, is one of the technologies that have a strict relationship with the IoT, especially when talking about gathering the data collected by sensors around the world in one place in order to be analyzed or used by some services or applications [7]. In the last decade, cloud computing has dominated the IoT industries and been used by enterprises in most IoT applications. Storing Data on the cloud and pushing the workloads of processing and computing to the remote servers has become a trend in the IoT industry world [8]. However, this new concept comes with a price that mainly affects the communication section. The cloud servers are located far away from the end-users, which results in some difficulties in storage, processing, and security management over billions of geographically distributed IoT devices [9]. Even though adopting the cloud-based IoT structure has many benefits that enrich the IoT world with infinite services, it creates massive data moving between the cloud and devices in the sensing layer resulting in the following issues: 1) a congested network with high traffic and lack/fast consuming of the network bandwidth, 2) most real-time and services experience a significant delay, 3) varied or poor Quality of Service (QoS) for most connections especially in the rush hours, and 4) handling heterogeneous data generated by different devices from different brands [10].

In order to solve these challenges or face what we called in this paper the “Connection Exploding”, there is a real need for new communication-based paradigms or structures to work

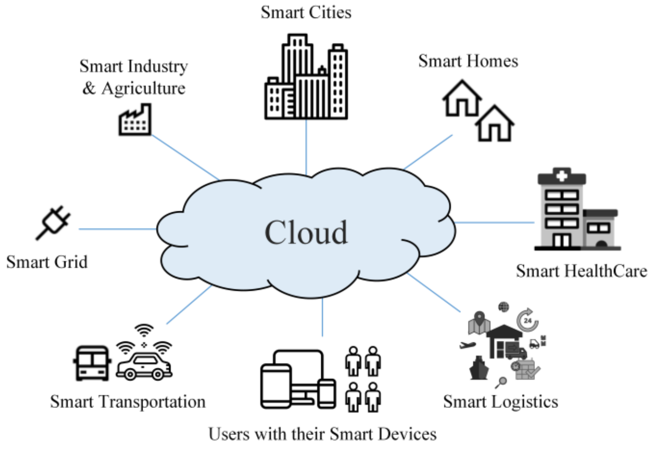

Fig. 1 Traditional Cloud-based IoT

---

[1] This work was supported in part by the National Natural Science Foundation of China under Grant 61471035 and Grant 61672131, and Civil Aviation Joint Funds of the National Natural Science Foundation of China (Grant No. U1633121).

between the cloud and sensing layer [11]. The new layer includes some architecture-related schemes such as edge computing, fog computing, cloudlet, mobile edge computing, mobile cloud computing, dew computing, and mist computing [4]. In addition to software-related solutions like Software Defined Network, and Network Function Virtualization, etc.

II. MOTIVATIONS

The idea of “information at my fingertips at any time and place” was just a dream in the 1990s [12], and the world today is very close to achieving this goal. However, there are still some challenges that stand against the efficient cloud-based IoT system. The traditional structure of it experiences some issues such as the massive scale of network devices, heterogeneity of data sources, high latency of the network connections [13]. Nevertheless, how robust is the communication infrastructure or how active are the servers at the cloud level, they cannot handle the exponential growth of the data and the connections brought by the new devices and services. Therefore, the researchers and the IT companies propose and emerge innovative solutions to fill the gaps in the traditional cloud-users structure and face the challenges shown on the way between the users and the cloud. These solutions involve the whole system starting by the smart IoT end devices (applying selective data schemes and reducing the unnecessary data from being sent on the network) to building a near-user edge computing and pushing some of the cloud services of computing, caching, storage and communication management to be available locally [11]. Most of the solutions succeed in varied degrees to achieve high throughput by benefiting of being geographically closer to the users’ layer (Architecture-related solution) or by introducing software-related solutions.

In this survey, we focus on the solutions of near-user edge computing and how they can achieve minimum latency, decentralized computational paradigms, and communicate with the centralized cloud computing to serve IoT applications and users efficiently. Section III explores the challenges facing the communication technologies used in the cloud-based structure. In Section IV, a taxonomy is presented to show the architecture-related schemes. Section V explores some of the software-related solutions that been used in the new cloud-based IoT structure. In Section VI, we list some of the typical IoT-enabled applications and how they benefit from the new solutions. Finally, we present a conclusion in Section VII.

III. CHALLENGES FACING COMMUNICATIONS IN THE CLOUD-BASED ARCHITECTURE

In this section, a number of the challenges facing the centralized cloud-based architecture, which make communication explosion a vital issue to be solved, are listed below:

1) Heterogeneity and Interoperability: Heterogeneity in the cloud-based architecture means that there are different hardware, structures, infrastructure, and technologies used for end devices, clouds, and communications networks. The newly proposed technologies are predicted to accomplish collaboration between these heterogeneous devices because there are many cloud vendors and devices manufacturers in addition to a variety of communications stacks and protocols [14]. Interoperability refers to the capability of different equipment or networks to communicate and exchange data and information. For example, in the smart cities, there are many domains, including smart healthcare, smart grid, and smart logistics, which makes interoperability an essential issue for enabling the communication between these domains [15]. Interoperability needs to be guaranteed between the different connected devices, communication companies, and regions on the way to/from the cloud [16]. Such variations represent predominant challenges in cloud computing, especially that the competition between business companies makes the cloud providers offer various frameworks on the cloud side [17].
2) Computation power: Supporting various cloud services represents a big challenge for end-users and devices. Besides, handling the storage capacity and the overhead caused by long-distance communications drain computation resources.
3) Connectivity: Compared with the wired connection, wireless communications are intermittent (caused by keeping continuous connectivity and consuming power immoderately), less reliable, and require low bandwidth (which varies from kbps to Mbps according to the adopted communication type). Maintaining the connection link between the sensing layer entities and the clouds (which consists of different types of communication technologies) and handling the high WAN latency are troublesome for resource-restrained IoT devices [17]. It is very challenging to keep receiving the Radio Frequency (RF) signals (which is the connection medium of most IoT devices) while respecting the sleep mode of the IoT terminals without causing transmission delays [16].
4) Devices Management: IoT devices often receive and broadcast messages within their connection range. This range could be within a building, a city, or even a country. Making the cloud a part of the broadcasting is complicated and resource-consuming [18]. That requires the cloud-based structure to be layered and support clustering the devices into groups, which makes the management easy to handle. Doing that also brings benefits for resource-restrained IoT devices for which there will be no need to process unnecessary broadcast messages generated from all the devices in the network range.
5) Context-Processing: IoT sensors and devices gather a considerable amount of various data types from the surrounding environment, such as temperature and humidity values from the sensors in smart homes, the speed and acceleration of the vehicles, and voice and gestures from the smartphones of the mobile users [19]. Some of these data require immediate processing and being transformed into useful information to be used in real-time activities.
6) Power Constraint: IoT devices are mostly small, resource-restrained, battery-powered, and equipped with sensors. The intensive computation tasks are usually passed to the cloud, which costs time and computation power for maintaining the long-distance connection. Besides, it

consumes the processing power of the network equipment that establishes and maintains the connection to the cloud [18]. In order to handle the challenge of battery life and cost, it is necessary to make some improvements in the wireless communication domain and provide the devices with the required resource at a less cost [15].

7) Security and Privacy: Security and privacy issues in IoT are more challenging to achieve compared with that in the traditional networks, due to the numerous amount of personal data loaded to the cloud, including the locations, medical information, and social statements [16]. The sharp increase in cyber-crimes and internet threats forces the cloud vendors to add constraints on the public cloud resources, mainly storage. For devices and data protection in IoT, the closer the IoT device is to the terminal, the more ideal the result for security and privacy can be achieved. Applying security and privacy between heterogeneous clouds, networks, and devices all at once is a big challenge because of the insecure nature of the wireless medium and the poor availability of resources in the sensing layer devices [17]. Most of the existing security protocols are built to be handled by humans and cannot be used directly in the IoT devices. Besides, security and privacy rules are changing according to IoT applications and the capability of the devices at the lowest layer [16]. For example, the inappropriate encryption methods used in some communications protocol, the insufficient authorization policies, and the lack of the protection software make 70% of the IoT devices in a smart city vulnerable to different types of attacks [20]. The IoT is becoming ubiquitous, which requires more storage and processing power. The IoT devices directly depend on the cloud due to resource constraints, which induces more questions about security and privacy issues [18]. The following issues need to be addressed when handling the IoT terminals:
   - Identity Privacy: The identities of users and devices need to be well-protected and unavailable for public use. However, these identities should be accessible by the authorized party in emergency cases.
   - Location Privacy: This is one of the critical issues in IoT security and privacy. Location exposure could lead to tracking the IoT users, recognizing their habits, and making the devices vulnerable to the physical attacks. However, many IoT applications need to access the locations of the devices to offer the best services, especially in the case of auto-drive cars and weather services [18].
   - Cloud Policies: Cloud vendors usually apply some policies to control information access. These policies can be varied according to the area, application, and the organizations [17]. Therefore, sometimes it is too generalized to apply the network policy on the cloud level. Instead, they could be applied locally.
   - Simplicity and Robustness: Privacy-aware communication and lightweight efficient security mechanisms are required for guaranteeing data integrity, identity authentication, and encryption for the user data transmitted between IoT terminals and the cloud services.

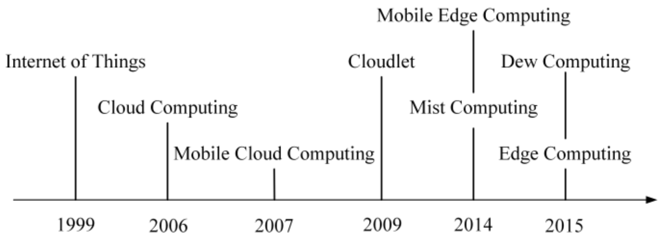

Fig. 2 Cloud computing Paradigms Timeline

IV. ARCHITECTURE-RELATED SOLUTIONS

Architecture-related solutions consider adding layers or sub-layers between the cloud and the sensing layer. In Fig.2, we list the timeline of these solutions and show when they are proposed in the first place. Besides, in this section, we give definitions about architecture-related solutions, show how they are being used, and highlight the advantages of each one of them. At the end of this section, TABLE I summarizes the differences between architectures, services, and applications where these solutions can be deployed.

A. Edge Computing

Processing the data at the edge of the network emerged in the 2000s [21], [22]. The main purpose behind it is to address the centralized cloud system issue. The concept "Edge Computing" was introduced [9] by Karim Arabi in 2014 [5] and subsequently in an invited talk at MIT's MTL Seminar in 2015. While end devices and users are at the sensing layer, and the cloud with its services are at the application layer, the edge computing was presented to at the bottom of the communication layer, near to the end-devices [11] as shown in Fig. 3.

Another reason behind the edge computing was that the cloud is not set up for velocity, variety, and volume of heterogeneous data items. Thus, researchers agree that handling the different types of data can be done on the network edge. As a result, the devices at the edge usually are equipped with essential capabilities for supporting edge storage and computations [23]. Because of that, the edge computing can do its role of providing faster responses to some services requests, handling some real-time requests to locally [24], storing and caching data [25]. Besides, it prevents the raw data bulks from pass to the core network before filtering, compression, or removing the duplicated data [26], [27].

The edge computing concept is that the things (devices/ users), most likely, act as data producers and, at the same time, as data consumers. When those "things" request some data or information, these queries can be handled locally [25]. Therefore, the nodes at the edge should be designed well to do their tasks and meet the requirements of the service [28].

B. Fog Computing

It is cloud-based solution introduced by Cisco in 2012 [29]. As shown in Fig. 3, Fog computing has multi-layer architecture proposed for enabling access to scalable and ubiquitous resources of computing, cashing, and storage [30]. It consists of

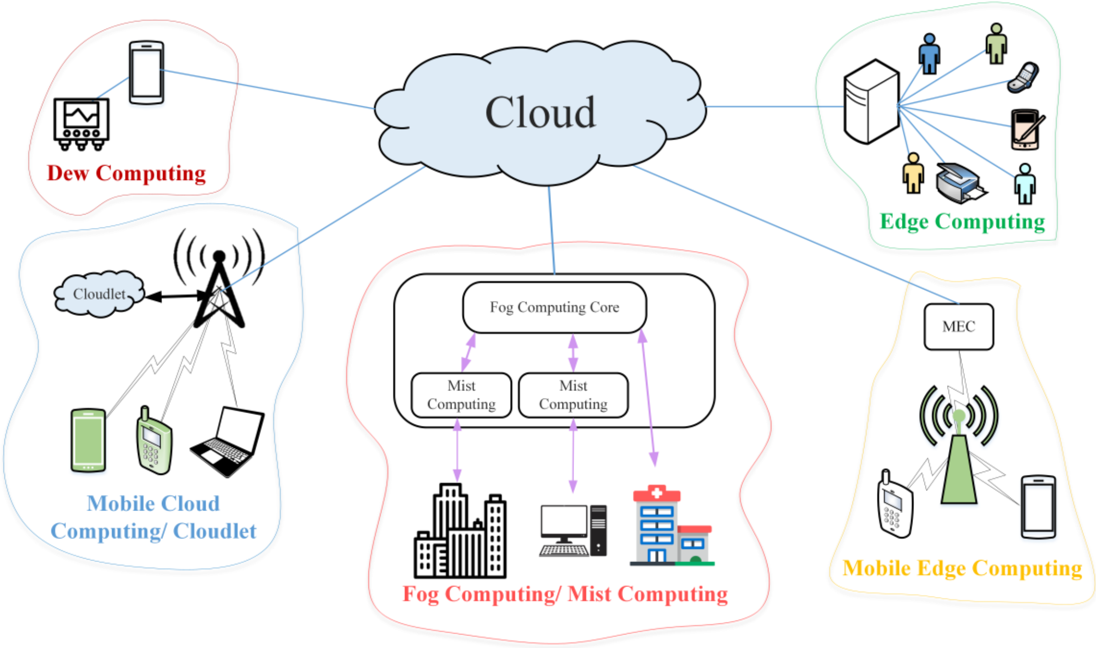

Fig. 3 Cloud Computing Paradigms Architectures

fog nodes which can be physical components meshes and connected, or virtual components and software functions responsible for adjusting the configurations to suit the different IoT applications. These nodes are located between the cloud and the network edge of the sensor and actuators [11]. Fog nodes could be any device with computation, networking, and storage capabilities. Besides, there are fog servers to manage the fog nodes and fog gateways to transmit data on the edge of the sensing layer, fog, and cloud layers [31]. The nodes are aware of their physical location and logical location inside the fog architecture. They could be machine-to-machine (M2M) gateways, wireless routers, and servers that do local computing and can store data [24]. Some examples of the devices that are used as Fog devices are Smart gateways [32], IoT Hub [33], Intel Edison, and Raspberry Pi [34].

Fog computing was introduced to serve of latency-sensitive cloud-based IoT applications by minimizing request/reply time and providing the local computing resources with network connectivity to the cloud [29], [11]. The other advantages of deploying fog computing are insuring low latency, less network traffic, and low power consumption [35]. Besides, fog computing facilitates location-awareness, scalability, and interoperability (its components across the whole structure must be able to interoperate to offer good services). It also supports wide-spread geographical distribution networks, mobility, content distribution, heterogeneity (collecting the data from different sensors types over different types of network communication) [29], [35].

For benefiting from these features, the fog nodes need to be autonomous, organized in hierarchical clusters, manageable, decentralized, and programmable. An example of the fog computing scenario is when delivering high-quality and real-time streaming services to auto-drive cars. In this case, the datacenters are usually located along highways and tracks [11].

C. *Mist Computing*

Cisco in [29] also proposed the mist computing paradigm. As shown in Fig. 3, it is a small form of fog computing that locates at the edge of the network. Its concept is a merge form of the edge and the fog computing that pushes some cloud services near to the sensing layer. The devices in mist computing are usually microcomputers and microcontrollers (low-power nodes) that send data to the fog nodes and, in some cases, directly to the cloud. It is not considered a mandatory layer of fog computing [11].

Some researchers consider the mist as a cloud smaller than fog and bigger than a cloudlet. It can be placed in a Local Area Network (LAN) such as a home network and plays the gateway role in providing cloud services to the local network [36].

The purpose behind the mist computing is minimizing the latency and raising the throughput rate [37]. Also, for the delay-sensitive tasks, mist computing is the answer. It has less storage space and transmission power than the fog nodes and can be used for data analysis [38], [11]. If some tasks need computations to be done by the edge devices, the tasks will be performed at the mist, and in case the mist has not enough processing power, the tasks will be forwarded to the fog.

D. *Mobile Cloud Computing (MCC)/cloudlet*

MCC is a proposed solution for enhancing traditional cloud computing in terms of mobile devices [39]. In recent years, end-users are more likely to run applications using their smartphones rather than using traditional computers [40]. However, these small devices have some limitations related to energy consumption, storage capacity, and computational power. In order to address these issues, the researchers suggest executing these kinds of applications whose requirements exceed the capacity of the smartphones outside of these devices.

MCC is a cloud computing paradigm oriented to the mobile network, and it provides services, computing, and storage. As shown in Fig. 3, cloudlets usually support MCC located at the edge of the mobile network [41]. It coordinates between cloud, mobile devices, and network operators to achieve a better Quality of Sevices (QoS) to the smartphone end-users [42]. It is like a small cloud which represents a mini data center for several devices [22], [23], [24] and offers sufficient resources to support the execution of such remote mobile application [43], [44]. Cloudlet is one of the early proposed solutions to extend the cloud to the edge of end devices[12]. However, the cloudlet was not just used with MCC. In several works [45], [46], cloudlets are considered as parts of Fog computing. Using hybrid systems of both the fog and the cloudlet will bring significant benefits to the network, like handling a large number of requests locally and simultaneously, mainly if some of the cloud-based services required by the cloudlet are located on the fog. That will reduce the network latency and the request delay.

Recently, many applications used by smartphone users require strong computation power are available and frequently. Such applications are based on artificial intelligence and machine learning like speech recognition or the maps that suggest the shortest pass according to the traffic and the distance. A simple powerful mobile device could be unable to satisfy all the requirements of those applications [44]. Therefore, these applications need collaborations of cloud and edge processing, and thus, MCC/cloudlet is the solution. Mobile cloud services provide location-based services, mobile application cloud infrastructure optimization, caches services, and so on [44]. The MCC/cloudlet, for instance, a VM-based cloudlet located near mobile devices, is predicted to minimize network latency by providing cashing and computation power and save the bandwidth [41]. From the viewpoints of service providers and application developers, cloudlet is a perfect solution for improving mobile services [47].

E. Mobile Edge Computing (MEC)

MEC is another cloud computing paradigm that brings computational and storage capacity to the mobile network edge at the cellular network base station to reduce the delay in handling the cloud requests and boost the context-awareness [48].

MEC was firstly proposed by European Telecommunications Standards Institute (ETSI) [49]. Currently, ETSI Industry Specification Group (ISG) MEC has 53 members, including Nokia, Huawei, IBM, Intel, NTT DoCoMo, Vodafone, ZTE, and others.

MEC is well-known and represents a hot topic in the research domain of mobile computing. It is regarded as a good key enabler for modern evolutions of cellular base stations where it is placed in cellular base stations [50]. MEC is used in many applications such as IoT location services, augmented reality. It also enables access to the information in real-time by caching the information at its server [51]. It supports both 2 and 3 tier hierarchical structure, and it is not mandatory to connect MEC to the cloud [42].

MEC is target adaptive and can enhance network efficiency and support 5G communication. Besides, in terms of developing software and content distribution, MEC has an open connection to mobile network information [52], [53].

The MEC servers are placed in the station towers to provide efficient capability in processing and storage at the edge as shown in Fig. 3. For the MEC paradigm to run, it needs four components as follows, mobile users, network operators, Internet Infrastructure Providers (InPs), and application service providers. In this structure, the users' requests will be sent to the MEC server which, in turn, processes the requests or sends them to the cloud [48].

F. Dew Computing

It was firstly introduced in 2015 [54], [55]. The idea beyond dew computing is that the devices which use cloud-based services cannot reach the services when there is no internet connection. Therefore, there is a need for stronger equipment to support the limited-resources devices that depend on the cloud to do tasks of computation and storage when they are off-line [54].

Dew Computing can also be defined as computer hardware and software which provides functionality independently from the cloud but, at the same time, have well-collaborate with the cloud services [46].

According to the current cloud computing structure, dew computing [47] is placed at the bottom under the other cloud paradigms, as shown in Fig. 3. It uses ad-hoc-based networking technologies for computing, storage, and networking [56]. The nodes in the dew computing scan are sensors, tablets, and smartphones.

The authors in [56] believe that dew Computing is beneficial to our daily life. It is a microservice paradigm that does not depend on any centralized system and can be used for novice distribution applications. Its nodes cannot be edge devices like routers and switches, and there is no network topology restriction on dew computing [47].

V. SOFTWARE-RELATED TECHNOLOGIES

Software-related solutions are more likely to be programs or code running on the network devices, which can help the current cloud-based IoT structure to face the challenges of connection exploding without the need for real changes in the architecture. In this section, we have listed some of the software-related technologies used for addressing the connection exploding issue.

A. Mobile Internet Networks as an IoT Application Transmitting Technology

The fourth generation (4G) long-term evolution (LTE)-Advanced started the flourishing of mobile Internet and supported the IoT applications, including smart cities and smart homes with a high transmission speed [57]. It uses the concept of multiple parallel point-to-point links. 5G and future 6G will continue the ultimate support for IoT applications. Many researchers and companies already put their efforts into 5G design to serve this purpose which takes into consideration the nature of end-user applications. 6G, from the industry and researchers perspective, will add the support of ubiquitous Artificial Intelligence (AI) services in the whole network from

TABLE I COMPARISON OF CLOUD-BASED IOT PARADIGMS

Computing Paradigm & Application	Cloud Computing	Edge Computing	Fog Computing	MEC	MCC/Cloudlet	Mist Computing	Dew Computing
Application	IoT and mobile applications	IoT-related applications	IoT-related applications, video streaming, big data processing	Mobile	Mobile	Work with Fog and cloud platform	Smart Devices, health monitoring
Connection to the Cloud	--	Yes or No	Yes	Yes or No	Yes	No	Yes or No
Target users	All users	IoT devices	IoT devices	Mobile	Mobile	IoT devices	Smart Sensor based devices
Main Computation Element	Servers clusters	Micro Data Center	Any device with capability of computation	MEC Server	Base station server and cloudlet	The gateway	smartphone
Node Devices	Cloud and end devices	IoT devices	Router, Switch, Access points, Gateway	Servers in Base station	Data Center in a Box	Micro Controllers and Microchips	Sensors and smartphones
Node Location	In specific locations around the world	The last place which can connect the cloud directly	Varying between End Devices and Cloud	Radio Network Controller/Macro Base Station	Local Outdoor Installation	The edge of fog computing	Sensor and end device
Location awareness	No	Yes	Yes	Yes	Yes	Yes	Yes
Access Mechanisms	Internet	Bluetooth, Wi-Fi, ZigBee, etc.	Wi-Fi, Mobile Networks	Mobile Network	Wi-Fi/Mobile Network	Wi-Fi, Mobile Networks, bluetooth ZigBee, etc	ad hoc
Distance to users	Multiple hops	One hop	One or more hops	One or more hops	One or more hops	One hop	One hop
Geo-distribution	centralized	distributed	distributed	distributed	distributed	distributed	distributed
Coverage	All the world	LAN, WLAN	WAN	Mobile network	Mobile network	LAN, WLAN	WPAN
Data source	All the world	an organization or facility	City or group of facilities	Within the base station coverage	Mobile data from all the world	an organization or facility	Small area around the smartphone
Latency	high	low	medium	low	low	low	low
Number of Users/Devices	billions	Hundreds or thousands	Thousands or millions	thousands	thousands	Hundreds	Few devices
Content accessibility	End users/ devices	Any device in range	Any device in range of fog and the end devices	Any device in range of the base station	End users/ devices	Any device in range of fog and the end devices	Any device directly connected to the smartphone

the core to the terminals [58]. In this survey, we focus on the 5G since it is currently being deployed around the world and will be used until the next decade before the 6G is launched.

Fifth-generation (5G) broadband technology provides a high data transmission speed, high data bandwidth, and very low delays because the data are handled very quickly and efficiently using built-in computing intelligence [59]. Other communication technologies provide specific use cases of IoT connectivity, but 5G is a network that could connect all of IoT devices and satisfy all the requirements of these devices. It incorporates cloud, virtualization, smart edge infrastructure, and distributed computing platforms that serve billions of end-users [60].

Cloud computing innovations and virtualization are widening the networks everywhere. Therefore, IoT could be incorporated in different networking systems including the 5G mobile network. In 5G infrastructure, in order to get better performance for smartphones applications, the edge of cloud computing could be implemented in the cell towers (NodeB) within the 5G networks [61].

5G is anticipated to handle a considerable number of devices and offer new services such as enhancing broadband usage, providing reliable connections, ensuring the low-latency, and efficient supporting of critical network operations. The 5G network would meet all of the IoT's basic requirements, such as high throughput and scalability and low-latency for providing a large number of devices with practical solutions [62].

B. Network Abstraction

The network protocols and architecture in the traditional IoT cannot support high-level scalability, massive amounts of data, and mobility all at once. They have some limitations and, in many cases, are not qualified to support the real-time IoT applications.

To overcome these challenges, two emerging technologies, namely, Software Defined Network (SDN) and Network Function Virtualization (NFV), are used [8].

In terms of pushing computations, cashing, and communication resources to the edge of the network, there is a need for small scale cloud computing platforms for potential IoT applications. NFV and SDN are essential cooperatives in supporting the technologies to realize such vision [61].

1) Software Defined Network

Recently, SDN has become a hot topic in some areas such as datacenters networks, where it mainly achieves network optimization and resource management. An example of using SDN is Google, which uses SDN for network management and interconnection between the data centers [63]. SDN overcomes the challenges and difficulties facing the existing network infrastructure by separating the data plane from the control plane. The control plane is incorporated inside the network operating system, simplifying policy compliance, network setup, and evolution [64].

SDN adopts a different strategy by optimizing networks through the dynamically automate use of network resources. The network operators can program the network to manage data plane devices which improves network performance according to network management and guarantees reasonable control and data handling over the network [65].

2) Network Function Virtualization

NFV is a network architecture proposed for utilizing software virtualization methods to replace networking devices such as switches, routers, and firewalls, with software running on general-purpose servers. It is a good solution to save network energy, achieve load optimization, and improve network scalability [66].

NFV enhances the leverage of network services and minimizes the time required by new services to be put on the market [66]. Besides, it separates software from hardware, which makes their developments independent from each other and allows different timelines for upgrading and maintenance. NFS also offers flexibility in the implementation of the network functions since new services can be deployed on the same physical infrastructure.

3) The convergence of NFV and SDN

NFV and SDN technically are necessary for the edge-cloud paradigm. The decoupling in SDN of the control and data will simplify the contrast between NFV and existing deployments. NFV and SDN integration at the edge-cloud will open the door for a new era of innovation, offering fast and cost-effective infrastructure and delivery of software and implementation [61].

The investors would include Infrastructure Service Providers (ISPs), Application Service Providers (ASPs), and software vendors in the potential edge cloud and app business. The integration of NFV and SDN will make it easy and straightforward to benefit from the potential infrastructure and implementations [67]. Indeed, deploying NFV and SDN convergence in edge cloud is the next-generation 5G network and the trend of the "Network Softwarization" [68].

4) Vehicular Technology System

The concept of vehicles communication is considered an essential part of IoT communications. In Vehicle-to-Vehicle (V2V) communication, vehicles directly communicate with each other without the help of any fixed infrastructure. In contrast, Vehicle-to-Infrastructure (V2I) communication allows vehicles to communicate through road infrastructure (such as traffic light, lane markings, road signs, etc.) using wireless and bi-directional connections [69].

Both of them V2V and V2I are used to overcome the challenge of handling many dynamic parameters when making decisions. By using V2V and V2I, a significant number of devices can integrate and collaborate to do the tasks of collecting and processing the data [70]. In V2V communication, the vehicles act as nodes in the network, and their communications are done in ad-hoc-network within a range of 1000m. The vehicles are moving all the time from a place to another. Therefore, the V2V network does not have any fixed topology, and the infrastructure of the V2V network is quite complicated [71].

VI. IOT APPLICATIONS

According to the recent advancements in ubiquitous computing, a variety of IoT applications are used in different areas which improve and enhance the quality of our daily life. None of them is optimal for all solutions. Besides, the applications are different in characteristics, latency, data rate requirements, and broadly categorized into different fields [62]. Some of these applications are listed below.

A. Smart home

It is one of the main application domains in IoT and consists of a group of different sensors and devices connected together [72]. The sensors send their data to the internet through a gateway. After processing the data, decisions will be made and sent back to control of the smart home system and improve the personal life of the residents [73].

The smart home usually handles two environments. The first one consists of all the interconnected smart devices and the home appliance of the smart home. In contrast, the second environment includes the parts on which the smart home has no control, such as the automatic lighting system, which is controlled by the smart grid [74]. For the automatic lighting system to work efficiently, there should be sensing of the existence or presence of a human. According to this information, the lights in the smart home will turn on/off in some specific areas. The information is coming from analyzing the data generated by the sensors, which could be done locally or on the cloud. Therefore, the smart home regularly communicates to the cloud.

For mitigating the connections requests from the smart home to the cloud, some researchers used mobile edge computing (LTE-device-to-device communication) for applying a local execution of IoT applications [75]. Other researchers used fog computing to assist the smart home in monitoring the patients experiencing intensive care by using fog computing [76].

B. Smart Transportation

It is another IoT-enabled technology in which smart transportations management, control systems, communications networks, and computational technologies work together to make transport systems more safe, effective, and secure [77].

In smart transportation, also known as the Intelligent Transportation System (ITS), a significant number of vehicles are connected using wireless communication [78], [79]. Each vehicle can efficiently collect, manage the trips, and share the traffic data and scheduler and in more efficient, reliable, and secure way. The smart vehicles utilize various Electronic Control Units (ECUs), which are recognized as an internal vehicle network for the gathering and exchange of data within the vehicle [80]. Also, they can share and receive data from the external network using V2V and V2I communication [79].

Smart vehicles, which are connected to the smart transport system, share a tremendous amount of traffic status information, which helps in providing more efficient and secure travel to costumers. These data can be processed or stored in Fog/Edge computing for the sake of providing efficient and convenient services to drivers and system operators [81]. Also, in another research [82], the author proposed using MEC with Big Data analysis for charging electric cars.

C. Smart City

The smart city is a sophisticated IoT technology that provides multiple sub-applications or utilities, such as smart logistics, smart transportation, smart buildings, smart health, to make efficient use of public resources in the city [83], [84]. The smart city application aims to improve the quality of the service with less operational costs [83], [85]. It depends on Information and Communication Technology (ICT) solutions [83]. Padova Smart City, a city in Italy, is an example of the implementation of smart cities. It used ICT solutions for public administration in order to achieve better use of public resources [86].

The new trend of big data in smart cities is to process the data near to the end-users on edge. Therefore, fog computing is an optimal solution for such a process. In [87], the authors use four-layer fog computing architecture to provide computing power and use artificial intelligence for smart cities. Besides, the fog servers are distributed and installed at specific places like bus stops, malls, and parks [30]. In other researches, the authors proposed using edge computing for managing the power supplies cross smart cities [88]. MEC framework was also used in [89] for smart cities in order to provide a detection system for critical events or suspicious and notify the users nearby.

D. Smart Healthcare

The medical and healthcare system is another essential field of the IoT world. The wearable devices, advanced sensors devices attached to the patients, opened the door and opportunities for the healthcare system. They sense health-related data such as blood pressure, temperature, heartbeat rate, blood sugar, cholesterol level, etc., and then automatically send the data to be used in diagnosing the conditions [90], tracking all the progress, and detecting the abnormalities. That makes the low-power wearable devices with their sensors serve as an adaptive data source platform for service providers and doctors [91].

In [92], [93], the authors proposed a healthcare framework where the fog represents an intermediate layer between end-users and cloud. In another research, the authors presented an IoT based U-healthcare monitoring system's architectural view, which also used fog computing on the edge of smart homes and hospitals [94]. In [95], the authors proposed a rate control algorithm in order to optimize the QoS in MEC based healthcare infrastructure.

E. Smart Grid

The smart grid is an IoT-enabled application designed for enhancing the power system and providing consumers with a more reliable and efficient electricity supply [96]. With the advent of IoT, a considerable number of smart meters could be installed in buildings and houses linked via smart grid communications networks [97].

Smart grids use some techniques to achieve better reliability, efficiency, high safety, and good interactivity [98], [99]. The distributed energy generators are an example of this technology used to increase the conservation of electricity and reduce Carbon dioxide (CO_2) emissions. Another example is the smart meters that control energy generation, storage, and usage and can communicate with service providers to disclose customers' energy demands and collect customers ' electricity prices in real-time [98], [100]. Some bidirectional communication networks are responsible for the interconnection between costumers and service providers.

The significant amount of data obtained from smart meters could be retained and analyzed in Fog/Edge computing to ensure the smart grid network is run efficiently [81]. The author of the paper [101] used Mobile Edge Computing for Smart Grid in order to reduce the transmission cost and improve the efficiency of power management.

TABLE II summaries how the near-user edge solutions help the IoT applications facing the connection exploding challenges. All the proposed solutions are meant to perform the tasks of processing and long-distance communications on behalf of the IoT end devices resulting in reducing the power consumption. About the challenge raised by security and privacy, all the architecture-related solutions handle it locally. They have capable devices with powerful processing units that allow them to run the encryption algorithms and authentication mechanisms. Security and privacy issues are beyond this survey purpose, so we just mentioned it as a challenge.

VII. CONCLUSION

Cloud-based IoT is experiencing a "connection exploding" caused by "services exploding" and "data exploding" coming

TABLE II SUMMARY OF THE SOLUTIONS USED FOR MITIGATING CONNECTIONS EXPLODING IN THE IOT APPLICATIONS

Efficient communication challenges	IoT application/ cloud-based paradigms	Solutions
Heterogeneity and Interoperability	Smart City (edge computing [88]) Smart Healthcare and Smart Home (fog computing [94])	Dividing the cloud/end devices domain into sub domains will fix the heterogeneity and interoperability issue hierarchically in an easier way, because there is a responsible device in each subdomain which can address the issue locally with less devices number.
Computation power	Smart City (fog computing [87]) Smart Transportation (Fog/Edge computing [81], MEC [82]) Smart Healthcare (fog computing [92], [93]) Smart Grid (Fog / edge computing [81])	Moving the intensive computation operations to the stronger devices which are usually provided by the new paradigms at the edge, fog, mist, MEC, and dew computing.
Connectivity	All applications (NFV, SDN, and 5G) Smart Home (MEC [75]) Smart Transportation (V2V and V2I [79]) Smart Healthcare (MEC [95]) Smart Grid (MEC [101])	Handling the long-distance communication could be done by the devices in the communication layer instead of the sensing layer terminals. In addition, providing some of the cloud resources closer to the sensing layer have a significant role in reducing the connectivity overhead.
Devices Management	Smart City (fog computing [30])	Managing the IoT devices locally is much easier than transferring this responsibility to the cloud. Using a hierarchical structure will make the management task smoother and remove the complexity.
Context-Processing	Smart Home (fog computing [76]) Smart Transportation (MEC [82]) Smart City (MEC [89])	When different types of data need processing and that cannot be done by the limited-resources devices, the data are being sent to a higher level containing more powerful equipment. That can be done without the need to make the processing at the cloud level which reduce the communication overhead.

from the exponentially increased number of the newly joined sensors and services. The servers at the cloud layer cannot handle all the connections coming from millions to billions of sensors and users' devices. Therefore, some solutions are proposed to mitigate communication overhead. The cloud-based IoT consists of three layers namely the sensing layer, the network layer and the cloud layer. In this survey, we have discussed the network layer and how researchers were able to successfully reduce the network overhead, and at the same time, achieve significant results in terms of latency, throughput, real-time services, management over millions of devices, and collecting data from different sources and different communication stacks. The proposed solutions, in this survey, are categorized in architecture-related paradigms (edge, fog, mist, MCC, MEC, dew) and software-related technologies (virtualization in 5G, NFS, SDN, and network softwarization). Moreover, we have listed some of the IoT-enabled applications and how they benefit from the new cloud computing paradigms. Each one of these solutions is considered a beneficial research area, and there is still a long way to go with each of them.

Most of the recent researches agree that centralized cloud-based architecture is not the optimal solution for the future of the IoT. Applying decentralized paradigms at the edge of network close to the users show significant improvements to the quality of cloud services offered to the terminals. Also, the layered structure directly at the top of the edge is an efficient way to handle the big IoT-enabled applications such as the smart cities which connect other smaller IoT applications such as smart grid, smart houses, and smart healthcare together. In the network core, improving communication speed and network management is the best way for fast transmit of the data between the edge and the cloud. Therefore, more researches are needed in the SDN and NFV to enhance the connection quality. To sum up, pushing the IoT communication to the next level requires improvements in all the three layers of IoT structure.

TABLE III LIST OF ABBREVIATIONS

Abbr.	Explanation
4G	fourth generation
AI	Artificial Intelligence
ASPs	Application Service Providers
CO2	Carbon dioxide
ECUs	Electronic Control Units
ETSI	European Telecommunications Standards Institute
ICT	Information and Communication Technology
InPs	Internet Infrastructure Providers
IoT	Internet of Things
ISG	Industry Specification Group
ISPs	include Infrastructure Service Providers
ITS	Intelligent Transportation System
LAN	Local Area Network
LTE	long-term evolution
MCC	Mobile Cloud Computing
MEC	Mobile Edge Computing
NFV	Network Function Virtualization
QoS	Quality of Service
RF	Radio Frequency
RFID	Radio-frequency identification
SDN	Software Defined Network
V2I	Vehicle-to-Infrastructure
V2V	Vehicle-to-Vehicle

REFERENCES

[1] K. Ashton, “An Introduction to the Internet of Things (IoT),” *RFID Journal*, 1999.

[2] D. Evans, “The internet of things: How the next evolution of the internet is changing everything,” *CISCO white paper*, vol. 1, no. 2011, pp. 1–11, 2011.

[3] H. Chaouchi, *The Internet of Things: Connecting Objects to the Web*. Wiley, 2013.

[4] M. Asif-Ur-Rahman *et al.*, “Toward a Heterogeneous Mist, Fog, and Cloud-Based Framework for the Internet of Healthcare Things,” *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4049–4062, Jun. 2019.

[5] H. Liu *et al.*, “A review of the smart world,” *Future Generation Computer Systems*, vol. 96, pp. 678–691, 2019.

[6] F. Farha, H. Ning, H. Liu, L. T. Yang, and L. Chen, "Physical unclonable functions based secret keys scheme for securing big data infrastructure communication," *Information Sciences*, vol. 503, pp. 307–318, Nov. 2019.

[7] M. Armbrust *et al.*, "A view of cloud computing," *Communications of the ACM*, vol. 53, no. 4, pp. 50–58, 2010.

[8] X. Zhang, A. Kunjithapatham, S. Jeong, and S. Gibbs, "Towards an Elastic Application Model for Augmenting the Computing Capabilities of Mobile Devices with Cloud Computing," *Mobile Networks and Applications*, vol. 16, no. 3, pp. 270–284, 2011.

[9] P. Garcia Lopez *et al.*, "Edge-centric computing: Vision and challenges," *ACM SIGCOMM Computer Communication Review*, vol. 45, no. 5, pp. 37–42, 2015.

[10] S. Sarkar and S. Misra, "Theoretical modelling of fog computing: a green computing paradigm to support IoT applications," *Iet Networks*, vol. 5, no. 2, pp. 23–29, 2016.

[11] M. Iorga, L. Feldman, R. Barton, M. J. Martin, N. S. Goren, and C. Mahmoudi, "Fog computing conceptual model," 2018.

[12] M. Satyanarayanan, V. Bahl, R. Caceres, and N. Davies, "The Case for VM-based Cloudlets in Mobile Computing," *IEEE Pervasive Computing*, Nov. 2009.

[13] P. Hu, S. Dhelim, H. Ning, and T. Qiu, "Survey on fog computing: architecture, key technologies, applications and open issues," *Journal of Network and Computer Applications*, vol. 98, pp. 27–42, 2017.

[14] M. Hogan, F. Liu, A. Sokol, and J. Tong, "Nist cloud computing standards roadmap," *NIST Special Publication*, vol. 35, pp. 6–11, 2011.

[15] Y. Mehmood, F. Ahmad, I. Yaqoob, A. Adnane, M. Imran, and S. Guizani, "Internet-of-Things-Based Smart Cities: Recent Advances and Challenges," *IEEE Communications Magazine*, vol. 55, no. 9, pp. 16–24, 2017.

[16] S. Chen, H. Xu, D. Liu, B. Hu, and H. Wang, "A Vision of IoT: Applications, Challenges, and Opportunities With China Perspective," *IEEE Internet of Things Journal*, vol. 1, no. 4, pp. 349–359, 2014.

[17] Z. Sanaei, S. Abolfazli, A. Gani, and R. Buyya, "Heterogeneity in Mobile Cloud Computing: Taxonomy and Open Challenges," *IEEE Communications Surveys Tutorials*, vol. 16, no. 1, pp. 369–392, 2014.

[18] J. Zhou, Z. Cao, X. Dong, and A. V Vasilakos, "Security and Privacy for Cloud-Based IoT: Challenges," *IEEE Communications Magazine*, vol. 55, no. 1, pp. 26–33, 2017.

[19] P. Lukowicz, S. Pentland, and A. Ferscha, "From Context Awareness to Socially Aware Computing," *IEEE Pervasive Computing*, vol. 11, no. 1, pp. 32–41, 2012.

[20] A. Botta, W. [de Donato], V. Persico, and A. Pescapé, "Integration of Cloud computing and Internet of Things: A survey," *Future Generation Computer Systems*, vol. 56, pp. 684–700, 2016.

[21] X. Xie, H.-J. Zeng, and W.-Y. Ma, "Enabling Personalization Services on the Edge," in *Proceedings of the Tenth ACM International Conference on Multimedia*, 2002, pp. 263–266.

[22] P. P. Gelsinger, "Microprocessors for the new millennium: Challenges, opportunities, and new frontiers," in *2001 IEEE International Solid-State Circuits Conference. Digest of Technical Papers. ISSCC (Cat. No.01CH37177)*, 2001, pp. 22–25.

[23] B. Varghese, N. Wang, S. Barbhuiya, P. Kilpatrick, and D. S. Nikolopoulos, "Challenges and opportunities in edge computing," in *2016 IEEE International Conference on Smart Cloud (SmartCloud)*, 2016, pp. 20–26.

[24] K. Dolui and S. K. Datta, "Comparison of edge computing implementations: Fog computing, cloudlet and mobile edge computing," in *2017 Global Internet of Things Summit (GIoTS)*, 2017, pp. 1–6.

[25] M. Chiang and T. Zhang, "Fog and IoT: An overview of research opportunities," *IEEE Internet of Things Journal*, vol. 3, no. 6, pp. 854–864, 2016.

[26] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge computing: Vision and challenges," *IEEE Internet of Things Journal*, vol. 3, no. 5, pp. 637–646, 2016.

[27] A. Ullah, K. Hamza, M. Azeem, and F. Farha, "Secure Healthcare Data Aggregation and Deduplication Scheme for FoG-Orineted IoT," *2019 IEEE International Conference on Smart Internet of Things (SmartIoT)*, pp. 314–319, Aug. 2019.

[28] T. Wang, G. Zhang, M. D. Z. A. Bhuiyan, A. Liu, W. Jia, and M. Xie, "A novel trust mechanism based on Fog Computing in Sensor–Cloud System," *Future Generation Computer Systems*, 2018.

[29] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the internet of things," in *Proceedings of the first edition of the MCC workshop on Mobile cloud computing*, 2012, pp. 13–16.

[30] H. Dubey *et al.*, "Fog Computing in Medical Internet-of-Things: Architecture, Implementation, and Applications," in *Handbook of Large-Scale Distributed Computing in Smart Healthcare*, S. U. Khan, A. Y. Zomaya, and A. Abbas, Eds. Cham: Springer International Publishing, 2017, pp. 281–321.

[31] R. K. Naha *et al.*, "Fog Computing: Survey of Trends, Architectures, Requirements, and Research Directions," *IEEE Access*, vol. 6, pp. 47980–48009, 2018.

[32] M. Aazam and E.-N. Huh, "Fog computing and smart gateway based communication for cloud of things," in *2014 International Conference on Future Internet of Things and Cloud*, 2014, pp. 464–470.

[33] S. Cirani, G. Ferrari, N. Iotti, and M. Picone, "The iot hub: a fog node for seamless management of heterogeneous connected smart objects," in *2015 12th Annual IEEE International Conference on Sensing, Communication, and Networking-Workshops (SECON Workshops)*, 2015, pp. 1–6.

[34] R. K. Barik *et al.*, "MistGIS: Optimizing Geospatial Data Analysis Using Mist Computing," in *Progress in Computing, Analytics and Networking*, 2018, pp. 733–742.

[35] S. Sarkar, S. Chatterjee, and S. Misra, "Assessment of the Suitability of Fog Computing in the Context of Internet of Things," *IEEE Transactions on Cloud Computing*, vol. 6, no. 1, pp. 46–59, 2015.

[36] M. Uehara, "Mist Computing: Linking Cloudlet to Fogs," in *Computational Science/Intelligence and Applied Informatics*, R. Lee, Ed. Cham: Springer International Publishing, 2018, pp. 201–213.

[37] R. K. Barik *et al.*, "Mist Data: Leveraging Mist Computing for Secure and Scalable Architecture for Smart and Connected Health," *Procedia Computer Science*, vol. 125, pp. 647–653, 2018.

[38] A. Monteiro, H. Dubey, L. Mahler, Q. Yang, and K. Mankodiya, "Fit: A fog computing device for speech tele-treatments," in *2016 IEEE International Conference on Smart Computing (SMARTCOMP)*, 2016, pp. 1–3.

[39] A. u. R. Khan, M. Othman, S. A. Madani, and S. U. Khan, "A Survey of Mobile Cloud Computing Application Models," *IEEE Communications Surveys Tutorials*, vol. 16, no. 1, pp. 393–413, 2014.

[40] M. R. Mahmud, M. Afrin, M. A. Razzaque, M. M. Hassan, A. Alelaiwi, and M. Alrubaian, "Maximizing quality of experience through context-aware mobile application scheduling in Cloudlet infrastructure," *Software: Practice and Experience*, vol. 46, no. 11, pp. 1525–1545, 2016.

[41] M. Satyanarayanan, G. Lewis, E. Morris, S. Simanta, J. Boleng, and K. Ha, "The role of cloudlets in hostile environments," *IEEE Pervasive Computing*, vol. 12, no. 4, pp. 40–49, 2013.

[42] G. I. Klas, "Fog computing and mobile edge cloud gain momentum open fog consortium, etsi mec and cloudlets," *Google Scholar*, 2015.

[43] Z. Sanaei, S. Abolfazli, A. Gani, and R. Buyya, "Heterogeneity in mobile cloud computing: taxonomy and open challenges," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 1, pp. 369–392, 2013.

[44] P. Bahl, R. Y. Han, L. E. Li, and M. Satyanarayanan, "Advancing the state of mobile cloud computing," in *Proceedings of the third ACM workshop on Mobile cloud computing and services*, 2012, pp. 21–28.

[45] C. Dsouza, G.-J. Ahn, and M. Taguinod, "Policy-driven security management for fog computing: Preliminary framework and a case study," in *Proceedings of the 2014 IEEE 15th International Conference on Information Reuse and Integration (IEEE IRI 2014)*, 2014, pp. 16–23.

[46] V. Cardellini, V. Grassi, F. Lo Presti, and M. Nardelli, "On QoS-aware scheduling of data stream applications over fog computing infrastructures," in *2015 IEEE Symposium on Computers and Communication (ISCC)*, 2015, pp. 271–276.

[47] Y. Pan, P. Thulasiraman, and Y. Wang, "Overview of Cloudlet, Fog Computing, Edge Computing, and Dew Computing," in *Proceedings of The 3rd International Workshop on Dew Computing*, 2018, pp. 20–23.

[48] M. T. Beck, M. Werner, S. Feld, and S. Schimper, "Mobile edge computing: A taxonomy," in *Proc. of the Sixth International Conference on Advances in Future Internet*, 2014, pp. 48–55.

[49] M. Patel *et al.*, "Mobile-edge computing introductory technical white

paper," *White paper, mobile-edge computing (MEC) industry initiative*, pp. 1089–7801, 2014.

[50] Y. C. Hu, M. Patel, D. Sabella, N. Sprecher, and V. Young, "Mobile edge computing—A key technology towards 5G," *ETSI white paper*, vol. 11, no. 11, pp. 1–16, 2015.

[51] Q.-V. Pham *et al.*, "A Survey of Multi-Access Edge Computing in 5G and Beyond: Fundamentals, Technology Integration, and State-of-the-Art," *CoRR*, vol. abs/1906.0, 2019.

[52] E. Cau *et al.*, "Efficient exploitation of mobile edge computing for virtualized 5G in EPC architectures," in *2016 4th IEEE international conference on mobile cloud computing, services, and engineering (MobileCloud)*, 2016, pp. 100–109.

[53] N. Abbas, Y. Zhang, A. Taherkordi, and T. Skeie, "Mobile edge computing: A survey," *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 450–465, 2017.

[54] Y. Wang, "Cloud-dew architecture," *International Journal of Cloud Computing*, vol. 4, no. 3, pp. 199–210, 2015.

[55] K. Skala, D. Davidovic, E. Afgan, I. Sovic, and Z. Sojat, "Scalable Distributed Computing Hierarchy: Cloud, Fog and Dew Computing," *Open Journal of Cloud Computing (OJCC)*, vol. 2, no. 1, pp. 16–24, 2015.

[56] K. Skala, D. Davidovic, E. Afgan, I. Sovic, and Z. Sojat, "Scalable Distributed Computing Hierarchy: Cloud, Fog and Dew Computing," *Open Journal of Cloud Computing (OJCC)*, vol. 2, no. 1, pp. 16–24, 2015.

[57] K. B. Letaief, W. Chen, Y. Shi, J. Zhang, and Y. A. Zhang, "The Roadmap to 6G: AI Empowered Wireless Networks," *IEEE Communications Magazine*, vol. 57, no. 8, pp. 84–90, 2019.

[58] R. Shafin, L. Liu, V. Chandrasekhar, H. Chen, J. Reed, and J. C. Zhang, "Artificial Intelligence-Enabled Cellular Networks: A Critical Path to Beyond-5G and 6G," *IEEE Wireless Communications*, pp. 1–6, 2020.

[59] D. M. Gutierrez-Estevez *et al.*, "Artificial Intelligence for Elastic Management and Orchestration of 5G Networks," *IEEE Wireless Communications*, vol. 26, no. 5, pp. 134–141, Oct. 2019.

[60] D. M. West, "How 5G technology enables the health internet of things," *Brookings Center for Technology Innovation*, vol. 3, pp. 1–20, 2016.

[61] J. Pan and J. McElhannon, "Future Edge Cloud and Edge Computing for Internet of Things Applications," *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 439–449, Feb. 2018.

[62] G. A. Akpakwu, B. J. Silva, G. P. Hancke, and A. M. Abu-Mahfouz, "A Survey on 5G Networks for the Internet of Things: Communication Technologies and Challenges," *IEEE Access*, vol. 6, pp. 3619–3647, 2018.

[63] S. Jain *et al.*, "B4: Experience with a Globally-Deployed Software Defined Wan," in *Proceedings of the ACM SIGCOMM 2013 Conference on SIGCOMM*, 2013, pp. 3–14.

[64] S. Costanzo, L. Galluccio, G. Morabito, and S. Palazzo, "Software defined wireless networks (sdwn): Unbridling sdns," in *European workshop on software defined networking*, 2012, pp. 1–6.

[65] T. Luo, H. Tan, and T. Q. S. Quek, "Sensor OpenFlow: Enabling Software-Defined Wireless Sensor Networks," *IEEE Communications Letters*, vol. 16, no. 11, pp. 1896–1899, Nov. 2012.

[66] B. Han, V. Gopalakrishnan, L. Ji, and S. Lee, "Network function virtualization: Challenges and opportunities for innovations," *IEEE Communications Magazine*, vol. 53, no. 2, pp. 90–97, 2015.

[67] J. Pan, L. Ma, R. Ravindran, and P. TalebiFard, "HomeCloud: An edge cloud framework and testbed for new application delivery," in *2016 23rd International Conference on Telecommunications (ICT)*, 2016, pp. 1–6.

[68] F. Yang, H. Wang, C. Mei, J. Zhang, and M. Wang, "A flexible three clouds 5G mobile network architecture based on NFV SDN," *China Communications*, vol. 12, no. Supplement, pp. 121–131, Dec. 2015.

[69] J. W. Wedel, B. Schünemann, and I. Radusch, "V2X-Based Traffic Congestion Recognition and Avoidance," in *2009 10th International Symposium on Pervasive Systems, Algorithms, and Networks*, 2009, pp. 637–641.

[70] N. Parrado and Y. Donoso, "Congestion Based Mechanism for Route Discovery in a V2I-V2V System Applying Smart Devices and IoT," *Sensors*, vol. 15, no. 4, pp. 7768–7806, 2015.

[71] G.-J. van Rooyen, "Survey of media access control protocols for vehicular *ad hoc* networks," *IET Communications*, vol. 5, no. 11, pp. 1619-1631(12), Jul. 2011.

[72] P. P. Gaikwad, J. P. Gabhane, and S. S. Golait, "A survey based on Smart Homes system using Internet-of-Things," in *2015 International Conference on Computation of Power, Energy, Information and Communication (ICCPEIC)*, 2015, pp. 330–335.

[73] D. J. Cook, A. S. Crandall, B. L. Thomas, and N. C. Krishnan, "CASAS: A Smart Home in a Box," *Computer*, vol. 46, no. 7, pp. 62–69, Jul. 2013.

[74] N. Komninos, E. Philippou, and A. Pitsillides, "Survey in Smart Grid and Smart Home Security: Issues, Challenges and Countermeasures," *IEEE Communications Surveys Tutorials*, vol. 16, no. 4, pp. 1933–1954, 2014.

[75] C. Vallati, A. Virdis, E. Mingozzi, and G. Stea, "Mobile-Edge Computing Come Home Connecting things in future smart homes using LTE device-to-device communications," *IEEE Consumer Electronics Magazine*, vol. 5, no. 4, pp. 77–83, Oct. 2016.

[76] P. Verma and S. K. Sood, "Fog Assisted-IoT Enabled Patient Health Monitoring in Smart Homes," *IEEE Internet of Things Journal*, vol. 5, no. 3, pp. 1789–1796, Jun. 2018.

[77] J. Lin, W. Yu, X. Yang, Q. Yang, X. Fu, and W. Zhao, "A Novel Dynamic En-Route Decision Real-Time Route Guidance Scheme in Intelligent Transportation Systems," in *2015 IEEE 35th International Conference on Distributed Computing Systems*, 2015, pp. 61–72.

[78] R. Kim, H. Lim, and B. Krishnamachari, "Prefetching-Based Data Dissemination in Vehicular Cloud Systems," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 1, pp. 292–306, Jan. 2016.

[79] M. Khanjary and S. M. Hashemi, "Route guidance systems: Review and classification," in *2012 6th Euro American Conference on Telematics and Information Systems (EATIS)*, 2012, pp. 1–7.

[80] I. Studnia, V. Nicomette, E. Alata, Y. Deswarte, M. Kaâniche, and Y. Laarouchi, "Survey on security threats and protection mechanisms in embedded automotive networks," in *2013 43rd Annual IEEE/IFIP Conference on Dependable Systems and Networks Workshop (DSN-W)*, 2013, pp. 1–12.

[81] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1125–1142, Oct. 2017.

[82] Y. Cao *et al.*, "Mobile Edge Computing for Big-Data-Enabled Electric Vehicle Charging," *IEEE Communications Magazine*, vol. 56, no. 3, pp. 150–156, Mar. 2018.

[83] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of Things for Smart Cities," *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 22–32, Feb. 2014.

[84] S. Mallapuram, N. Ngwum, F. Yuan, C. Lu, and W. Yu, "Smart city: The state of the art, datasets, and evaluation platforms," in *2017 IEEE/ACIS 16th International Conference on Computer and Information Science (ICIS)*, 2017, pp. 447–452.

[85] A. Laya, V. Bratu, and J. Markendahl, "Who is investing in machine-to-machine communications?," 2013.

[86] P. Casari *et al.*, "The 'Wireless Sensor Networks for City-Wide Ambient Intelligence (WISE-WAI)' Project," *Sensors*, vol. 9, no. 6, pp. 4056–4082, May 2009.

[87] B. Tang, Z. Chen, G. Hefferman, T. Wei, H. He, and Q. Yang, "A Hierarchical Distributed Fog Computing Architecture for Big Data Analysis in Smart Cities," in *Proceedings of the ASE BigData & SocialInformatics 2015*, 2015.

[88] Y. Liu, C. Yang, L. Jiang, S. Xie, and Y. Zhang, "Intelligent Edge Computing for IoT-Based Energy Management in Smart Cities," *IEEE Network*, vol. 33, no. 2, pp. 111–117, Mar. 2019.

[89] M. Sapienza, E. Guardo, M. Cavallo, G. La Torre, G. Leombruno, and O. Tomarchio, "Solving Critical Events through Mobile Edge Computing: An Approach for Smart Cities," in *2016 IEEE International Conference on Smart Computing (SMARTCOMP)*, 2016, pp. 1–5.

[90] C. F. Pasluosta, H. Gassner, J. Winkler, J. Klucken, and B. M. Eskofier, "An Emerging Era in the Management of Parkinson's Disease: Wearable Technologies and the Internet of Things," *IEEE Journal of Biomedical and Health Informatics*, vol. 19, no. 6, pp. 1873–1881, Nov. 2015.

[91] P. A. Laplante and N. Laplante, "The Internet of Things in Healthcare: Potential Applications and Challenges," *IT Professional*, vol. 18, no. 3, pp. 2–4, May 2016.

[92] M. Ahmad, M. B. Amin, S. Hussain, B. H. Kang, T. Cheong, and S. Lee, "Health fog: a novel framework for health and wellness applications," *The Journal of Supercomputing*, vol. 72, no. 10, pp. 3677–3695, 2016.

[93] A. M. Rahmani *et al.*, "Exploiting smart e-Health gateways at the edge of healthcare Internet-of-Things: A fog computing approach," *Future Generation Computer Systems*, vol. 78, pp. 641–658, 2018.

[94] C. S. Nandyala and H.-K. Kim, "From cloud to fog and IoT-based real-time U-healthcare monitoring for smart homes and hospitals," *International Journal of Smart Home*, vol. 10, no. 2, pp. 187–196, 2016.

[95] A. H. Sodhro, Z. Luo, A. K. Sangaiah, and S. W. Baik, "Mobile edge computing based QoS optimization in medical healthcare applications," *International Journal of Information Management*, vol. 45, pp. 308–318, 2019.

[96] U.S. National Institute of Standards and Technology, "Guidelines for Smart Grid Cybersecurity NISTIR 7628 Revision 1," *U.S. Department of Commerce NISTIR*, vol. 1, no. September, p. 668, 2014.

[97] M. B. Line, I. A. Tøndel, and M. G. Jaatun, "Cyber security challenges in Smart Grids," in *2011 2nd IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies*, 2011, pp. 1–8.

[98] J. Lin, W. Yu, X. Yang, G. Xu, and W. Zhao, "On False Data Injection Attacks against Distributed Energy Routing in Smart Grid," in *2012 IEEE/ACM Third International Conference on Cyber-Physical Systems*, 2012, pp. 183–192.

[99] J. Lin, W. Yu, and X. Yang, "Towards Multistep Electricity Prices in Smart Grid Electricity Markets," *IEEE Transactions on Parallel and Distributed Systems*, vol. 27, no. 1, pp. 286–302, Jan. 2016.

[100] X. Zhang, X. Yang, J. Lin, G. Xu, and W. Yu, "On Data Integrity Attacks Against Real-Time Pricing in Energy-Based Cyber-Physical Systems," *IEEE Transactions on Parallel and Distributed Systems*, vol. 28, no. 1, pp. 170–187, Jan. 2017.

[101] K. Zhang, S. Leng, Y. He, S. Maharjan, and Y. Zhang, "Mobile Edge Computing and Networking for Green and Low-Latency Internet of Things," *IEEE Communications Magazine*, vol. 56, no. 5, pp. 39–45, May 2018.

Huansheng Ning received his Ph.D. degree from Beihang University in 2001. He is a professor and vice dean of the School of Computer and Communication Engineering, University of Science and Technology Beijing, China. He is the founder of the Cyberspace and Cybermatics International Science and Technology Cooperation Base. He has published more than 170 journal/conference papers. His research interests include Cybermatics, Internet of Things, Cyber-Physical Social Systems.

Fadi Farha received his BS from the faculty of Informatics Engineering, Aleppo University, Syria. He did his MS degree and currently working toward a Ph.D. degree in the School of Computer and Communication Engineering, University of Science and Technology Beijing, China. His current research interests include Physical Unclonable Function (PUF), Security Solutions, ZigBee, Computer Architecture, and Hardware Security.

Ziarmal Nazar Mohammad received his Bachelor Degree in the school of Computer Science, Sayed Jamalludin Afghan University, Afghanistan. Currently working toward Master degree in the school of Computer and Communication Engineering, University of Science and Technology Beijing, China. His current research interest includes Internet of Things and Cyberspace & Intelligence.

Mahmoud Daneshmand received his Ph. D and M.S. degrees in Statistics from the University of California, Berkeley; M.S. and B.S. degrees in Mathematics from the University of Tehran. He is currently an Industry Professor with the Department of Business Intelligence & Analytics as well as Department of Computer Science at Stevens Institute of Technology, USA. He has more than 35 years of Industry &University experience as: Professor, Researcher, Assistant Chief Scientist, Executive Director, Distinguished Member of Technical Staff, Technology Leader, Chairman of Department, and Dean of School at: Bell Laboratories; AT&T Shannon Labs–Research; University of California, Berkeley; University of Texas, Austin; Sharif University of Technology; University of Tehran; New York University; and Stevens Institute of Technology. He has published more than 150 journal and conference papers; authored/co-authored three books. He is well recognized within the academia and industry and holds key leadership roles in IEEE Journal Publications, Conferences, Industry IEEE Partnership, and IEEE Future Direction Initiatives. He is Co-Founder and Chair of Steering Committee of IEEE IoT Journal; Member of Steering Committee of IEEE Transaction on Big Data; guest editor of several IEEE publications; CoFounder of the IEEE Big Data Initiative; and has served as General Chair, Keynote Chair, Panel Chair, and Technical Program Chair of many IEEE major conferences. He has given several Keynote speeches in IEEE as well as international conferences. He is an expert on Big Data Analytics with extensive industry experience including with the Bell Laboratories as well as the Info Lab of the AT&T Shannon Labs – Research.