Computer Communications 180 (2021) 210–231

Contents lists available at ScienceDirect

Computer Communications

journal homepage: www.elsevier.com/locate/comcom

Review

Edge and fog computing for IoT: A survey on current research activities & future directions

Mohammed Laroui [a,b,c], Boubakr Nour [d], Hassine Moungla [b,c,*], Moussa A. Cherif [a], Hossam Afifi [c], Mohsen Guizani [e]

[a] Djillali Liabes University, Sidi Bel Abbes, Algeria
[b] Université de Paris, Paris, France
[c] Telecom SudParis, Institut Polytechnique de Paris, Palaiseau, France
[d] Beijing Institute of Technology, Beijing, China
[e] Qatar University, Doha, Qatar

ARTICLE INFO

Keywords:
Internet of Things (IoT)
Edge computing
Cloud computing

ABSTRACT

The Internet of Things (IoT) allows communication between devices, things, and any digital assets that send and receive data over a network without requiring interaction with a human. The main characteristic of IoT is the enormous quantity of data created by end-user's devices that needs to be processed in a short time in the cloud. The current cloud-computing concept is not efficient to analyze very large data in a very short time and satisfy the users' requirements. Analyzing the enormous quantity of data by the cloud will take a lot of time, which affects the quality of service (QoS) and negatively influences the IoT applications and the overall network performance. To overcome such challenges, a new architecture called edge computing — that allows to decentralize the process of data from the cloud to the network edge has been proposed to solve the problems occurred by using the cloud computing approach. Furthermore, edge computing supports IoT applications that require a short response time and consequently enhances the consumption of energy, resource utilization, etc. Motivated by the extensive research efforts in the edge computing and IoT applications, in this paper, we present a comprehensive review of edge and fog computing research in the IoT. We investigate the role of cloud, fog, and edge computing in the IoT environment. Subsequently, we cover in detail, different IoT use cases with edge and fog computing, the task scheduling in edge computing, the merger of software-defined networks (SDN) and network function virtualization (NFV) with edge computing, security and privacy efforts. Furthermore, the Blockchain in edge computing. Finally, we identify open research challenges and highlight future research directions.

Contents

* Corresponding author at: Université de Paris, Paris, France.
E-mail addresses: mohammed.laroui@u-paris.fr (M. Laroui), n.boubakr@bit.edu.cn (B. Nour), hassine.moungla@u-paris.fr (H. Moungla), moussa.alicherif@univ-sba.dz (M.A. Cherif), hossam.afifi@telecom-sudparis.eu (H. Afifi), mguizani@ieee.org (M. Guizani).

https://doi.org/10.1016/j.comcom.2021.09.003
Received 21 July 2020; Received in revised form 27 June 2021; Accepted 3 September 2021
Available online 23 September 2021
0140-3664/

1. Introduction

The successive emergence of new generations of networks has led to serious challenges in terms of providing the requirements of various new applications, most of which require advanced infrastructure in order to provide the necessary resources to ensure high quality of the service provided. For this reason, the short response time in addition to analyzing the various data in a short time is considered one of the most important problems that need care and scrutiny in order to ensure it at the highest level of continuity in providing the service.

The term Internet of things was envisaged and mentioned in the late 1990s by professors at MIT who defined the future world of communication. The main objective behind the IoT is to analyze and process data emanating from massive devices, in the cloud. This process, also called cloud computing [1] where the huge in numbers but rather small amounts of individual data gathered by connected things, can be processed in the cloud. Big data architectures such as Hadoop and Spark were initially employed but because of the dramatic increase of connected things and the evolution of the IoT, the cloud computing quickly showed its limits. It is not efficient to simultaneously support this large number of devices, especially that most applications in the IoT category, are time sensitive. Cloud was down-scaled to edge computing [2]. It allows data analysis process at the network edge and supports the requirements of the future generations of networks.

1.1. Related surveys

Different surveys have been proposed for each of cloud, edge, and fog computing based IoT. In the next step, we present a review of the related survey papers along with their contributions and limitations, Table 1 provides a summary of these subsections as well as a comparison with our survey.

Yi et al. [3] surveyed fog computing applications and use cases such as augmented reality (AR), content delivery and caching, mobile big data analytics, etc. The authors also discussed different issues related to fog computing with SDN/NFV, QoS metrics, computation offloading, etc. However, the study provided is very short and limited. Mouradian et al. [6] provided a review of different evaluation criteria in fog computing including network architectures and algorithms. The authors described both fog and content delivery networks [18], and a fog system for detecting and fighting fires [19].

Although the authors provided some key guidelines, the paper is missing different important aspects including security and privacy. Similarly, Hu et al. [7] presented the fog computing concept from different perspectives such as real-time interactions, low latency applications, mobility support, geographical distribution, etc. The authors highlighted the differences between cloud and fog computing, and the key technologies to enable fog computing based networks. However, the simulation tools and edge computing have not been covered.

Mukherjee et al. [10] summarized the fog computing architectures based on different technologies and systems. The authors also presented different open research challenges and future directions have been discussed. However, security and privacy efforts have not been reviewed. While Ni et al. [8] reviewed the security and privacy issues in fog computing in general and IoT applications in particular. Although, the authors presented some guidelines and research directions, focusing on one aspect is a major point of this work.

Mahmud et al. [12] focused on fog computing, the key components, and different challenges. The authors provided a comprehensive taxonomy on fog computing but, the simulation tools were not covered.

Table 1
A summary of existing related survey papers.

Ref.	Topics covered	Limitations	Year
Yi et al. [3]	• Overview of fog computing. • Fog computing use cases & applications. • QoS issues. • Security & privacy issues.	• Very short & limited study. • Learned lessons.	2015
Chiang et al. [4]	• Networking context of IoT based on edge computing. • Fog computing architecture benefits. • Fog computing use cases & applications.	• Integration of edge computing With other architectures (SDN/NFV, etc.).	2016
Shi et al. [5]	• A vision on edge computing. • Edge computing benefits. • Edge computing case studies. • Challenges & Opportunities.	• Edge computing platform & architecture. • Integration of edge computing With other architectures (SDN/NFV, etc.). • Recent research reviews. • Learned lessons.	2016
Mouradian et al. [6]	• Fog system research (architecture & algorithms). • Fog computing use cases and evaluation criteria. • Challenges & Research directions. • Learned lessons & Prospects.	• Security & Privacy.	2017
Hu et al. [7]	• Fog computing architecture & applications. • Challenges and open issues.	• Simulators for edge computing environment.	2017
Ni et al. [8]	• Overview of fog computing (evolution from cloud to fog, fog computing architecture,..). • IoT applications based on fog Computing. • Fog computing security. • Issues, challenges & future research directions.	• Fog computing protocols & services.	2017
Baktir et al. [9]	• SDN-Edge computing corporation. • Edge computing uses cases. • Future directions & research areas.	• Platforms & Simulators for SDN-Edge computing environment.	2017
Mukherjee et al. [10]	• Fog computing-based architectures. • QoS model in fog computing. • Resource management & Service allocation issues in fog computing. • Fog computing applications. • Open research challenges & Future directions.	• Security & Privacy review in fog computing.	2018
Yu et al. [11]	• Review of IoT & edge computing. • IoT-Edge computing integration. • Benefits of edge computing Based-IoT. • IoT-Edge computing challenges.	• Simulators for edge computing environment.	2018
Mahmud et al. [12]	• Taxonomy of fog computing. • Fog nodes configuration. • Challenges in fog computing.	• Simulators for edge computing environment.	2018
Omoniwa et al. [13]	• Fog/Edge computing-based IoT (FECIoT) architecture. • FECIoT protocols, services & applications. • Security & Privacy in FECIoT. • FECIoT simulation tools. • Open research issues.	• Integration of edge computing with other architectures (SDN/NFV, etc.). • Review of task scheduling in edge computing. • Review of vehicular edge computing (VEC).	2018
Naha et al. [14]	• Fog computing architecture. • Infrastructure & Platform requirements. • Fog computing applications.	• Learned lessons. • Integration with new technologies (blockchain, AI).	2018
khan et al. [15]	• Cloud & Edge computing systems. • Cloud & Edge computing applications. • Mobile Edge computing. • Open challenges.	• Integration of edge computing with other architectures (SDN/NFV, etc.). • Simulators for edge computing environment. • Review of Vehicular edge computing (VEC).	2019
Puliafito et al. [16]	• Fog-IoT platforms. • Fog-IoT application domains. • Fog-IoT open issues.	• Fog-IoT Integration with blockchain, AI, etc.	2019

(*continued on next page*)

Table 1 (*continued*).

Ref.	Topics covered	Limitations	Year
Martinez et al. [17]	• Fog computing design model. • Fog computing framework. • Simulation/Emulation tools. • Open issues & opportunities.	• Learned lessons. • Fog integration with blockchain, AI, etc.	2020
Our Survey	• IoT overview. • Edge computing architecture. • Edge computing use cases & applications. • Review of task scheduling in edge computing. • Integration of edge computing with SDN/NFV. • Review of security & privacy efforts. • Review of Blockchain in edge computing. • Future research directions. • Learned lessons.	–	2021

Baktir et al. [9] reviewed the edge computing concept and discussed the SDN-Edge computing cooperation paradigm. In addition, different scenarios and use cases have been elaborated, as well as describing the SDN capabilities on top of edge computing. However, it focuses only on one technology (i.e. SDN).

Focusing on IoT networks and applications,

Chiang et al. [4] focused on IoT applications and its challenges in the fog computing environment. The authors described how fog computing may help to overcome IoT issues in an effective way, such as latency, security, etc. However, the survey paper did not cover recent technologies such as VANET, SDN, NFV, etc. Also, other fog computing mechanism are not covered.

Similarly, Shi et al. [5] targeted the edge computing, and discussed its need in IoT networks. The authors also provided different use-case scenarios such as video analytics, cloud offloading, smart homes, smart cities, and collaborative edge. At the edge, a summary is provided with some challenges in programmability of edge computing, integration with Named Data Networking [20–23] and MobilityFirst [24], data abstraction, etc. However, this survey did not cover different platforms and network architectures for fog computing. Yu et al. [11] targeted edge computing for IoT applications, by providing the advantages of such a merger as well as the challenges. However, the work is missing the platforms, systems, and the used simulation tools.

Omoniwa et al. [13] reviewed edge/fog computing-based IoT applications. The authors provided a wide review on different architectures, protocols, and technologies. However, they did not cover the integration of edge computing with other recent architectures. Naha et al. [14] discussed and presented the overview, state-of-the-art, architecture, and other similar technologies in fog computing. Nevertheless, the survey did not cover recent technologies based on edge computing such as AI.

Khan et al. [15] presented a comprehensive survey on edge computing, they reviewed the cloud, edge and mobile edge computing systems, besides they detailed the different applications. However, the authors did not cover the integration of edge computing with other recent architectures. Puliafito et al. [16] reviewed the fog-IoT domain. Authors focused on the fog-IoT platforms, and application domains, while the integration of fog-IoT with blockchain AI is missing in this survey.

Finally, Martinez et al. [17] presented a detailed overview of fog computing by reviewing the design model, architectures, and framework. However, the combination of fog computing with recent technologies is missing in this work.

1.2. Our contributions

In contrast with the aforementioned related surveys, our work focuses on edge/fog computing[1] for the IoT.

[1] Without loss of generality, we use the terms 'Edge Computing', and 'Fog Computing' interchangeably in this paper.

In this regard, the major contributions are summarized as follows:

1. We comprehensively review edge computing technology in the environment of the IoT.
2. We describe in detail, the IoT technology, the edge computing technology, and its benefits compared to cloud computing. Moreover, we overview the applications of edge computing based IoT.
3. We present an in-depth overview of the issues raised in the Edge-IoT environment such as *Task Scheduling, SDN/NFV, Security & Privacy, and the Blockchain.*
4. We describe the challenges faced the edge computing on top of the IoT applications such as *scalability, high mobility support, energy management, artificial intelligence , and of course security & privacy.*
5. We present the learned lessons for Edge-IoT. In particular, we focus on the necessary transition from cloud to edge. Then, the evolution of Edge-IoT applications. Moreover, the security importance of Edge-IoT.

1.3. Organization

The remainder of the paper is organized as follows. Section 2 presents an overview of the IoT. In Section 3, we show a vision on cloud computing. In Section 4 the detail of edge computing is presented. In Section 5, we present edge computing use cases and applications. Section 6 provides a research review of task scheduling in edge computing. Beside, the SDN/NFV based edge computing is presented in Section 7. Moreover, in Section 8 the security & privacy efforts in edge computing are presented. While the Blockchain findings in edge computing environment is presented in Section 9. Next, Section 10 highlights the future research guidelines & directions. Finally, the learned lessons and conclusion are presented in Section 11.

Fig. 1 shows the reading plan of our survey.

2. Internet of Things (IoT)

The evolution of mobiles devices, embedded systems, and vehicles helped to create a smart world of connected devices that may sense, collect data, collaborate, and take decisions without interaction with humans [25]. This smart ecosystem is called the Internet of things [26].

2.1. Definition

It is a new technology envisioned as a network of devices and machines that communicate with each other and the Internet. The IoT is known as one of the important enablers for future technologies. It also has a great interest from companies. In a broader sense, IoT aims to create systems based on the interconnection of smart objects. These objects exchange information among themselves using different

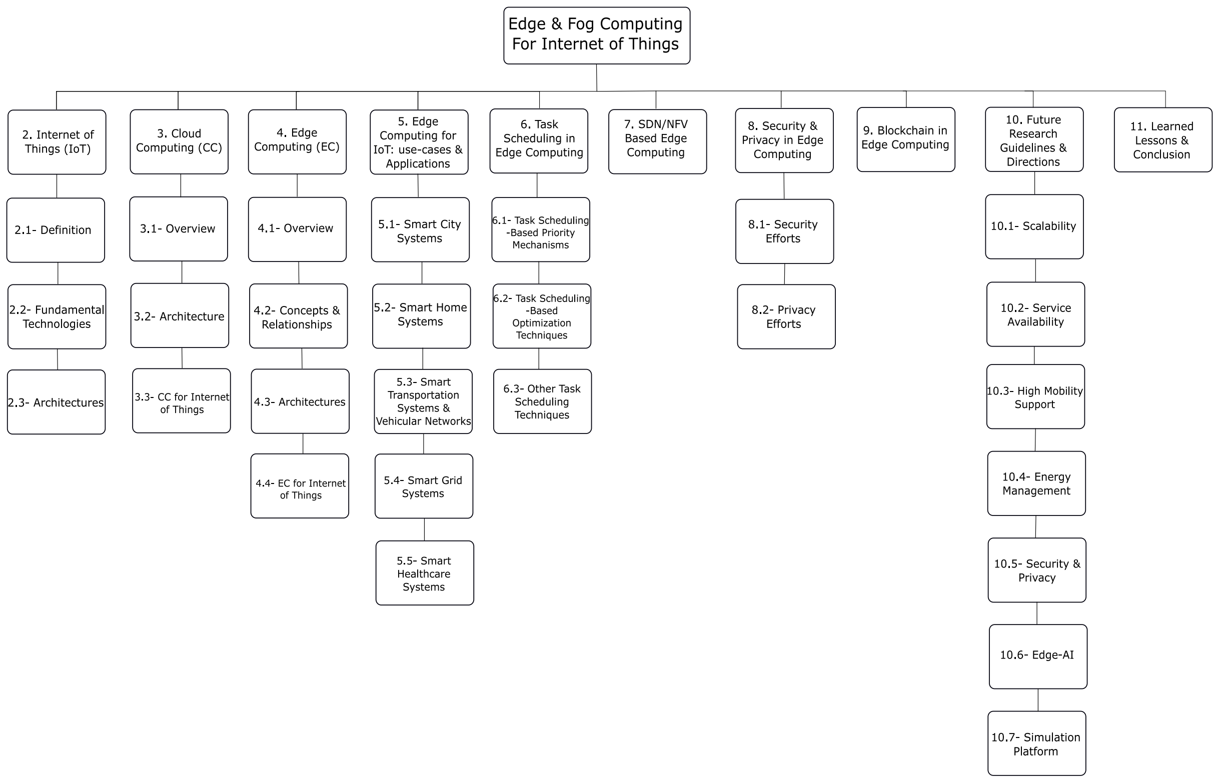

Fig. 1. Survey reading plan..

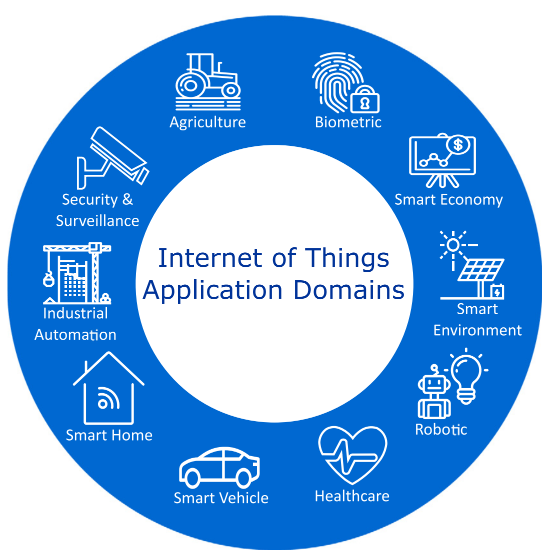

Fig. 2. IoT application domains [27].

protocols, such as Wi-Fi, Bluetooth, ZigBee, etc. The main characteristic of the IoT is the integration of different technologies of communications (e.g. wired & wireless sensors, actuator networks, tracking and identification networks, etc.) to improve the cooperation and interaction between various technologies. Fig. 2 shows the application domains of the IoT.

2.2. Fundamental technologies

The required components for the IoT consist of three types [27]: (a) actuator: hardware equipped with sensors, (b) middleware of storage and data analytics, and (c) interpretation and visualization tools. The following technologies make up the components defined above:

- *RFID & NFC*: RFID (Radio Frequency Identification) technology [28] is a major innovation in the communication paradigm that enables the design and development of microchips. It allows an automatic identification of anything attached with an electronic barcode. RFID devices, generally called RFID tags, is a microchip for wireless data transmission. the RFID tags send data over the air, the signal is recovered by an RFID reader which allows the identification of objects corresponding to the received information (barcode). For the IoT, the RFID is one of the devices most used for the building of applications, such as controlling privacy [29], smart healthcare and social applications. NFC (Near Field Communication) [30], is a half-duplex protocol for wireless short-range communication which facilitates the mobile phone usage of people, it offers various services of loyalty applications such as access keys for houses and offices. In addition, it allows smartphones to be used to lock/unlock the house doors, and car, exchange business cards, pay for public transportation, newspaper, and much more.
- *Wireless Sensor Networks (WSN)* [31]: is a large number of smart sensors that aim to collect data (e.g., movement, temperature, etc.), process, analyze and transfer information [27]. A Wireless Sensor Network is mainly composed of the following components: (a) the capture unit (sensor) which is responsible for collecting data as signals, and transforming these signals into digital information understandable by the processing unit, (b) the processing unit which is responsible for analyzing the data captured, (c) the transmission unit that performs all transmission and reception of the data, and (d) the energy control unit which is an essential part of the system, it must distribute the energy available to the other modules in an optimal manner.

Moreover, several types of applications can be in operation using WSN including environmental monitoring (e.g., pollution, landslides, forest fires, etc.), commercial (e.g., smart light control, robotic), military, and medical applications, etc [32].

- *Data Storage and Analytics*: in IoT, an enormous quantity of data is generated and exchanged which requires a very large storage size.

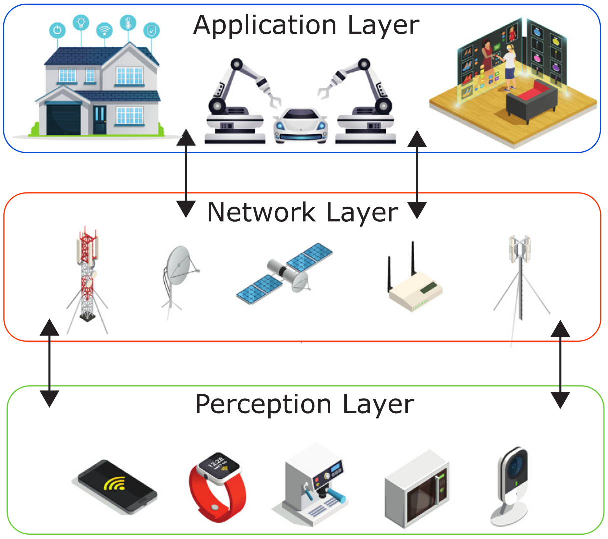

Fig. 3. Three-layer IoT architecture.

For this reason, the data storage is an important issue in the IoT. Different solutions have been proposed for the analysis and storage of data to provide efficient communication, e.g., smart cities, smart and connected communities, and smarter healthcare. In the last years, the storage of data in the cloud became more popular [27], while nowadays, cloud-based storage and analytics are mostly used and preferred which can accelerate data processing and provide a reliable data exchange.

2.3. Architectures

The IoT architecture is still under construction and there is no standardized architecture yet proposed [33]. Different IoT architectures have been proposed that can support specific or generic use cases. A basic/generic IoT architecture consists of three layers (see Fig. 3):

(a) perception layer that includes sensors, cameras, RFIDs, etc., (b) a network layer that is responsible for the transmission of the collected/generated data from the previous layer, and (c) the application layer that represents the user application. An-other IoT architecture called cloud computing [1] has been designed with 2-tiers perspectives. The IoT devices may connect directly to the cloud for data processing. This architecture has some problems in the IoT, for example, it does not support delay-based applications that require a short response time. To overcome such issues, a new architecture based on edge computing [2] which is a 3-tiers architecture that processes the data on the network edge which provide an efficient services close to end-user devices.

3. Cloud computing (CC)

The rapid increase in connected/smart devices in the world and the change in users' and applications' requirements with a large quantity of data processing led to a set of novel technologies to allow fast data processing and reliable services. Cloud computing is one of these technologies.

3.1. Overview

The use of smartphones and computers has increased exponentially. This growth has heightened the need for efficient architectures that have naturally emerged to support the increase of connected devices, as well as the data generated and processed. Cloud computing [1] is an innovation paradigm, it seeks to provide various services to end-users in the cloud. Different types of cloud can be deployed including private, public, hybrid, and community. The public cloud [34] provides services to a large number of users on the Internet. The private cloud [35] offers specific services to private organizations. The community cloud [36] aims to provide services to a group of organizations. Finally, the hybrid cloud [37] is good for organizations to balance between cost and issues of control.

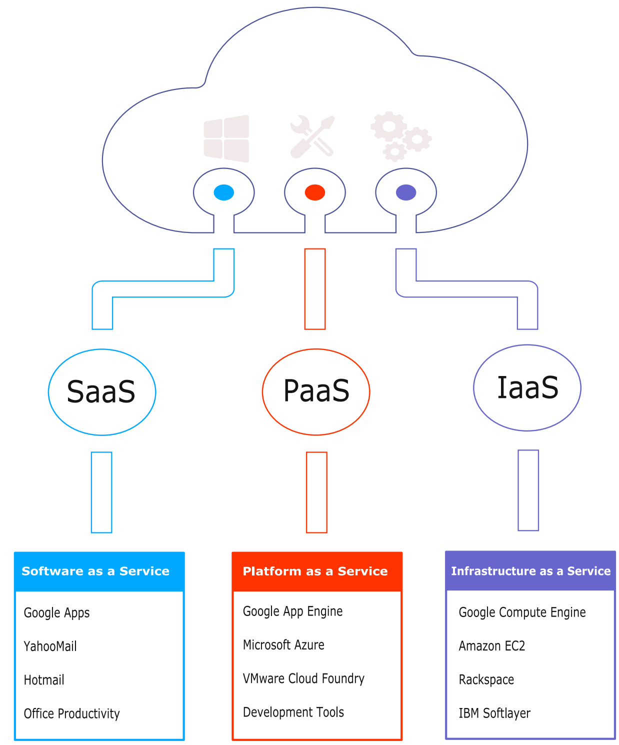

Fig. 4. Cloud computing services.

3.2. Architecture

An architecture must define what kind of service to offer by the cloud system. Three main categories of cloud services (as shown in Fig. 4) can be distinguished:

1. *Software as a service (SaaS):* [38] is an application programming interface (API) or web service(s) that encourages developers to create their applications in the cloud. SaaS provides software solutions that can be accessed via the Internet without the need to install any application on a user's local computer.

2. *Platform as a service (PaaS):* [39] is a way to rent operating systems, network capacity, storage and hardware over the Internet. This model allows users to run their applications in virtualized servers in the cloud without the need to extend their local resources. PaaS generally provides services for designing and deploying applications.

3. *Infrastructure as a Service (IaaS):* [40] allows users to manage and control software and hardware resources at the cloud. The use of IaaS has different benefits where users can access applications and platform from anywhere, using any-device, and from any-network, provide virtual infrastructure, as well as provide services of load balancing and a large capacity for computing.

3.3. CC for Internet of Things

The cloud computing and the IoT are two main technologies that contribute to our daily life by providing various services to the IoT users. Therefore, we can merge them into one global technology, namely CloudIoT paradigm [41]. Botta et al. [42] tried to integrate cloud and the IoT, by allowing the cloud to provide the required

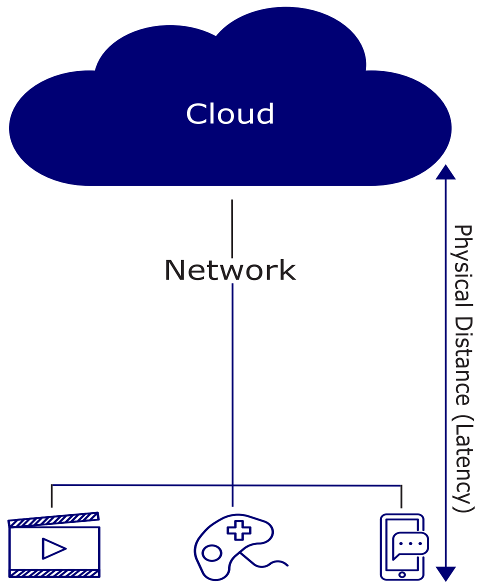

Fig. 5. Generic cloud computing architecture.

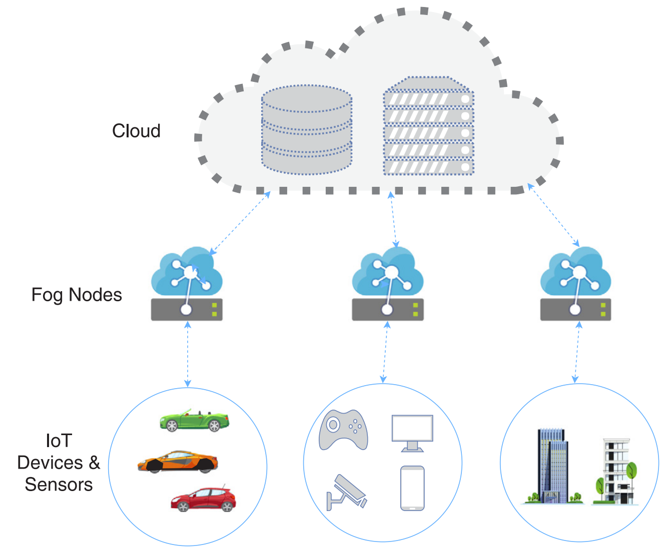

Fig. 6. Generic edge computing architecture.

services to IoT devices such as storage and computation. Similarly, Neagu et al. [43] proposed a health monitoring service called the HM oriented Sensing Service scenario (HM-SS) that provides large medical facilities based on the cloud-IoT architecture. Ismail et al. [44] studied the efficiency of a virtual machine placement and task scheduling algorithm in the Cloud-IoT architecture in terms of energy consumption by data centers. Almolhis et al. [45] presented a review of the security issues in the CloudIoT system. In the *CloudIoT* paradigm, the end users connect directly to the cloud using the Internet and start exchanging data over the network which results a massive quantity of data in a short time, a generic cloud computing architecture for IoT is illustrated in Fig. 5. However, the centralized architecture of the cloud is not efficient to process the massive quantity of data generated by the IoT devices that require a short response time. To overcome such an issue, an alternative paradigm, namely edge computing, has been used which processes the data in connected devices or the local gateways.

4. Edge computing (EC)

The IoT will potentially connect billions or trillions of devices [46]. All these devices generate a massive quantity of data [5]. Furthermore, the new generation of applications such as video streaming, online gaming,..etc, requires a short response time [5,47], besides, energy consumption is an important issue in wireless communication because of the limited resources of IoT devices that cannot provide computation and processing locally. Thus, the centralized architecture does not fulfill IoT application requirements by providing storage, computation, and networking resources in data-centers that are owned by companies, such as Google, Microsoft, and Amazon. In addition, the data generated and processed needs to be sent to the cloud for processing which takes a large response time and may effect both end-user QoS and experience.

4.1. Overview

The edge computing aims to be the future IoT solution that solves different issues including time-constrained and computation-based applications. The benefits of processing data at the network edge are: reduce the networking load and communication latency, break the monopoly of big inventors [2], give the small and medium inventors every chance to help nurture future innovations, reduce the energy consumption of the mobile nodes, and eliminating the congestion within the core network, as well as provide more reliability, security, and the privacy protection.

4.2. Concepts & relationships

To cope with the confusion over the difference between edge computing and fog computing, we start this discussion by describing both edge and fog computing from different perspectives.

Some researchers define edge and fog computing as the same concept with differences only in their names [48], while others differentiate them as two different concepts. Goscinski et al. [49] claims that edge computing focuses on data processing at the edge, while fog computing is located out between the cloud and the edge cloud, and thereby include the edge. On the other hand, Chiang et al. [50] said that the fog computing is an end-to-end architecture that distributes the control, storage, computing and networking function closer to end-users along the cloud-to-things, while the edge refers to the edge network, with equipment such as base stations, home gateways and edge routers. Furthermore, Pan et al. [51] said that the fog computing is a background of the IoT, it extends the cloud computing and different services to the devices such as switches, routers, multiplexers, etc. While the edge computing pushes data, services and applications from the core to the network edge, based on the core-edge topology [5,52]. The video analytics, smart city, smart home and cloud offloading are application examples of edge computing.

In a nutshell, both edge and fog computing have the same research topics and both of them aim at the decentralization of data processing from the cloud to the network edge.

4.3. Architectures

The fog/edge layer generally is located between the cloud and the end users (as shown in Fig. 6), and includes the following main components [48,53,54]: (a) *Authentication and Authorization*: identify the access control rules and policies, (b) *Offloading Management*: defines types of information in the offloading process, the partition for offloading and the manner to design an optimal offloading scheme, (c) *Location Services*: that tends to learn the mobility model by mapping the network with the physical locations, (d) *System Monitor*: to provide different information such as usage, workload and energy to the other components, (e) *Resource Management*: which is responsible for resource discovery and allocation, dynamic joining and leaving of the fog node and maintaining and provisioning of resources, and (f) *VM Scheduling*: that aims to provide an optimal strategy for virtual machine scheduling.

4.4. EC for Internet of Things

The edge provides networking services, storage and computation to end users in IoT [55]. For example, a CCTV network does not need to send all data to the cloud, the movement detection algorithms or facial recognition running on the fog/edge layer, hence saving storage space and bandwidth. So, the fog/edge will be the best option of applications that require a temporary storage. In addition the fog/edge can play its role in the future, where the IoT and wireless sensors networks presents with the integration of heterogeneous protocols and devices for enhancing services [56].

The edge computing is an appropriate paradigm for the current Internet in general and the IoT in particular in which this distributed architecture may provide a high-level communication and efficiency in the edge network rather than at the cloud-level. It supports a wide range of today's IoT applications, especially those that require a short response time.

Table 2 outlines the main characteristics of cloud compared with fog/edge computing.

5. Edge computing for IoT: Use cases & applications

The edge computing provides an efficient platform for smart IoT applications, such as smart homes, smart vehicles, smart grid, smart cities, smart healthcare, etc. This section surveys the existing efforts on IoT application based edge computing, while Table 3 outlines the main features for such proposed applications.

5.1. Smart city systems

A smart city [80] is an urban area where numerous sectors pull together to achieve results efficiently through the real-time analysis of information collected from multiple sources. Smart cities aim to decrease the energy waste and traffic congestion which may directly enhance the quality of life. Different technologies are used in smart cities which will be a massive economic market [58]. The deployment of smart cities still faces different challenges and issues such as big data analysis, large-scale sensing networks due to thousands of connected sensors and actuators in a large geographic area, machine-to-machine (M2M) and cooperative communication (CC) in wireless networks that aim to improve the efficiency in M2M network resources, and road traffic networks consist of studding and integrating data learning and processing algorithms in the intelligent traffic system [81].

Smart cities require an efficient and intelligent data analysis for data monitoring in order to achieve a fast and automated decision without the need for human interaction [82]. Hereby, guarantee a reliability of components and safety of people. Moreover, the smartness requires an efficient platform which contains many advanced algorithms, such as supervised and non-supervised machine learning algorithms [83], density distribution modeling [84] and sequential data learning [85].

The edge computing is an ideal platform for smart cities [86], due to its design, the data process will happen at the network edge instead of the cloud [5] and enhance the network delay and user experience. This is an essential element to build reliable smart cities that are characterized by the following:

• *Huge Quantity of Data*: cities will produce massive data per day [87]. The data generated varies from transport, utility, traffic lights, etc. Handling all the data in a centralized cloud is unrealistic as the processing of the data will take a long time and too much resources. For this, the data processing in edge of the network will resolve the problems of centralized cloud by providing an efficient services for data processing which is required by smart cities applications.

• *Low Latency*: Most smart cities applications require a low latency such as public safety and health emergencies [88]. The edge computing is a promising paradigm, since it could organize the network structure and decrease the data transmission time. Diagnosis and decision could be made at the network edge which would decrease the latency compared to the centralized cloud paradigm that has a long response time [5].

• *Location Awareness*: some smart cities applications, such as utility management and transportation, are geographic-based in nature. The edge computing supports the location awareness by collecting the data based on geographic sites without the need to send data to the cloud. This prevents the data access delay, and increases the QoS, as well as speeding up and providing a transparency of the information transferred [5].

5.2. Smart home systems

The smart home [89] aims to allow intelligent control of different smart devices that are connected inside homes, such as TV, air-conditioner, cooker, fridge, etc. The intelligent services [90] can be classified into three types: (a) *Home Automation Services*: such as controlling air cleaners, air conditioners and curtain movements, (b) *Home Security Services*: such as preventing gas explosions and detection of potential crimes and lastly, (c) *Home Management Services*: such as intelligent control of smart devices like TV and cooker.

The connected smart devices generate a large quantity of data for smart control and decision-making inside homes. The analysis and the processing of this data require an enormous quantity of resources and storage which need a scalable architecture to guarantee quality and continuity of service without any degradation. The edge computing offers a highly distributed architecture for building smart homes in an efficient way [56,91] by processing the data at the network edge which provides: low latency, efficient data processing and less energy consumption.

The edge computing-based smart home aims to enhance the future IoT applications, especially those that require a short response time, such as intelligent control of smart devices and the surveillance inside the home.

5.3. Smart transportation systems & vehicular networks

A smart vehicle environment [92,93] consists of connected cars, it can be classified in the following communication models: vehicle-to-vehicle (V2V) [94], vehicle-to-infrastructure (V2I) [95], and vehicle-to-grid (V2G) [96]. The edge computing offers an efficient distributed architecture for smart vehicles. It can support high mobility of vehicles and interactions among them [97]. Different applications in smart vehicles and transportation systems may benefit from edge computing, including:

• *Safety Applications*: this kind of applications can be used to adjust hazards on the road [98], sending notifications and warnings about crashes, curve speeds, traffic violations, pre-crash sensing, etc. They could include sensing of approaching emergency vehicles.

• *Convenience Applications*: include personal routing and advice of congestion situations [99], as well as, in some incidents such as network breakdown and power failure. In some scenarios, the connected vehicle can play an important role in the monitoring of road and weather by sharing information from vehicle sensors, thus providing SOS and emergency calls.

• *Smart Traffic Lights*: smart lights synchronize the connected vehicles by sending warning signals to share traffic data which can help vehicles in different situations [100] including problems with traffic lights [101], and warnings of approaching pedestrian crossings [102].

• *Smart Parking Systems*: Most big cities faces traffic congestion. As a consequence, finding an empty space in a parking lot is difficult and expensive. For this it is important to solve the congestion problem by building smart parking connected to smart vehicles to automatically control the access to available spaces in parking lots. The parking system informs the smart vehicles if there are available spaces in the parking lot using notification messages through a wireless network or

Table 2
Characteristics of fog/edge compared to cloud.

Characteristics	Cloud	Edge/Fog
Location	Centralized.	Distributed in different geographical locations.
Capacity	Very large size data centers.	A lot of small size fog nodes that form a large system.
Energy consumption	High.	Low.
Latency	High, because of the large distance between the end users and the cloud.	Low, because of the short distance between the edge and the end users.
Proximity of resources and services	Far from end users, in the data centers.	Close to end users, in the edge of network.
Applications	Supports applications that does not require short delay. Mainstream cloud applications.	Support most types of applications. VR. Smart homes. Smart vehicles. Smart cities.
Service Cost	High, due to the monopoly of data centers by big companies.	Lower cost, due to the processing of data at the network edge.

publish–subscribe communication model. This allows people to gain time and effortlessly find a place to stop their vehicles.

• *Commercial Applications* : represents paid services of diagnostics for vehicle problems and location-based services, such as entertainment and advertisements, updates of social networks, etc [103]. These applications are provided by private companies to generally offer special applications or sensors installed on-board the vehicles which can directly connect with the edge server of the associated company.

The edge computing is an efficient platform that provides various benefits and responses to smart vehicles and intelligent transportation requirements. The edge servers are localized nearby to smart vehicles, which allows rapid and efficient services to enhance the quality of life and experience.

5.4. Smart grid systems

A smart grid system [104] consists of smart meters which exist in different locations to measure the real time status for the distribution of electricity. This information is analyzed by a centralized server called SCADA [105], that by its return sends commands about emergency demands, responds to any change request to stabilize the system and protects the power grid.

The edge computing may offer great services to smart grid [67,106]. With the edge computing paradigm, the SCADA can be equipped with a decentralized model which can improve the network cost, security and scalability. In addition, integrating power generators (e.g., solar panels, wind farms, etc.) with the main power grid that offers a centralized control of the power network [107,108]. With the edge computing, the smart grid system will turn into a hierarchical architecture (multi-tier architecture) with interactions among the SCADA [55]. In such a system, the edge layer is in charge of the micro-grid and exchanges information with the neighboring edge and the higher tiers. The final coverage is managed by SCADA which is responsible for economic analytics.

5.5. Smart healthcare systems

In healthcare systems [109], data management is one of the sensitive issues, as users' data contain important and private information that need to be analyzed and processed in an efficient and secure way. Remote Patient Monitoring (RPM) [110] allows the monitoring of patients regardless of their location, and their caregivers and families are engaged remotely [111]. The RPM system contains three modules: data acquisition, visualization and diagnostics. To acquire the data, the patient is equipped with sensors (e.g., blood glucose sensor), after acquiring the data it will be sent from the patient's smart phone to the processing unit (diagnostic module) for processing. Finally, the calculated analytics are displayed by the visualization module.

The edge computing guarantees the service efficiency in smart medical systems [112] which is considered as an important technology in the IoT ecosystem. The data analysis of the patient requires an efficient platform that guarantees short response time, security, etc., which is provided by the edge computing architecture.

6. Task scheduling in edge computing

The task scheduling problem in edge and fog computing [113] consists of assigning tasks to fog nodes that are located at the network edge, and providing a high-performance execution for end-users' requests. The objective is to find an optimal exploitation of memory allocation and CPU execution for tasks. In the following, we review the existing task scheduling techniques categorized into different classes:

6.1. Task scheduling-based priority mechanisms

Priority-based task scheduling is a mechanism where tasks are scheduled according to the priority order. In the following, we present the existing solutions proposed for priority-based task scheduling in the edge computing environment.

Pham et al. [114] presented a task scheduling algorithm in the Fog-Cloud environment. The proposed algorithm performs the scheduling by specifying the priorities of tasks, and determining which node to execute tasks. The obtained results show that the proposed algorithm provides an efficient balance between the cost and performance of task execution compared to other algorithms, such as Dynamic Level Scheduling (DLS) algorithm [115], and Heterogeneous Earliest-Finish-Time (HEFT) algorithm [116]. However, this algorithm did not take into consideration the energy consumption.

Wang et al. [117] proposed an approach for task scheduling named HealthEdge, which sets the priorities for different tasks using the collected data of human health status and determines if the said task should run in the local device or in the cloud. Based on real traces of five patients, the performance evaluation shows that HealthEdge can efficiently assign different tasks between the network edge and the cloud., which reduces the task processing, bandwidth and time, as well as increasing the workstation utilization in the local edge. The major drawback of this solution is ignoring the energy consumption.

Choudhari et al. [118] proposed a priority levels-based task scheduling algorithm in the fog environment. The fog server processes the tasks sent from the clients to the fog layer if the required resources to perform the tasks are available in the assigned fog server and are satisfied by the fog layer, the tasks processed by one or many fog servers in the fog layer. Otherwise, (no resources available), the tasks are forwarded to the cloud for processing. The performance evaluation results show that this approach reduces the response time and decreases the cost.

Table 3
Summary of IoT applications using edge computing.

Use case	Ref.	Purpose	Limitations
Smart cities	[57]	• Power monitoring/element control. • Access control and cabinet telemetry. • Event-Based video. • Traffic management. • Connectivity on demand.	• There are not any analytical approach to substantiate their design choices.
	[58]	• A distributed architecture that supports the integration of many infrastructures in smart cities.	• Lack of mobility. • Lack of QoS management.
	[59]	• A framework perform green survivable for collaborative edge computing in the Wireless-Optical Broadband Access Network (WOBAN) supporting smart cities.	• Lack of scalability.
	[60]	• Fog computing architecture for smart living application.	• Require the scalability and mobility support.
	[61]	• Fog computing-based smart urban surveillance (traffic monitoring).	• Huge computational resources.
	[62]	• An OpenStack platform (Stack4Things) based fog computing in smart cities.	• Lack of dynamic discovery of internet objects. • Require the support of multi-protocol in the applications and communications level.
	[63]	• A multi-tier model for smart cities applications in fog computing.	• Real-time data processing become huge in the space based storage.
Smart homes	[64]	• Smart devices connected via home gateways constitute a local home network to help persons in activities of daily life.	• Require security mechanism.
	[65]	• Home energy management system in fog computing environment.	• Require security mechanism.
	[66]	• Intelligent decision system in fog computing environment to manage residence requests.	• Require security mechanism.
Smart grid	[67]	• A fog computing based smart grid model for control the balance energy load and power usage.	• Require to ensure the security.
	[68]	• A cloud-fog computing based model for resource management in smart grids.	• Require to ensure the security.
	[69]	• A resource allocation model for fog computing based micro grids to optimize resources in the residential building.	• Require to ensure the security of the system.
Healthcare	[70]	• Telehealth application in fog computing environment.	• Require mechanisms of scalability. • The mobility criteria is not met.
	[71]	• Smart e-health gateway in Fog-IoT to assist healthcare services.	• Require to ensure the security of the system.
	[72]	• Remote patient health monitoring system in fog computing environment.	• Require some mechanisms for securing the data and the fog system.
	[73]	• Fog-Cloud architecture for monitoring the health of person during working hours.	• Require some mechanisms for optimal network load.
	[74]	• IoT based architecture for u-Healthcare monitoring.	• Require security mechanism.
	[75]	• An architecture named FIT for analyzing and processing the clinical data of patients.	• The Scalability is not considered. • The mobility of patients is not met. • The interoperability is not met.
	[76]	• An architecture for applications that offering support to persons influenced by COPD.	• The mobility is not met. • The interoperability is not met.
Smart vehicles	[77]	• Smart surveillance for vehicle tracking.	• Require to increase the confidence of accuracy for space–time tracks from the systems.
	[78]	• A vehicular architecture named VFC, where the vehicles are used as infrastructures for computation and communication.	• Need for architectural modules to guarantee the scalability.

(continued on next page)

Table 3 (*continued*).

Use case	Ref.	Purpose	Limitations
	[79]	• An architecture for smart vehicles, where the fog server is located at M2M gateways and RSUs.	• Need to guarantee the scalability.

6.2. Task scheduling-based optimization techniques

Optimization-based task scheduling algorithms allow us to determine an optimal assignment of a lot of tasks submitted to be executed using the lowest number of resources. In edge computing, different solutions have been proposed whose objective is to reduce the resources utilization in the edge layer.

Liu et al. [119] proposed an algorithm for task scheduling in the fog environment, namely Adaptive Double fitness Genetic Task Scheduling (ADGTS). This algorithm optimizes the communication cost. In addition, it provides perfect performance compared to the Min–Min algorithm. However, this approach did not take into consideration the energy consumption and did not discuss the complexity of the used model.

Hoang et al. [120] proposed a task scheduling algorithm in Fog-based Region and Cloud (FBRC). The data processing happens in both the local regions and/or in the remote cloud servers. The authors formulated an integer program named FBRC-IP for task scheduling and showed that it is an NP-hard problem. Hence, they designed a heuristic algorithm to solve this problem. The results demonstrate the performance of the proposed model in terms of resources utilization and latency. However, this approach did not take into account the energy consumption.

Pham et al. [121] proposed the Cost-Makespan aware Scheduling heuristic algorithm (CMaS) in the collaborative cloud and fog environment. The system architecture used composed of three layers: (a) the bottom-most layer that contains IoT devices such as smart-phones and wireless sensor devices, etc. (b) the middle layer that consists of fog computing components which are intelligent fog devices, such as access points, switches and routers, and (c) the upper-most layer that consists of cloud computing components which contain a large number of heterogeneous VMs or cloud nodes. The proposed task scheduling approach is composed of three phases: (i) first, the task prioritizing phase that assigns a priority level to each task, (ii) second, the node selection phase that assigns each task to a processing cloud or fog node in order to achieve an optimal value of the utility function that defines the trade-off between the cloud cost and the schedule length, and (iii) finally, the task reassignment phase that improves the QoS of the system by guaranteeing to satisfy the user-defined deadline. Compared to other algorithms that are Greedy for Cost algorithm (GFC), the well-known HEFT [116], and the CCSH [122], the proposed algorithm is more cost-effective and has better performance. However, this approach did not take account the energy consumption.

Fan et al. [123] presented a solution based on Ant Colony Optimization (ACO) for task scheduling in the IoT environment as a multi-level 0–1 Knapsack problem, which is an NP hard problem. In the proposed algorithm, the value of pheromone is placed between hosts and tasks, which enables the proposed algorithm to maximize the net profits. The results of the simulation show that the proposed solution outperforms the existing heuristic with Min–min and FCFS algorithms. Despite the fact that the proposed algorithm improves system performance, it is costly as it requires a lot of resources for computation.

Kabirzadeh et al. [124] proposed a hyper heuristic algorithm based on test and select technique for scheduling problems in the fog network. The proposed algorithm is used in intelligent surveillance as a case study. In addition, the authors compared the proposed algorithm to three other algorithms; Genetic Algorithm (GA) [125], Particle Swarm Optimization Algorithm (PSO) [126], Ant Colony Optimization Algorithm (ACO) [127], and Simulated Annealing Algorithm (SA) [128]. The performance evaluation shows the efficiency of the proposed hyper-heuristic in terms of energy consumption and execution time. However, the main drawback is the high computational requirements.

Bitam et al. [113] proposed an optimization method called Bees Life Algorithm (BLA). In the first step of BLA, the mobile device sends a request to the fog node located at the network edge. Next, the fog node sends the required parameters and the requested data as a job directly to the administrator node. Afterwards, the administrator node breaks down the received job into a collection of tasks. Here, the bees life algorithm is executed to find the best solution for job scheduling, where each fog node receives its task, executes the job, and sends the results back to the administrator node. Based on the received results, the administrator node waits for the final results. Finally, the final results are sent to the mobile users. The performance evaluation showed that the BLA method is more effective in terms of memory allocation and execution time compared to the Particle Swarm Optimization Algorithm (PSO) [126] and the Genetic algorithm (GA) [125]. However, this approach did not take account the energy consumption.

Wan et al. [129] presented an Energy-aware Load Balancing and Scheduling (ELBS) method based on fog computing in smart factory. The authors established an energy consumption model and an optimization function for load balancing of the manufacturing cluster. They used a PSO algorithm [130] to obtain an efficient solution. Then, they used a multi-agent system in order to guide the workload scheduling of the equipment with the task scheduling mechanism. The obtained results generated from the candy packing line showed that the ELBS method provides an optimal load balancing and tasks scheduling. However, this method requires resources such as computation cost.

Zeng et al. [131] proposed an optimization of image placement and task scheduling based on mixed-integer non-linear programming (MINLP) problem [132] in a fog computing platform supported by SDN Embedded System (FC-SDES). The computational resources are provided from fog nodes and embedded clients. The storage servers are shared by both computation servers and clients. This approach structures resources locally from embedded clients and fog devices. However, it was unavoidable to use more resources from the cloud as the latter is so intensive and large-scale tasks submitted from clients will take a long time to be processed.

Li et al. [133] presented the Task Scheduling of Edge-Cloud System (TSECS) algorithm for task scheduling and resource allocation. TSECS is based on the Markov Decision Process (MDP) and uses real-life data. The authors compared the TSECS algorithm to two other algorithms: a load-balanced algorithm that consists in dispatching the requests to the cloud or edge servers based on serving capacity with the same management of TSECS, and the Best Effort algorithm that allows servers to keep running until the queue is empty. The experiment's results show that the proposed algorithm has less consumption of energy, but it takes a long response time.

Yang et al. [134] proposed a Maximal Energy-Efficient Task Scheduling algorithm (MEETS) algorithm for homogeneous fog networks. The authors formulated the optimization problem as a multi-nodes programming. Then, they presented the MEETS algorithm with a low complexity to get an efficient solution for the energy consumption. Finally, they derived the joint time and the task modulation allocations to maximize the efficiency of the consumed energy of the fog networks. The performance evaluation shows that MEETS algorithm achieves a better energy efficiency. However, the proposed algorithm requires a lot of computation resources.

6.3. Other task scheduling techniques

Different efforts have been proposed to address the task scheduling issue in edge computing. Cardellini et al. [135] evaluated a distributed QoS aware scheduler for data stream processing, that is operating in a fog computing platform. The authors introduced different components: (a) the worker monitor component: is responsible for obtaining the outgoing and incoming data rate for each computing component (executor) that executes a set of tasks on the fog node. (b) the QoS monitor that estimates the QoS, and is responsible for obtaining availability, internode information and intra-node utilization. Then this information is forwarded to the distributed adaptive scheduler, and (c) the adaptive scheduler that runs a loop iteration periodically and verifies each candidate's task to be executed. This algorithm enhances the run-time adaptation capabilities in the system and improves the application performance. Nevertheless, some instability caused by complex fog topologies which decreases the data stream processing application's availability.

Verma et al. [136] proposed a Real-Time Efficient Scheduling and load balancing algorithm, namely RTES, for task scheduling and load balancing in a fog computing platform. The results of the evaluation performance show that the RTES algorithm achieves a short execution time and completes tasks before their deadline compared with other algorithms like the priority algorithm [137], FCFS algorithm [138], and Multi Objective Tasks scheduling algorithm [139]. However, the proposed approach did not take the energy consumption into consideration.

Ghanavati et al. [140] Proposed a task scheduling model to reduce both the energy consumption and the system makespan in a fog computing environment. The proposed system is composed of two components, first, a new optimization model called Ant Mating Optimization, and the second component is an optimized distribution of tasks. The numerical results show the efficiency of the proposed system. However, the application of the proposed approach in a dense network is complex.

Ali et al. [141] Proposed a task-scheduling model to minimize both total costs and makespans in a fog-cloud system. Then, a genetic algorithm is suggested to automatically allocate tasks and deal with the task-scheduling problem. The outcomes show that the proposed approach can achieve dynamic task scheduling by minimizing both cost and execution time. However, the possibility of application of the proposed approach in dense networks is an open issue.

Various and efficient scheduling mechanisms have been proposed for edge computing that aim to guarantee a short time for task processing and efficient resource allocation. Therefore, the key problem is the decision on where the submitted tasks can be scheduled in an efficient way which is offered by different proposed task scheduling techniques as shown in this section. Besides, the future can be more prosperous for task scheduling issues at the network edge that becoming an important challenge for future networks.

Table 4 outlines the technical comparison for task scheduling efforts.

7. SDN/NFV based edge computing

The concept of SDN [142] and NFV [143] has emerged as a popular mechanism for management and virtualization of network services and functions through an abstraction of functionality on a large cluster of devices in the network. The concept of SDN/NFV can be applied to edge computing at a more abstract level by allowing a centralized control, storage of network resources in the edge infrastructure.

Truong et al. [144] proposed an architecture called FSDN by merging fog computing and SDN technology in a vanet network. The FSDN VANET architecture is composed of the following components: SDN controller which is the main intelligence responsible for the control of all the network. It also works as a fog orchestration for the fog layer, SDN wireless nodes that represent the data plane elements, SDN road-side-unit which is a fog device, SDN road-side-unit controller which is a cluster of RSUs controlled by the SDN controller and is responsible for the forwarding of data and storing local road system information, and a cellular base station which is controlled by the SDN controller and is responsible for conveying data and carrying voice calls as well as a local intelligence and a fog device. The authors claimed that the proposed architecture optimizes the resources utility and reduces latency. However, this work did not present any experimental results or theoretical formulation to validate its architecture.

Huang et al. [145] proposed an SDN-based QoS provisioning mechanism for fog computing advanced WSNs, which realizes a dynamic QoS configuration. The fog nodes receive data sent from sensors then leave the QoS provisioning and process the data content to the SDN controller. The performance evaluation results show that the proposed mechanism achieves a great performance by improving latency. Nevertheless, this work did not describe the effectiveness of the mechanism in large-scale networks.

Liang et al. [146] proposed an architecture called software defined and virtualized RANs (SDVRANs) with fog computing. The SDN is used to split up the control plane and the data plane. Furthermore, the network virtualization allows to share network resources to diverse applications. Moreover, The authors presented an example of SaaS named *OpenPipe*, they also used a hybrid control model in order to support the fog computing in SDN. The effectiveness of the proposed network architecture based on a lab demo show that this architecture can fulfill a better performance in terms of low overheads, low latency, and less energy consumption. However, this work did not provide explanations of the use of this technology in the future virtualized networks.

Tomovic et al. [147] proposed an architecture for IoT which combines fog computing and SDN. The fog computing platform resolves the problem of latency, while SDN allows sophisticated mechanisms for resource management and traffic control by a centralized control plane. The proposed IoT architecture allows a high level of scalability and low latency. However, this work does not present any theoretical or experimental results to validate its architecture.

Vilalta et al. [148] Proposed an architecture for remotely controlled cars using fog computing and SDN/NFV technologies. the remote control process is running as a service application on fog nodes located close to RSUs. Moreover, a fog architecture is proposed to enable the connected cars to cooperate with each other. The proposed solution achieved good results in terms of delay. However, the car's mobility is not considered in this work.

Kiran et al. [149] Proposed a distributed NFV-enabled mobile edge computing (MEC) solution for VNF placement by assigning computing resources to incoming VNFs to satisfy the requests of users in the network. For this, an SDN-NFV infrastructure is proposed to resolve the resource allocation and VNF placement problem in the MEC networks. Moreover, a genetic algorithm is used to find approximate solutions. The obtained results show that the proposed solution is efficient in terms of the overall cost.

The SDN paradigm based on fog computing can solve some important issues, such as irregular connectivity. Furthermore, the NFV decouples the network function by abstraction and virtualization technologies which can notably improve the telecommunication service provisioning flexibility.

Table 5 display the technical comparison for SDN/NFV assisted EC efforts

8. Security & privacy in edge computing

Edge computing uses a wide range of communication technologies including mobile data acquisition, peer-to-peer networking, WSNs, mobile signature analysis and so on. It is necessary to apply advanced security mechanisms, such as cryptography techniques to secure edge computing, it may be at the system design level or network architecture level.

Table 4
Technical comparison for task scheduling in EC efforts.

Research direction	Work	Application scenario	Edge computing system	Edge nodes	End devices
Task scheduling	[114]	Tasks scheduling	Cloud-fog	Network devices	IoT
	[117]	e-Health	HealthEdge	Edge workstations	IoT
	[118]	Tasks scheduling	Client-fog-cloud	Micro datacenters	IoT
	[119]	Tasks scheduling	Fog-enabled IoT	Network devices	IoT
	[120]	Tasks scheduling	Fog-based Region and Cloud	High-end servers	Mobile devices
	[121]	Tasks scheduling	Fog-cloud cooperation	Network devices	IoT
	[123]	Tasks scheduling	Tiered IoT system	Cloudlet	IoT
	[124]	Tasks scheduling	Fog-enable jobs scheduling	Network devices	IoT
	[113]	Tasks scheduling	Scheduling-in-fog	Network devices	Mobile devices
	[129]	Smart factory	Flexible smart factory scheduling in fog	Network devices	IoT
	[131]	Tasks scheduling	Fog-supported embedded system	Network devices	End-user devices
	[133]	Tasks scheduling	Edge-IoT for task scheduling	Network devices	IoT
	[134]	Tasks scheduling	Homogeneous fog network	User devices	IoT
	[135]	Tasks scheduling	Data stream application in fog	Worker nodes	Distributed sources
	[136]	Tasks scheduling	Efficient scheduling in fog computing	Servers	IoT
	[140]	Tasks scheduling	Fog-enabled tasks scheduling for IoT	Network devices	IoT
	[141]	Tasks scheduling	Fog-cloud for scheduling	Servers	Connected devices

Table 5
Technical comparison for SDN/NFV in EC efforts.

Research direction	Work	Application scenario	Edge computing system	Edge nodes	End devices
SDN/NFV	[144]	Vanet	Fog-SDN for Vanet	Network devices	Vehicles
	[145]	Fog QoS policy for data content	Fog-SDN for QoS Provisioning	Micro data center	Wireless sensor networks
	[146]	vRAN	SDN-Fog for vRAN	Network devices	Connected devices
	[147]	- Transportation - Surveillance - Agriculture	SDN-Fog for IoT	Network devices	IoT
	[148]	Remote vehicle control	SDN/NFV-Fog for V2X	Network devices	Vehicles
	[149]	VNF management	Distributed SDN/NFV-enabled MEC	Network devices	Connected devices

8.1. Security efforts

Al Hamid et al. [150] proposed a security model to maintain the privacy of medical data in fog environment based healthcare systems. The authors used a one-round authenticated key protocol based on bilinear pairing cryptography which allows a session key to be generated between participants and data to be exchanged between them securely. The model ensures the security of private data by allowing participants to communicate between themselves securely. However, the key produced by the proposed protocol is static, which may have other security issues.

Similarly, Abdul et al. [151] presented a security mechanism to face images using zero watermarking and visual cryptography in the edge environment. The advantage of this mechanism is the copyright protection and authentication of different multimedia content. Although this work is practical, it did not describe how the proposed mechanism could secure the system against different attacks.

Mukherjee et al. [152] proposed an end-to-end middleware for IoT security in a cloud-fog environment. The proposed middleware is composed of two main components: a flexible security module that allows users to configure the required higher security and an intermittent security module to allow users to reuse an encrypted session from the recent past. The obtained results show that the proposed middleware can guarantee the security in the communications. However, some attacks can affect the security such as Distributed Denial of Service (DDoS) and man in the middle (MITM).

Diro et al. [153] proposed a fog computing based publish–subscribe lightweight protocol based on Elliptic Curve Cryptography (ECC) that has four security requirements: scalability, integrity/confidentiality, authentication and performance. The proposed security scheme provides lower resource usage and shorter key lengths. In addition, it provides lower overheads and better scalability compared to RSA. However, the proposed scheme has some issues, such as the choice of a suitable curve.

Huang et al. [154] proposed a secure data access control scheme with computation outsourcing and cipher text update in the fog computing environment. All the sensitive data for the owner is encrypted, then outsourced to the cloud for storage. Only the user that has the attributes that satisfy the access policy can directly decrypt the ciphertext. Similarly, only the user that has the attributes that satisfy the update policy can renew the stocked ciphertext. Although The results of experiments' illustrate that the proposed scheme can achieve data access control and secure cipher text, the proposed scheme does not support the efficiency in data search.

Hu et al. [155] proposed security and privacy mechanisms in face resolution and identification framework based on fog computing. They designed a data integrity/encryption scheme and an authentication scheme to meet the demands of integrity, availability and confidentiality in the face identification and resolution processes. The performance evaluation results prove that the proposed scheme guarantees the security of the system and the preservation of privacy. However, the proposed scheme requires a large amount of computation resources.

Cui et al. [156] proposed an edge-computing concept for message authentication in vanet networks. The proposed solution resolves different issues, such as the failure to search for invalid messages, redundant authentication by centralizing all the authentication tasks of vehicles on RSUs and the Edge Computing Vehicles (ECVs). The performance evaluation shows that the proposed scheme can rapidly identify valid and invalid messages when attacks are carried out. However, a MITM attack can affect the proposed scheme.

He et al. [157] proposed a data security storage model for fog computing, namely FCDSSM. They included in their architecture a control layer (top layer), authentication service layer (medium layer) and a data storage layer at the bottom. This model permits the integration of data storage and security mechanism to be achieved in large-scale IoT applications. The numerical results prove that the FCDSSM model has a better scalability and it can be adapted to the security of big data in large-scale IoT applications. However, the proposed model did not protect the system against data-clone attacks that can affect the storage system by the duplication of data, which can use up a massive amount of storage capacity.

He et al. [158] proposed a method to detect GPS spoofing attacks using a combination of visual sensors and Inertial Measurement Units (IMU) of unmanned aerial vehicles (UAVs) [159]. The method is demonstrated using drones. The obtained results prove the efficiency of the proposed method in terms of detected GPS spoofing. Nevertheless, there is a risk of MITM attack.

Alharbi et al. [160] proposed a fog-based security system namely FOCUS that aims to protect the IoT against a dangerous attacks named malware cyber-attacks. The FOCUS system uses a Virtual Private Network (VPN) to secure the communication channel from the IoT devices. Also, FOCUS protects the VPN server against DDoS attacks by adopting a challenge-response authentication, which can enhance the security of the IoT system. The results of experiments' validate the efficiency of the FOCUS system which can effectively filter out the different malicious attacks with small network bandwidth consumption and low response time. However, this work needs to be verified in a real fog computing framework.

Ni et al. [161] proposed a fog-assisted mobile crowd-sensing (Fo-MCS) framework that tends to improve the precision of task allocation with the help of fog nodes. Moreover, they proposed a fog-assisted secure data deduplication scheme, namely Fo-SDD, in order to reduce the overhead and allow the fog nodes to detect and remove the replicate data in sensing reports and which provides a high level of security against duplicate-replay attacks and brute force attacks. Nevertheless, this work requires some security mechanisms against Denial-of-Service and MITM attacks.

Zhang et al. [162] Proposed an architecture to improve the edge computing security by virtualizing the edge nodes. First, an edge node partition strategy is proposed to virtualize the edge network. Second, a security mechanism is proposed to measure the edge nodes security level. And finally, a mapping algorithm is modeled for data transmission. The outcome prove the efficiency of the proposed architecture that maintain the security of the edge.

Razaque et al. [163] Proposed a reliable and efficient framework for critical security issue in edge computing environment. The proposed framework consists of a module to detect the interaction between the edge and the end-user, and a model for validation integrated with the proposed framework that is more safer than key-based cryptographic solutions. The outcome validate the efficiency of the proposed framework.

8.2. Privacy efforts

Wang et al. [164] proposed a privacy-preserving scheme with differential privacy levels in the fog computing environment, called privacy-preserving content-based subscribe/publish scheme (PCP) with differential privacy in fog environment, which can efficiently achieve a protection against collusion attacks. However, the authors did not provide a deficiency in the real scenario in terms of reducing the availability of the aggregated data streams.

Okay et al. [165] proposed an additive privacy based Secure Data Aggregation scheme for Fog Computing based Smart Grids (FCSG) which ensures data privacy based on homomorphic encryption [166]. This encryption scheme enables users to perform a different operations on encrypted data without affecting the privacy of the data. The performance results show that the proposed scheme ensures low communication and storage, as well as ensuring end-to-end confidentiality and guaranteeing the privacy of collected data. However, the proposed scheme requires the system to be protected against some dangerous attacks, like MITM.

Wang et al. [167] proposed a high-level privacy protection mechanism for the Internet of medical things (IoMT) in the fog computing environment, called Fog-based Access Control Model (FACM), which deploys an access control layer at the fog server. The proposed solution offers a high-level privacy protection with a short execution time. However, the algorithm used requires high computational resources.

Fan et al. [168] Proposed an efficient privacy scheme for fog-enabled IoT where all users attribute transformed to be authenticable and anonymous to achieve privacy-preserving. To reduce computation overhead, the outsourced decryption is introduced. As well, a method for user revocation is proposed. The outcome proves the scheme's efficiency.

Gu et al. [169] Proposed a dynamic privacy-preserving scheme based on Markov decision in an edge computing environment to get the optimized trade-off between data utility and privacy protection. A game model is established between adversaries and users, then a reinforcement learning model is used. The outcomes demonstrate the feasibility and the efficiency of the proposed solution.

Qu et al. [170] Proposed FL-Block, federated learning with blockchain scheme that enables local learning updates of different exchanges between end devices and the global model for learning in blockchain verified by miners. FL-Block allows self machine learning without interactions with any authority. The outcomes prove the performance of the proposed FL-Block in terms of privacy protection and resistance against poisoning attacks.

In a nutshell, the security and privacy aspects in edge computing is an important element that must be developed in a critical way, to ensure the security against malicious and dangerous nodes/attacks that threaten the fog system functionalities and the privacy of data and end-users.

Table 6 show the technical comparison for security & privacy in EC efforts

9. Blockchain in edge computing

The Blockchain [171] is a technique for information transmission and storage without control organs. Technically, it is a distributed database, its information sent by the users and the internal links to the database are checked then grouped in blocks at uniform time intervals, the whole being secured by cryptography and consequently forming a chain. By extension, a Blockchain maintains a list of records protected from modification or falsification by storage nodes, so it is a distributed, secure registry of all transactions made since the startup of the distributed system.

The Blockchain was initially designed for the cryptocurrencies such as Bitcoin [172] and it is used for several sectors like intelligent transportation, agriculture and the Internet of energy. Moreover, the IoT can be combined with the Blockchain technology [173] in several domains such as healthcare, SDN and Smart Electric Vehicles, which allow the IoT to benefit from the decentralized resource management, lower operational cost, robustness against attacks and threats and so on. Moreover, the Blockchain can be used with the edge computing [174] in order to facilitate communications between the edge nodes and the IoT devices which enhance the efficiency of the edge computing based IoT networks.

Jiao et al. [175], proposed an edge computing model in a mobile Blockchain network. Where the mining process of miners is offloaded to the edge computing service provider (ECSP). Moreover, a combinatorial auction-based pricing approach is used for the allocation of edge resources to the miners. The proposed model maximizes the social welfare

Table 6
Technical comparison for security & privacy in EC efforts.

Research direction	Work	Application scenario	Edge computing system	Edge nodes	End devices
Security & Privacy	[150]	Healthcare	Fog with pairing-based cryptography	Network devices	Connected devices
	[151]	Face recognition	Edge-biometric	Network devices	IoT
	[152]	End-to-end IoT security	Edge middleware for IoT security	Network devices	IoT
	[153]	Cybersecurity	IoT/Fog publish–subscribe model	Network devices	IoT
	[154]	Secure data access control for IoT	Fog-IoT for data security	Network devices	IoT
	[155]	Face identification	Fog-IoT for security and privacy preservation	Network devices	Connected devices
	[156]	Vanet	Message-Authentication in vehicular edge computing	Vehicles (server)	Vehicles (clients)
	[157]	University campus data storage security	Fog enabled IoT data storage security	PCs	IoT
	[158]	Drones flight safety	Airborne fog computing systems	UAV	UAV
	[160]	DDoS attack	Fog security system for IoT	PC (VPN server)	IoT
	[161]	Secure data deduplication	Fog-assisted mobile crowdsensing	Servers	IoT
	[162]	Edge nodes virtualization	Edge-IoT security tactic	Network devices	IoT
	[163]	Identify criminal activities	Industrial edge security	Framework	Connected devices
	[164]	Content privacy	Edge privacy-preserving	Network devices	Connected devices
	[165]	Smart home	Fog-based smart grids	Servers	IoT
	[167]	Internet of medical things	Fog-based access control	Servers	IoT
	[168]	Privacy-preserving	Fog-enabled IoT	Proxy servers	IoT
	[169]	Privacy protection and data utility	Hierarchical edge computing	Network devices	Connected devices
	[170]	Blockchain	Fog-enabled decentralized privacy	Servers	Connected devices

and also guarantees the incentive compatibility (IC). Nevertheless, the ECSP revenue has not considered.

Luong et al. [176], developed an optimal auction based on the deep learning [177] for resource allocation in the edge computing environment based mobile Blockchain networks, they constructed a multi-layer neural network architecture that first performs some transformations of the miners' bids, then calculates the allocation and the conditional payment rules. They designed the neural networks data training by using the miners' valuations, then using the training data, they trained the neural networks by tuning parameters to enhance the revenue of the ECSP. The obtained results showed that the proposed scheme achieved a higher revenue of the ECSP compared to the baseline scheme. However, only one unit of resource is considered in the auction.

Xiong et al. [178] considered the edge computing as a resource management for mobile Blockchain applications where the mining process can be offloaded to the ECSP because the mining process requires the proof-of-work puzzle to be solved, which needs large computation resources which are not adopted in the mobile applications [179]. They analyzed two pricing schemes for miners, a uniform pricing and discriminatory pricing, then they formulated a Stackelberg model to study the maximization of the ECSP revenue and the benefit of miners. The performance evaluation showed that the ECSP achieved the maximum revenue under the uniform pricing, moreover, the discriminatory pricing helps the ESP to achieve a greater profit by encouraging a higher demand of service from miners. However, this work only addressed the revenues of the ESP, it requires other quality of service (QoS) metrics.

Casado et al. [180], proposed a Blockchain-based architecture with a view to improve the data security, it consists of the following layers: an IoT layer, a Blockchain layer and an edge computing layer. Moreover, they proposed a self-organized and distributed algorithm based on the game theory executed in the edge computing layer where it is applied on the data collected by the IoT devices whose objective is to improve the false data detection and the data quality. However, the complexity of the algorithm is missing from this work.

Zhang et al. [181] Proposed an efficient and reliable system based on blockchain and edge computing. First, a group-agent strategy is designed to improve transmission efficiency and guarantee the reliability of edge devices. Second, a sorting and ranking mechanism is introduced to improve resource allocation. Third, a new model to predict the popularity of the keywords and encrypt data. The outcomes prove the efficiency and the reliability of the proposed approach.

Abdellatif et al. [182] Proposed MEdge-Chain, a medical-edge-blockchain framework that integrates blockchain with edge computing to process medical data. the proposed framework aims to secure storage, exchange of medical data, and aggregate many health entities in a unique healthcare system. Moreover, a patient monitoring scheme is designed to enable efficient discovery and remote monitoring of critical medical events. Then the blockchain is used to secure and optimize the exchange of medical data. The results demonstrate the efficiency of the proposed work.

Table 7 display the technical comparison for EC-blockchain efforts.

The integration of Blockchain with IoT and the edge computing offers many benefits for the future applications in the Internet, such as data security, efficient energy consumption and of course efficient services. Moreover, the Blockchain guarantees the security of the interactions in the system and the users' privacy, in addition the edge computing provides a distributed computing model for the connected devices to execute their tasks, also it offers a rapid and efficient processing and computing services to the Blockchain such as the mining process.

Table 8 outlines the improved criteria of each research.

Table 7
Technical comparison for blockchain in EC efforts.

Research direction	Work	Application scenario	Edge computing system	Edge nodes	End devices
Blockchain	[175]	Mobile blockchain	Edge for mobile blockchain	Servers	Mobile devices
	[176]	Computing services	Edge resource allocation	Servers	Mobile devices
	[178]	Resource management	Edge-based optimal pricing	Servers	Mobile devices
	[180]	Data Security	Edge-blockchain for data quality	Network devices	IoT
	[181]	Resource allocation	Edge-assisted blockchain	Network devices	Connected devices
	[182]	e-Health	Medical-Edge-Blockchain	Servers	IoT

Table 8
Improved criteria of each research.

Ref.	QoS enhanced metric							Security Concerns	
	Energy	Latency	Delay	Bandwidth	Memory	CPU	Cost	Security	Privacy
[124,129,133,134,140,146]	✓	✗	✗	✗	✗	✗	✗	—	—
[118–120,135,144–147]	✗	✓	✗	✗	✗	✗	✗	—	—
[117,119]	✗	✗	✗	✓	✗	✗	✗	—	—
[113]	✗	✗	✗	✗	✓	✗	✗	—	—
[148]	✗	✗	✓	✗	✗	✗	✗	—	—
[113,114,117,121,123,124,131,136]	✗	✗	✗	✗	✗	✓	✗	—	—
[140,141,149,176,178,181,182]	✗	✗	✗	✗	✗	✗	✓	—	—
[150,154,155,157,161–163,180–182]	✗	✗	✗	✗	✗	✗	✗	Data Sec.	—
[151,155,156]	✗	✗	✗	✗	✗	✗	✗	Authentication	—
[152,153,163]	✗	✗	✗	✗	✗	✗	✗	Network Sec.	—
[164]	✗	✗	✗	✗	✗	✗	✗	—	Collusion Att.
[158]	✗	✗	✗	✗	✗	✗	✗	Spoofing Att.	—
[160]	✗	✗	✗	✗	✗	✗	✗	Malware & DDoS	—
[165,168–170]	✗	✗	✗	✗	✗	✗	✗	—	Data
[167,168]	✗	✗	✗	✗	✗	✗	✗	—	User

10. Future research guidelines & directions

Although the aforementioned advantages and existing solutions, various issues and challenges need to be studied for a full integration of edge and fog computing on top of IoT applications. In the following, we discuss the major challenges, highlight new ideas and guidelines that need to be addressed seriously by the research community.

10.1. Scalability

Scalability is an indispensable factor for any network architecture in which the system must manage a wide number of demands, requests and services regardless of the growing number of clients, e.g. mobile devices in the edge network. Recently, the number of different connected things has increased rapidly, in which it may interrupt services and their quality and creates bottlenecks in the network caused by the enormous quantity of data generated by the connected things [6]. For this reason the edge servers should guarantee the scalability of the service in the fog layer by applying some mechanisms such as server clusters and load balancing.

10.2. Service availability

The availability is an indispensable factor in network architectures where the system must guarantee the service anytime and from anywhere without degradation or interruption which is considered the important issue for real-time applications such as video streaming that require a short time for processing and response especially in vehicular edge computing where many factors can affect the service availability such as vehicles mobility, and obstacles, etc. For this, the efficient service availability needs to be assured for the current and next generation of applications in edge computing by applying some mechanisms, including system backups, prediction, and monitoring.

10.3. High mobility support

Mobility is a very important aspect in the IoT due to the fact that most of the connected things, such as mobile devices, vehicles, and drones are highly mobile, which is a reason for frequent link failure among devices and servers. This problem leads to a decrease in the QoS and the security of the fog system, the high mobility device support is a very important issue that needs to be addressed in future generations of networks [183,184]. For this reason, it is necessary to propose some algorithms, such as the prediction of link failures to ensure the path stability, detection of obstacles, etc.

10.4. Energy management

The fog computing architecture consists of different distributed systems, therefore the energy consumption is expected to be high, which increase the costs. Thus, a lot of works need to address this issue by optimizing and developing a new effective energy protocol in the fog computing systems, specifically in the virtual and the Adhoc fog systems, such as network and computing resource optimization, reliance on environmentally friendly energies (renewable energy) and so on [185]. And on the other hand, at the end users' level, and because the devices use batteries which is limited energy savings, this will cause some problems, such as the disconnection of devices during the upload/download of data in/from fog devices. Therefore, it is a big challenge to provide solutions for this problem, such as providing sources for charging devices in the streets, reliance on friction (movement of cars and people) as a power source for devices.

10.5. Security & privacy

The security issue is one of the most important problems that needs to be studied carefully in edge & fog computing networks. For this there are different mechanisms such as cryptography, hash functions, etc. It is necessary to be used to guarantee the security of communications in the IoT network with fog computing environment.

The privacy leakage of end users' information in the IoT networks, like location, usage, and data, is attracting the attention of unauthorized users to threaten the privacy of end-users, such as location privacy issue because most IoT devices are location-based, this allows the adversary to change the location of end-users, which will affect the decision of fog servers that are based on the end users' location. Moreover, data privacy-preserving is a critical issue especially in the new generation of networks based on edge computing technology where a huge amount of data is exchanged between communication nodes which can be exploited by unauthorized systems or users. For this, important challenges need to be addressed in future works to resolve serious privacy issues by ensuring security against MITM attacks and use the infrastructure of public key for data block encryption. Techniques such as homomorphic encryption for data aggregation can provide data privacy without decryption, while pseudo-random permutation [186] and Probabilistic public-key encryption [187] can be used to preserve data privacy in lightweight methods.

10.5.1. Authentication

Authentication is essential in the security of IoT devices. Regrettably, the IoT devices do not have enough capacity such as CPU and memory to execute the cryptographic operations used for authentication. The IoT devices can use an outsourced storage and computations capacity in the fog devices to execute the authentication protocol. Therefore, the fog server will be considered as an authentication server of the IoT devices.

10.5.2. Data protection

The huge volume of data generated by IoT devices must be protected at the communication level and at the processing level at the network edge or the cloud. The risk of data replication/sharing attack, data altering attacks, data loss at the edge or cloud level needs to be resolved to ensure data integrity by the encryption mechanisms, backup and recovery of data, policy enforcement, and network monitoring.

10.5.3. Preventing cache attacks

The edge servers cache the contents sent from mobile devices and then forward to the cloud the cached data for storage. The cached data can be threatened by some malicious programs that can change or erase the data content. For this, the security of data caching in fog computing is an important issue. Moreover, as a future challenge the data cached in fog servers need to be protected by several mechanisms, such as hash functions, cryptography and also ensure the data recovery and backup.

10.6. Artificial intelligence (AI) assisted EC (Edge-AI)

Machine learning is a promising approach and an important methodology to resolve different problems, it helps the IoT in many fields [188] such as smart cities, smart homes, also in smart healthcare systems, and it can also used in game programming such as puzzles and video games.

The machine learning is structured in three categories: *Supervised learning* where the training set consists of input vectors (samples) together with their labels also known as corresponding appropriate target vectors, *Unsupervised learning* where for the training set no labels are required, and finally, *Reinforcement learning*, that deals with learning appropriate actions problems, in order to maximize the payoff, furthermore, the multi-agent reinforcement learning (MADRL)[2,3] is a learning paradigm to control a system with a view to maximizing an objective over the long term. Thus, the Multi-Agent Systems interacting in mixed competitive and cooperative environments, it can be used in a variety of domains like economics, robotics, games, etc.

Different works have been proposed for machine learning and deep learning in Edge-IoT environment [189], where the machine learning provide a great number of services to the network edge to enhance the efficiency of the edge services.

The edge AI applications and activities are developing rapidly. Note that it is important to develop software and hardware to achieve efficient service by the application of edge AI. For this, there are still important challenges and future directions to integrate efficiently the edge computing with AI as listed below:

Power and processing resource utilization: AI models consist of two main parts, training and inferencing. In edge computing, both two parts can be executed at the edge layer near to IoT devices which puts more demand on the edge node's processing requirements, especially for the training part. This increases the energy consumption in the edge layer that poses a big problem, requiring a rebalancing of power requirements versus processing capacity. Therefore, the open challenge for tech companies is to develop new generation of hardware that has high computing resources and low energy consumption with advanced softwares that performs learning more efficiently to make a robust computing ecosystem.

The second challenges is the storage and the security of data especially the AI algorithms are based-training models that use a huge amount of data for training which create a critical issue for edge layer that need to offer large size storage for only AI models. Moreover, the security of data (models and datasets) pose an important challenge where any security issue can cause damage during models training by modifying the data or models parameters. For this, the research community need to focus more on proposing efficient solutions to create balance between data storage and data security for AI which can enhance the Edge-AI services.

10.7. Simulation platform

Simulation is a process of modeling a real scenario using a mathematical formula and implementing it using programming language. The advantage of using simulation is because it helps us to understand the system and apply experiments at a cheap cost. The experiments and testing in real edge computing infrastructure require a lot of resources (finance and effort) which-can not be possible for all researchers. Instead of that, developing a simulation platform for edge computing will encourage researchers to implements their new ideas. For this, the future simulation platforms must support the high mobility of end users and fog servers, also ensure task migration and provide a model of energy consumption for end users and fog servers. In addition a visual tool and detailed guide for using the simulator.

Table 9 Outlines the summary of EC challenges and future directions.

11. Learned lessons & conclusion

11.1. Learned lessons

In this part, we present the learned lessons for EC-IoT. In particular, we focus on the necessary transition from cloud to edge by moving a part of processing from the central cloud to the edge of the network, then, the important evolution of EC-IoT applications and the need for more computing resources. Moreover, we discuss the security importance for EC.

[2] DeepMind: https://deepmind.com/.
[3] OpenIA: https://openai.com/.

Table 9
EC challenges & future direction.

Topic	Challenges	Future Directions
Scalability	High network traffic High number of users	• Load balancing • Auto scaling
Availability	System availability Network availability Service availability	• Standby replica for the system • Increase the number of edge locations • Increase the number of regional edge caches
High mobility support	Devices mobility management Servers mobility management	• Artificial intelligence
Energy management	Devices energy consumption Servers energy consumption	• Artificial intelligence
Security & Privacy	Authentication Data protection Preventing cache attacks	• Efficient encryption models • Data backup and recovery • Network monitoring
Edge-AI	Processing resource Power resource Data Storage Data Security	• Big data management • Data archiving • AI services • Dedicated computing resources
Simulation Platform	Devices energy consumption Different mobility models support Services simulation In/out data from/to other platforms	• Cellular networks support • High mobility support • Efficient energy management models • AI models support

11.1.1. From cloud to edge

The CC is considered the key to provide the required resources of IoT applications. However, it suffers from latency problems, especially with real-time applications, such as online gaming and video streaming. For this, the EC architecture is proposed to resolves the latency issue in CC and provides efficient services near to IoT devices. Effective edge layer integration between IoT devices and the cloud needs further study by the research community to ensure a balance between service efficiency and cost.

11.1.2. Edge use cases & applications

EC is a typical solution that supports the ultra-low latency and bandwidth consumption requirements of IoT applications. EC resources can be used to provide network scalability, massive data pre-processing, and ensure short response time to user requests. However, to maximize the benefits of EC for IoT, it is important to achieve an in-depth research related to computing resources and data storage at the network edge especially for next-generation of IoT applications.

11.1.3. Security importance

It is important to realize that the EC system will be controlled by a different service providers or owners. Thus, it is sure that all EC relevant assets such as the virtualization infrastructure, the service infrastructure, the user devices, and the network infrastructure will be controlled by different entities because of the diversity of IoT applications that accesses to EC services at any time from anywhere. Conversely, the "from anywhere" principle can cause attacks from anywhere which makes the EC model a double-edged sword. For this, the need for robust security measures is growing to cover the global networking exchange, especially for the EC-IoT system.

11.2. Conclusion

With the huge development of IoT networks, edge computing is becoming a solution to the complex challenges and difficulties of managing connected devices/sensors, and the huge computing resources that they use. Compared to the cloud computing technology, the edge computing will offer a large data computation and storage at the network edge which is required by future applications, such as smart homes, smart cities, smart vehicles and so on. This manuscript presents a survey on edge computing for IoT, with recent research activities like task scheduling, SDN/NFV, security and privacy and the Blockchain. In addition, the future applications and use cases are detailed, furthermore we identify the open research challenges and highlight future research directions, and learned lessons.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] P.K. Senyo, E. Addae, R. Boateng, Cloud computing research: A review of research themes, frameworks, methods and future research directions, Int. J. Inf. Manage. (IJIM) 38 (1) (2018) 128–139, http://dx.doi.org/10.1016/j.ijinfomgt.2017.07.007.

[2] J. Pan, J. McElhannon, Future edge cloud and edge computing for internet of things applications, IEEE Internet Things J. (IoT-J) 5 (1) (2018) 439–449, http://dx.doi.org/10.1109/JIOT.2017.2767608.

[3] S. Yi, C. Li, Q. Li, A survey of fog computing: concepts, applications and issues, in: Workshop on Mobile Big Data, ACM, 2015, pp. 37–42, http://dx.doi.org/10.1145/2757384.2757397.

[4] M. Chiang, T. Zhang, Fog and IoT: An overview of research opportunities, IEEE Internet Things J. (IoT-J) 3 (6) (2016) 854–864, http://dx.doi.org/10.1109/JIOT.2016.2584538.

[5] W. Shi, J. Cao, Q. Zhang, Y. Li, L. Xu, Edge computing: Vision and challenges, IEEE Internet Things J. (IoT-J) 3 (5) (2016) 637–646, http://dx.doi.org/10.1109/JIOT.2016.2579198.

[6] C. Mouradian, D. Naboulsi, S. Yangui, R.H. Glitho, M.J. Morrow, P.A. Polakos, A comprehensive survey on fog computing: State-of-the-art and research challenges, IEEE Commun. Surveys Tutorials (COMST) 20 (1) (2017) 416–464, http://dx.doi.org/10.1109/COMST.2017.2771153.

[7] P. Hu, S. Dhelim, H. Ning, T. Qiu, Survey on fog computing: architecture, key technologies, applications and open issues, J. Netw. Comput. Appl. 98 (2017) 27–42, http://dx.doi.org/10.1016/j.jnca.2017.09.002.

[8] J. Ni, K. Zhang, X. Lin, X.S. Shen, Securing fog computing for internet of things applications: Challenges and solutions, IEEE Commun. Surveys Tutorials (COMST) 20 (1) (2017) 601–628, http://dx.doi.org/10.1109/COMST.2017.2762345.

[9] A.C. Baktir, A. Ozgovde, C. Ersoy, How can edge computing benefit from software-defined networking: a survey, use cases, and future directions, IEEE Commun. Surveys Tutorials (COMST) 19 (4) (2017) 2359–2391, http://dx.doi.org/10.1109/COMST.2017.2717482.

[10] M. Mukherjee, L. Shu, D. Wang, Survey of fog computing: Fundamental, network applications, and research challenges, IEEE Commun. Surveys Tutorials (COMST) (2018) http://dx.doi.org/10.1109/COMST.2018.2814571.

[11] W. Yu, F. Liang, X. He, W.G. Hatcher, C. Lu, J. Lin, X. Yang, A survey on the edge computing for the internet of things, IEEE Access 6 (2018) 6900–6919, http://dx.doi.org/10.1109/ACCESS.2017.2778504.

[12] R. Mahmud, R. Kotagiri, R. Buyya, Fog computing: A taxonomy, survey and future directions, in: Internet of Everything, Springer, 2018, pp. 103–130, http://dx.doi.org/10.1007/978-981-10-5861-5_5.

[13] B. Omoniwa, R. Hussain, M.A. Javed, S.H. Bouk, S.A. Malik, Fog/Edge Computing-based IoT (fecIoT): Architecture, applications, and research issues, IEEE Internet Things J. (IoT-J) (2018) http://dx.doi.org/10.1109/JIOT.2018.2875544.

[14] R.K. Naha, S. Garg, D. Georgakopoulos, P.P. Jayaraman, L. Gao, Y. Xiang, R. Ranjan, Fog computing: Survey of trends, architectures, requirements, and research directions, IEEE Access 6 (2018) 47980–48009, http://dx.doi.org/10.1109/ACCESS.2018.2866491.

[15] W.Z. Khan, E. Ahmed, S. Hakak, I. Yaqoob, A. Ahmed, Edge computing: A survey, Future Gener. Comput. Syst. (FGCS) 97 (2019) 219–235, http://dx.doi.org/10.1016/j.future.2019.02.050.

[16] C. Puliafito, E. Mingozzi, F. Longo, A. Puliafito, O. Rana, Fog computing for the internet of things: A survey, ACM Trans. Internet Technol. (TOIT) 19 (2) (2019) 1–41, http://dx.doi.org/10.1145/3301443.

[17] I. Martinez, A.S. Hafid, A. Jarray, Design, resource management and evaluation of fog computing systems: A survey, IEEE Internet Things J. (2020) http://dx.doi.org/10.1109/JIOT.2020.3022699.

[18] J. Dilley, B. Maggs, J. Parikh, H. Prokop, R. Sitaraman, B. Weihl, Globally distributed content delivery, IEEE Internet Comput. (IC) 6 (5) (2002) 50–58, http://dx.doi.org/10.1109/MIC.2002.1036038.

[19] S. Yangui, P. Ravindran, O. Bibani, R.H. Glitho, N.B. Hadj-Alouane, M.J. Morrow, P.A. Polakos, A platform as-a-service for hybrid cloud/fog environments, in: IEEE International Symposium on Local and Metropolitan Area Networks (LANMAN), 2016, pp. 1–7, http://dx.doi.org/10.1109/LANMAN.2016.7548853.

[20] B. Nour, K. Sharif, F. Li, S. Biswas, H. Moungla, M. Guizani, Y. Wang, A survey of Internet of Things Communication using ICN: A use case perspective, Comput. Commun. (ComCom) 142–143 (2019) 95–123, http://dx.doi.org/10.1016/j.comcom.2019.05.010.

[21] L. Zhang, D. Estrin, J. Burke, V. Jacobson, J.D. Thornton, D.K. Smetters, B. Zhang, G. Tsudik, D. Massey, C. Papadopoulos, et al., Named data networking (NDN) project, Relatório Técnico NDN-0001, Xerox Palo Alto Research Center-PARC 157 (2010) 158.

[22] H. Khelifi, S. Luo, B. Nour, H. Moungla, Y. Faheem, R. Hussain, A. Ksentini, Named data networking in vehicular Ad hoc networks: State-of-the-Art and challenges, IEEE Commun. Surv. Tutor. (2019) http://dx.doi.org/10.1109/COMST.2019.2894816.

[23] B. Nour, K. Sharif, F. Li, H. Moungla, Y. Liu, A unified hybrid information-centric naming scheme for IoT applications, Comput. Commun. 150 (2019) 103–114, http://dx.doi.org/10.1016/j.comcom.2019.11.020.

[24] D. Raychaudhuri, K. Nagaraja, A. Venkataramani, Mobilityfirst: a robust and trustworthy mobility-centric architecture for the future internet, ACM SIGMOBILE Mob. Comput. Commun. Rev. (MC2R) 16 (3) (2012) 2–13, http://dx.doi.org/10.1145/2412096.2412098.

[25] R.K. Chahal, N. Kumar, S. Batra, Trust management in social Internet of Things: A taxonomy, open issues, and challenges, Comput. Commun. (ComCom) (2019) http://dx.doi.org/10.1016/j.comcom.2019.10.034.

[26] E. Borgia, The Internet of Things vision: Key features, applications and open issues, Comput. Commun. (ComCom) 54 (2014) 1–31, http://dx.doi.org/10.1016/j.comcom.2014.09.008.

[27] J. Gubbi, R. Buyya, S. Marusic, M. Palaniswami, Internet of things (IoT): A vision, architectural elements, and future directions, Future Gener. Comput. Syst. (FGCS) 29 (7) (2013) 1645–1660, http://dx.doi.org/10.1016/j.future.2013.01.010.

[28] D.-H. Shih, P.-L. Sun, D.C. Yen, S.-M. Huang, Taxonomy and survey of RFID anti-collision protocols, Comput. Commun. (ComCom) 29 (11) (2006) 2150–2166, http://dx.doi.org/10.1016/j.comcom.2005.12.011.

[29] B. Sun, Y. Xiao, C.C. Li, H.-H. Chen, T.A. Yang, Security co-existence of wireless sensor networks and RFID for pervasive computing, Comput. Commun. (ComCom) 31 (18) (2008) 4294–4303, http://dx.doi.org/10.1016/j.comcom.2008.05.035.

[30] M.A. Mohandes, Mobile technology for socio-religious events: a case study of NFC technology, IEEE Technol. Soc. Mag. 34 (1) (2015) 73–79, http://dx.doi.org/10.1109/MTS.2015.2396122.

[31] H. Guo, Y. Zheng, X. Li, Z. Li, C. Xia, Self-healing group key distribution protocol in wireless sensor networks for secure IoT communications, Future Gener. Comput. Syst. (FGCS) 89 (2018) 713–721, http://dx.doi.org/10.1016/j.future.2018.07.009.

[32] S. Wan, Z. Gu, Q. Ni, Cognitive computing and wireless communications on the edge for healthcare service robots, Comput. Commun. (ComCom) (2019) http://dx.doi.org/10.1016/j.comcom.2019.10.012.

[33] H. Ning, Z. Wang, Future internet of things architecture: like mankind neural system or social organization framework? IEEE Commun. Lett. (COMML) 15 (4) (2011) 461–463, http://dx.doi.org/10.1109/LCOMM.2011.022411.110120.

[34] P. Mell, T. Grance, et al., The NIST definition of cloud computing, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology Gaithersburg, 2011.

[35] D. Zissis, D. Lekkas, Addressing cloud computing security issues, Future Gener. Comput. Syst. (FGCS) 28 (3) (2012) 583–592, http://dx.doi.org/10.1016/j.future.2010.12.006.

[36] S. Marston, Z. Li, S. Bandyopadhyay, J. Zhang, A. Ghalsasi, Cloud computing—The business perspective, Decision Support Systems (DSS) 51 (1) (2011) 176–189, http://dx.doi.org/10.1016/j.dss.2010.12.006.

[37] G. Mateescu, W. Gentzsch, C.J. Ribbens, Hybrid computing—where HPC meets grid and cloud computing, Future Gener. Comput. Syst. (FGCS) 27 (5) (2011) 440–453, http://dx.doi.org/10.1016/j.future.2010.11.003.

[38] M. Cusumano, Cloud computing and SaaS as new computing platforms, Commun. ACM (CACM) 53 (4) (2010) 27–29, http://dx.doi.org/10.1145/1721654.1721667.

[39] C. Pahl, Containerization and the PaaS cloud, IEEE Cloud Comput. 2 (3) (2015) 24–31, http://dx.doi.org/10.1109/MCC.2015.51.

[40] S. Bhardwaj, L. Jain, S. Jain, Cloud computing: A study of infrastructure as a service (IAAS), Int. J. Eng. Inf. Technol. (IJEIT) 2 (1) (2010) 60–63.

[41] E. Cavalcante, J. Pereira, M.P. Alves, P. Maia, R. Moura, T. Batista, F.C. Delicato, P.F. Pires, On the interplay of Internet of Things and cloud computing: A systematic mapping study, Comput. Commun. (ComCom) 89 (2016) 17–33, http://dx.doi.org/10.1016/j.comcom.2016.03.012.

[42] A. Botta, W. De Donato, V. Persico, A. Pescapé, Integration of cloud computing and Internet of Things: a survey, Future Gener. Comput. Syst. (FGCS) 56 (2016) 684–700, http://dx.doi.org/10.1016/j.future.2015.09.021.

[43] G. Neagu, Ş. Preda, A. Stanciu, V. Florian, A Cloud-IoT based sensing service for health monitoring, in: IEEE E-Health and Bioengineering Conference (EHB), 2017, pp. 53–56, http://dx.doi.org/10.1109/EHB.2017.7995359.

[44] L. Ismail, H. Materwala, Energy-aware VM placement and task scheduling in cloud-IoT computing: Classification and performance evaluation, IEEE Internet Things J. (IoT-J) (2018) http://dx.doi.org/10.1109/JIOT.2018.2865612.

[45] N. Almolhis, A.M. Alashjaee, S. Duraibi, F. Alqahtani, A.N. Moussa, The security issues in IoT-Cloud: A review, in: IEEE International Colloquium on Signal Processing & Its Applications (CSPA), 2020, pp. 191–196, http://dx.doi.org/10.1109/CSPA48992.2020.9068693.

[46] J. Pan, J. McElhannon, Future edge cloud and edge computing for internet of things applications, IEEE Internet Things J. (IoT-J) (2017) http://dx.doi.org/10.1109/JIOT.2017.2767608.

[47] B. Nour, S. Mastorakis, A. Mtibaa, Compute-less networking: Perspectives, challenges, and opportunities, IEEE Netw. (2020).

[48] M. Aazam, E.-N. Huh, Fog computing: The cloud-iot/ioe middleware paradigm, IEEE Potentials 35 (3) (2016) 40–44, http://dx.doi.org/10.1109/MPOT.2015.2456213.

[49] A.M. Goscinski, Z. Tari, I.A. Aziz, E.J. Alzahrani, Fog computing as a critical link between a central cloud and IoT in support of fast discovery of new hydrocarbon reservoirs, in: International Conference on Mobile Networks and Management (MONAMI), Springer, 2017, pp. 247–261, http://dx.doi.org/10.1007/978-3-319-90775-8_20.

[50] M. Chiang, S. Ha, I. Chih-Lin, F. Risso, T. Zhang, Clarifying fog computing and networking: 10 questions and answers, IEEE Commun. Mag. (COMMAG) 55 (4) (2017) 18–20, http://dx.doi.org/10.1109/MCOM.2017.7901470.

[51] Y. Pan, P. Thulasiraman, Y. Wang, Overview of Cloudlet, Fog Computing, Edge Computing, and Dew Computing, in: International Workshop on Dew Computing, 2018, pp. 20–23.

[52] M. Satyanarayanan, The emergence of edge computing, IEEE Comput. 50 (1) (2017) 30–39, http://dx.doi.org/10.1109/MC.2017.9.

[53] S. Yi, Z. Hao, Z. Qin, Q. Li, Fog computing: Platform and applications, in: IEEE Workshop on Hot Topics in Web Systems and Technologies (HotWeb), 2015, pp. 73–78, http://dx.doi.org/10.1109/HotWeb.2015.22.

[54] F. Bonomi, R. Milito, P. Natarajan, J. Zhu, Fog computing: A platform for internet of things and analytics, in: Big Data and Internet of Things: A Roadmap for Smart Environments, Springer, 2014, pp. 169–186.

[55] F. Bonomi, R. Milito, J. Zhu, S. Addepalli, Fog computing and its role in the internet of things, in: Mobile Cloud Computing (MCC) Workshop, ACM, 2012, pp. 13–16, http://dx.doi.org/10.1145/2342509.2342513.

[56] B. Negash, A.M. Rahmani, P. Liljeberg, A. Jantsch, Fog computing fundamentals in the Internet-of-Things, in: Fog Computing in the Internet of Things, Springer, 2018, pp. 3–13, http://dx.doi.org/10.1007/978-3-319-57639-8_1.

[57] M. Yannuzzi, F. van Lingen, A. Jain, O.L. Parellada, M.M. Flores, D. Carrera, J.L. Pérez, D. Montero, P. Chacin, A. Corsaro, et al., A new era for cities with fog computing, IEEE Internet Comput. (IC) 21 (2) (2017) 54–67, http://dx.doi.org/10.1109/MIC.2017.25.

[58] B. Tang, Z. Chen, G. Hefferman, T. Wei, H. He, Q. Yang, A hierarchical distributed fog computing architecture for big data analysis in smart cities, in: ASE BigData & SocialInformatics, ACM, 2015, p. 28, http://dx.doi.org/10.1145/2818869.2818898.

[59] W. Hou, Z. Ning, L. Guo, Green survivable collaborative edge computing in smart cities, IEEE Trans. Ind. Inform. (TII) 14 (4) (2018) 1594–1605, http://dx.doi.org/10.1109/TII.2018.2797922.
[60] J. Li, J. Jin, D. Yuan, M. Palaniswami, K. Moessner, EHOPES: Data-centered Fog platform for smart living, in: IEEE International Telecommunication Networks and Applications Conference (ITNAC), 2015, pp. 308–313, http://dx.doi.org/10.1109/ATNAC.2015.7366831.
[61] N. Chen, Y. Chen, S. Song, C.-T. Huang, X. Ye, Smart urban surveillance using fog computing, in: IEEE/ACM Symposium on Edge Computing (SEC), 2016, pp. 95–96, http://dx.doi.org/10.1109/SEC.2016.25.
[62] D. Bruneo, S. Distefano, F. Longo, G. Merlino, A. Puliafito, V. D'Amico, M. Sapienza, G. Torrisi, Stack4Things As a fog computing platform for Smart City applications, in: IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 2016, pp. 848–853, http://dx.doi.org/10.1109/INFCOMW.2016.7562195.
[63] J. He, J. Wei, K. Chen, Z. Tang, Y. Zhou, Y. Zhang, Multitier fog computing with large-scale iot data analytics for smart cities, IEEE Internet Things J. (IoT-J) 5 (2) (2018) 677–686, http://dx.doi.org/10.1109/JIOT.2017.2724845.
[64] M. Bansal, I. Chana, S. Clarke, Enablement of IoT based context-aware smart home with fog computing, in: Fog Computing: Breakthroughs in Research and Practice, IGI Global, 2018, pp. 251–263, http://dx.doi.org/10.4018/978-1-5225-5649-7.ch013.
[65] Y.-D. Chen, M.Z. Azhari, J.-S. Leu, Design and implementation of a power consumption management system for smart home over fog-cloud computing, in: IEEE International Conference on Intelligent Green Building and Smart Grid (IGBSG), 2018, pp. 1–5, http://dx.doi.org/10.1109/IGBSG.2018.8393553.
[66] G.P. Rocha Filho, L.Y. Mano, A.D.B. Valejo, L.A. Villas, J. Ueyama, A low-cost smart home automation to enhance decision-making based on fog computing and computational intelligence, IEEE Lat. Am. Trans. (LATAM) 16 (1) (2018) 186–191, http://dx.doi.org/10.1109/TLA.2018.8291472.
[67] F.Y. Okay, S. Ozdemir, A fog computing based smart grid model, in: IEEE International Symposium on Networks, Computers and Communications (ISNCC), 2016, pp. 1–6, http://dx.doi.org/10.1109/ISNCC.2016.7746062.
[68] S. Zahoor, S. Javaid, N. Javaid, M. Ashraf, F. Ishmanov, M.K. Afzal, Cloud–fog–based smart grid model for efficient resource management, Sustainability (2071-1050) 10 (6) (2018) http://dx.doi.org/10.3390/su10062079.
[69] A. Fatima, N. Javaid, M. Waheed, T. Nazar, S. Shabbir, T. Sultana, Efficient resource allocation model for residential buildings in smart grid using fog and cloud computing, in: International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), Springer, 2018, pp. 289–298, http://dx.doi.org/10.1007/978-3-319-93554-6_26.
[70] H. Dubey, J. Yang, N. Constant, A.M. Amiri, Q. Yang, K. Makodiya, Fog data: Enhancing telehealth big data through fog computing, in: Proceedings of the ASE BigData & SocialInformatics, ACM, 2015, p. 14, http://dx.doi.org/10.1145/2818869.2818889.
[71] B. Negash, T.N. Gia, A. Anzanpour, I. Azimi, M. Jiang, T. Westerlund, A.M. Rahmani, P. Liljeberg, H. Tenhunen, Leveraging fog computing for healthcare iot, in: Fog Computing in the Internet of Things, Springer, 2018, pp. 145–169, http://dx.doi.org/10.1007/978-3-319-57639-8_8.
[72] P. Verma, S.K. Sood, Fog assisted-IoT enabled patient health monitoring in smart homes, IEEE Internet Things J. (IoT-J) (2018) http://dx.doi.org/10.1109/JIOT.2018.2803201.
[73] M. Bhatia, S.K. Sood, Exploring temporal analytics in fog-cloud architecture for smart office HealthCare, Mob. Netw. Appl. (2018) 1–19, http://dx.doi.org/10.1007/s11036-018-0991-5.
[74] C.S. Nandyala, H.-K. Kim, From cloud to fog and IoT-based real-time U-healthcare monitoring for smart homes and hospitals, Int. J. Smart Home (IJSH) 10 (2) (2016) 187–196, http://dx.doi.org/10.14257/ijsh.2016.10.2.18.
[75] A. Monteiro, H. Dubey, L. Mahler, Q. Yang, K. Mankodiya, FIT A fog computing device for speech TeleTreatments, IEEE Int. Conf. Smart Comput. (SMARTCOMP) (2016) http://dx.doi.org/10.1109/SMARTCOMP.2016.7501692.
[76] O. Fratu, C. Pena, R. Craciunescu, S. Halunga, Fog computing system for monitoring Mild Dementia and COPD patients-Romanian case study, in: IEEE International Conference on Telecommunication in Modern Satellite, Cable and Broadcasting Services (TELSIKS), 2015, pp. 123–128, http://dx.doi.org/10.1109/TELSKS.2015.7357752.
[77] Z. Xu, H. Gupta, U. Ramachandran, STTR: A system for tracking all vehicles all the time at the edge of the network, in: ACM International Conference on Distributed and Event-Based Systems, 2018, pp. 124–135, http://dx.doi.org/10.1145/3210284.3210291.
[78] X. Hou, Y. Li, M. Chen, D. Wu, D. Jin, S. Chen, Vehicular fog computing: A viewpoint of vehicles as the infrastructures, IEEE Trans. Veh. Technol. 65 (6) (2016) 3860–3873, http://dx.doi.org/10.1109/TVT.2016.2532863.
[79] S.K. Datta, C. Bonnet, J. Haerri, Fog computing architecture to enable consumer centric internet of things services, in: IEEE International Symposium on Consumer Electronics (ISCE), 2015, pp. 1–2, http://dx.doi.org/10.1109/ISCE.2015.7177778.
[80] K. Abas, K. Obraczka, L. Miller, Solar-powered, wireless smart camera network: An IoT solution for outdoor video monitoring, Comput. Commun. (ComCom) 118 (2018) 217–233, http://dx.doi.org/10.1016/j.comcom.2018.01.007.
[81] S. Sudhakar, V. Vijayakumar, C.S. Kumar, V. Priya, L. Ravi, V. Subramaniyaswamy, Unmanned Aerial Vehicle (UAV) based Forest Fire Detection and monitoring for reducing false alarms in forest-fires, Comput. Commun. (ComCom) 149 (2020) 1–16, http://dx.doi.org/10.1016/j.comcom.2019.10.007.
[82] D. Jiang, The construction of smart city information system based on the internet of things and cloud computing, Comput. Commun. (ComCom) (2019) http://dx.doi.org/10.1016/j.comcom.2019.10.035.
[83] H. Li, K. Ota, M. Dong, Learning IoT in edge: deep learning for the internet of things with edge computing, IEEE Netw. 32 (1) (2018) 96–101, http://dx.doi.org/10.1109/MNET.2018.1700202.
[84] B. Tang, H. He, Q. Ding, S. Kay, A parametric classification rule based on the exponentially embedded family, IEEE Trans. Neural Netw. Learn. Syst. (TNNLS) 26 (2) (2015) 367–377, http://dx.doi.org/10.1109/TNNLS.2014.2383692.
[85] B. Tang, S. Khokhar, R. Gupta, Turn prediction at generalized intersections, in: IEEE Intelligent Vehicles Symposium (IV), 2015, pp. 1399–1404, http://dx.doi.org/10.1109/IVS.2015.7225911.
[86] H. Luo, H. Cai, H. Yu, Y. Sun, Z. Bi, L. Jiang, A short-term energy prediction system based on edge computing for smart city, Future Gener. Comput. Syst. (FGCS) (2019) http://dx.doi.org/10.1016/j.future.2019.06.030.
[87] Cisco, Cisco Global Cloud Index: Forecast and methodology, 2014–2019, White Paper, 2014.
[88] B. Nour, K. Sharif, F. Li, H. Moungla, A distributed ICN-based IoT network architecture: An ambient assisted living application case study, in: IEEE Global Communications Conference (GLOBECOM), Singapore, 2017, pp. 1–6, http://dx.doi.org/10.1109/GLOCOM.2017.8255022.
[89] L.Y. Mano, B.S. Faiçal, L.H. Nakamura, P.H. Gomes, G.L. Libralon, R.I. Meneguete, P.R. Geraldo Filho, G.T. Giancristofaro, G. Pessin, B. Krishnamachari, et al., Exploiting IoT technologies for enhancing Health Smart Homes through patient identification and emotion recognition, Comput. Commun. (ComCom) 89 (2016) 178–190, http://dx.doi.org/10.1016/j.comcom.2016.03.010.
[90] D.-M. Han, J.-H. Lim, Design and implementation of smart home energy management systems based on zigbee, IEEE Trans. Consum. Electron. 56 (3) (2010) http://dx.doi.org/10.1109/TCE.2010.5606278.
[91] X. Wang, B. Gu, Y. Ren, W. Ye, S. Yu, Y. Xiang, L. Gao, A fog-based recommender system, IEEE Internet Things J. 7 (2) (2019) 1048–1060, http://dx.doi.org/10.1109/JIOT.2019.2949029.
[92] A. Aliyu, A.H. Abdullah, O. Kaiwartya, Y. Cao, J. Lloret, N. Aslam, U.M. Joda, Towards video streaming in IoT environments: Vehicular communication perspective, Comput. Commun. (ComCom) 118 (2018) 93–119, http://dx.doi.org/10.1016/j.comcom.2017.10.003.
[93] J. Bhatia, R. Dave, H. Bhayani, S. Tanwar, A. Nayyar, SDN-Based real-time urban traffic analysis in VANET environment, Comput. Commun. (ComCom) 149 (2020) 162–175, http://dx.doi.org/10.1016/j.comcom.2019.10.011.
[94] K. Ansari, Cooperative position prediction: Beyond vehicle-to-vehicle relative positioning, IEEE Trans. Intell. Transp. Syst. (TITS) (2019) http://dx.doi.org/10.1109/TITS.2019.2902572.
[95] J. Shi, Z. Yang, H. Xu, M. Chen, B. Champagne, Dynamic resource allocation for LTE-based vehicle-to-infrastructure networks, IEEE Trans. Veh. Technol. (2019) http://dx.doi.org/10.1109/TVT.2019.2903822.
[96] L. Noel, G.Z. de Rubens, J. Kester, B.K. Sovacool, The technical challenges to V2G, in: Vehicle-To-Grid, Springer, 2019, pp. 65–89, http://dx.doi.org/10.1007/978-3-030-04864-8_3.
[97] M. Laroui, B. Nour, H. Moungla, H. Afifi, M. Cherif, Mobile vehicular edge computing architecture using rideshare taxis as a mobile edge server, in: IEEE Annual Consumer Communications Networking Conference (CCNC), IEEE, Las Vegas, NV, USA, 2020, pp. 1–2, http://dx.doi.org/10.1109/CCNC46108.2020.9045741.
[98] A. Gregoriades, A. Sutcliffe, Simulation-based evaluation of an in-vehicle smart situation awareness enhancement system, Ergonomics (2018) 1–28, http://dx.doi.org/10.1080/00140139.2018.1427803.
[99] J. Singh, K. Singh, Congestion control in vehicular Ad Hoc network: A review, in: Next-Generation Networks (NGN), Springer, 2018, pp. 489–496, http://dx.doi.org/10.1007/978-981-10-6005-2_49.
[100] K. Qin, A. Sun, M. Xue, K. Zhong, C. Jia, Traffic alert methods in an intersection and vehicle multi-functional ambient light systems, Google Patents, US Patent App. 15/673,956, 2018.
[101] J. Liu, J. Li, L. Zhang, F. Dai, Y. Zhang, X. Meng, J. Shen, Secure intelligent traffic light control using fog computing, Future Gener. Comput. Syst. (FGCS) 78 (2018) 817–824, http://dx.doi.org/10.1016/j.future.2017.02.017.
[102] T. Lehr, Smart cities: Vision on-the-ground, in: Smart Cities, Springer, 2018, pp. 3–15, http://dx.doi.org/10.1007/978-3-319-59381-4_1.
[103] J.A. Jimenez, Smart transportation systems, in: Smart Cities, Springer, 2018, pp. 123–133, http://dx.doi.org/10.1007/978-3-319-59381-4_8.
[104] N. Komninos, E. Philippou, A. Pitsillides, Survey in smart grid and smart home security: Issues, challenges and countermeasures, IEEE Commun. Surv. Tutor. (COMST) 16 (4) (2014) 1933–1954, http://dx.doi.org/10.1109/COMST.2014.2320093.
[105] S.S. Sk, G. Thatiparthi, R.S. Gunturi, Cloud and intelligent based SCADA technology, Int. J. Adv. Res. Comput. Sci. (IJARCS) Electron. Eng. (IJARCSEE) 2 (3) (2013) 293.

[106] M.M. Hussain, M.S. Alam, M.S. Beg, Feasibility of fog computing in smart grid architectures, in: International Conference on Communication, Computing and Networking (ICCCN), Springer, 2019, pp. 999–1010, http://dx.doi.org/10.1007/978-981-13-1217-5_98.

[107] J. Jiang, L. Gao, J. Jin, T.H. Luan, S. Yu, Y. Xiang, S. Garg, Sustainability analysis for fog nodes with renewable energy supplies, IEEE Internet Things J. 6 (4) (2019) 6725–6735, http://dx.doi.org/10.1109/JIOT.2019.2910875.

[108] Q. Zheng, J. Jin, T. Zhang, J. Li, L. Gao, Y. Xiang, Energy-sustainable fog system for mobile web services in infrastructure-less environments, IEEE Access 7 (2019) 161318–161328, http://dx.doi.org/10.1109/ACCESS.2019.2951162.

[109] T.N. Gia, I.B. Dhaou, M. Ali, A.M. Rahmani, T. Westerlund, P. Liljeberg, H. Tenhunen, Energy efficient fog-assisted IoT system for monitoring diabetic patients with cardiovascular disease, Future Gener. Comput. Syst. (FGCS) 93 (2019) 198–211, http://dx.doi.org/10.1016/j.future.2018.10.029.

[110] M.M. Mahmoud, J.J. Rodrigues, K. Saleem, J. Al-Muhtadi, N. Kumar, V. Korotaev, Towards energy-aware fog-enabled cloud of things for healthcare, Comput. Electr. Eng. 67 (2018) 58–69, http://dx.doi.org/10.1016/j.compeleceng.2018.02.047.

[111] S. Tuli, N. Basumatary, S.S. Gill, M. Kahani, R.C. Arya, G.S. Wander, R. Buyya, HealthFog: An ensemble deep learning based smart healthcare system for automatic diagnosis of heart diseases in integrated IoT and fog computing environments, Future Gener. Comput. Syst. (2019) http://dx.doi.org/10.1016/j.future.2019.10.043.

[112] P.H. Vilela, J.J. Rodrigues, P. Solic, K. Saleem, V. Furtado, Performance evaluation of a fog-assisted IoT solution for e-Health applications, Future Gener. Comput. Syst. (FGCS) 97 (2019) 379–386, http://dx.doi.org/10.1016/j.future.2019.02.055.

[113] S. Bitam, S. Zeadally, A. Mellouk, Fog computing job scheduling optimization based on bees swarm, Enterp. Inf. Syst. (EIS) 12 (4) (2018) 373–397, http://dx.doi.org/10.1080/17517575.2017.1304579.

[114] X.-Q. Pham, E.-N. Huh, Towards task scheduling in a cloud-fog computing system, in: IEEE Asia-Pacific Network Operations and Management Symposium (APNOMS), 2016, pp. 1–4, http://dx.doi.org/10.1109/APNOMS.2016.7737240.

[115] G.C. Sih, E.A. Lee, A compile-time scheduling heuristic for interconnection-constrained heterogeneous processor architectures, IEEE Trans. Parallel Distributed Syst. (TPDS) 4 (2) (1993) 175–187, http://dx.doi.org/10.1109/71.207593.

[116] H. Topcuoglu, S. Hariri, M.-y. Wu, Performance-effective and low-complexity task scheduling for heterogeneous computing, IEEE Trans. Parallel Distributed Syst. (TPDS) 13 (3) (2002) 260–274, http://dx.doi.org/10.1109/71.993206.

[117] H. Wang, J. Gong, Y. Zhuang, H. Shen, J. Lach, Healthedge: Task scheduling for edge computing with health emergency and human behavior consideration in smart homes, in: IEEE International Conference on Big Data (Big Data), 2017, pp. 1213–1222, http://dx.doi.org/10.1109/BigData.2017.8258047.

[118] T. Choudhari, M. Moh, T.-S. Moh, Prioritized task scheduling in fog computing, in: Annual ACM Southeast Conference (ACMSE), 2018, p. 22, http://dx.doi.org/10.1145/3190645.3190699.

[119] Q. Liu, Y. Wei, S. Leng, Y. Chen, Task scheduling in fog enabled Internet of Things for smart cities, in: IEEE International Conference on Communication Technology (ICCT), 2017, pp. 975–980, http://dx.doi.org/10.1109/ICCT.2017.8359780.

[120] D. Hoang, T.D. Dang, FBRC: Optimization of task scheduling in Fog-based Region and Cloud, in: IEEE International Conference on Big Data Science and Engineering, and IEEE International Conference on Embedded Software and Systems (Trustcom/BigDataSE/ICESS), 2017, pp. 1109–1114, http://dx.doi.org/10.1109/Trustcom/BigDataSE/ICESS.2017.360.

[121] X.-Q. Pham, N.D. Man, N.D.T. Tri, N.Q. Thai, E.-N. Huh, A cost-and performance-effective approach for task scheduling based on collaboration between cloud and fog computing, Int. J. Distributed Sens. Netw. (IJDSN) 13 (11) (2017) 1550147717742073, http://dx.doi.org/10.1177/1550147717742073.

[122] J. Li, S. Su, X. Cheng, Q. Huang, Z. Zhang, Cost-conscious scheduling for large graph processing in the cloud, in: IEEE International Conference on High Performance Computing and Communications (HPCC), 2011, pp. 808–813, http://dx.doi.org/10.1109/HPCC.2011.147.

[123] J. Fan, X. Wei, T. Wang, T. Lan, S. Subramaniam, Deadline-aware task scheduling in a tiered IoT infrastructure, in: IEEE Global Communications Conference (GLOBECOM), 2017, pp. 1–7, http://dx.doi.org/10.1109/GLOCOM.2017.8255037.

[124] S. Kabirzadeh, D. Rahbari, M. Nickray, A hyper heuristic algorithm for scheduling of fog networks, in: IEEE Conference of Open Innovations Association (FRUCT), 2017, pp. 148–155, http://dx.doi.org/10.23919/FRUCT.2017.8250177.

[125] R.L. Kadri, F.F. Boctor, An efficient genetic algorithm to solve the resource-constrained project scheduling problem with transfer times: The single mode case, European J. Oper. Res. (EJOR) 265 (2) (2018) 454–462, http://dx.doi.org/10.1016/j.ejor.2017.07.027.

[126] M. Nouiri, A. Bekrar, A. Jemai, S. Niar, A.C. Ammari, An effective and distributed particle swarm optimization algorithm for flexible job-shop scheduling problem, J. Intell. Manuf. 29 (3) (2018) 603–615, http://dx.doi.org/10.1007/s10845-015-1039-3.

[127] S. Mirjalili, Ant colony optimisation, in: Evolutionary Algorithms and Neural Networks, Springer, 2019, pp. 33–42, http://dx.doi.org/10.1007/978-3-319-93025-1_3.

[128] T. Zhu, S. Chen, W. Zhu, Y. Wang, Optimization of sound absorption property for polyurethane foam using adaptive simulated annealing algorithm, J. Appl. Polym. Sci. 135 (26) (2018) 46426, http://dx.doi.org/10.1002/app.46426.

[129] J. Wan, B. Chen, S. Wang, M. Xia, D. Li, C. Liu, Fog computing for energy-aware load balancing and scheduling in smart factory, IEEE Trans. Ind. Inform. (TII) (2018) http://dx.doi.org/10.1109/TII.2018.2818932.

[130] B. Liu, L. Wang, Y.-H. Jin, An effective PSO-based memetic algorithm for flow shop scheduling, IEEE Trans. Syst. Man Cybern. B 37 (1) (2007) 18–27, http://dx.doi.org/10.1109/TSMCB.2006.883272.

[131] D. Zeng, L. Gu, S. Guo, Z. Cheng, S. Yu, Joint optimization of task scheduling and image placement in fog computing supported software-defined embedded system, IEEE Trans. Comput. (TC) 65 (12) (2016) 3702–3712, http://dx.doi.org/10.1109/TC.2016.2536019.

[132] C. Adjiman, I. Androulakis, C. Floudas, Global optimization of MINLP problems in process synthesis and design, Comput. Chem. Eng. 21 (Suppl S) (1997) S445–S450, http://dx.doi.org/10.1016/S0098-1354(97)87542-4.

[133] S. Li, J. Huang, Energy efficient resource management and task scheduling for IoT services in edge computing paradigm, in: IEEE International Conference on Ubiquitous Computing and Communications, IEEE International Symposium on Parallel and Distributed Processing with Applications (ISPA/IUCC), 2017, pp. 846–851, http://dx.doi.org/10.1109/ISPA/IUCC.2017.00129.

[134] Y. Yang, K. Wang, G. Zhang, X. Chen, X. Luo, M.-T. Zhou, MEETS: Maximal energy efficient task scheduling in homogeneous fog networks, IEEE Internet Things J. (IoT-J) (2018) http://dx.doi.org/10.1109/JIOT.2018.2846644.

[135] V. Cardellini, V. Grassi, F.L. Presti, M. Nardelli, On QoS-aware scheduling of data stream applications over fog computing infrastructures, in: IEEE Symposium on Computers and Communication (ISCC), 2015, pp. 271–276, http://dx.doi.org/10.1109/ISCC.2015.7405527.

[136] M. Verma, N. Bhardwaj, A.K. Yadav, Real time efficient scheduling algorithm for load balancing in fog computing environment, Int. J. Inf. Technol. Comput. Sci. 8 (4) (2016) 1–10, http://dx.doi.org/10.5815/ijitcs.2016.04.01.

[137] C.S. Pawar, R.B. Wagh, Priority based dynamic resource allocation in cloud computing with modified waiting queue, in: IEEE International Conference on Intelligent Systems and Signal Processing (ISSP), 2013, pp. 311–316, http://dx.doi.org/10.1109/ISSP.2013.6526925.

[138] A. Marphatia, A. Muhnot, T. Sachdeva, E. Shukla, Optimization of FCFS based resource provisioning algorithm for cloud computing, IOSR J. Comput. Eng. (IOSR-JCE) (2013) http://dx.doi.org/10.9790/0661-1050105, 2278–0661.

[139] A.V. Lakra, D.K. Yadav, Multi-objective tasks scheduling algorithm for cloud computing throughput optimization, Procedia Comput. Sci. 48 (2015) 107–113, http://dx.doi.org/10.1016/j.procs.2015.04.158.

[140] S. Ghanavati, J.H. Abawajy, D. Izadi, An energy aware task scheduling model using ant-mating optimization in fog computing environment, IEEE Trans. Serv. Comput. (2020) http://dx.doi.org/10.1109/TSC.2020.3028575.

[141] I.M. Ali, K.M. Sallam, N. Moustafa, R. Chakraborty, M.J. Ryan, K.-K.R. Choo, An automated task scheduling model using non-dominated sorting genetic algorithm II for fog-cloud systems, IEEE Trans. Cloud Comput. (2020) http://dx.doi.org/10.1109/TCC.2020.3032386.

[142] J. Xie, D. Guo, Z. Hu, T. Qu, P. Lv, Control plane of software defined networks: A survey, Comput. Commun. (ComCom) 67 (2015) 1–10, http://dx.doi.org/10.1016/j.comcom.2015.06.004.

[143] D. Qi, S. Shen, G. Wang, Towards an efficient VNF placement in network function virtualization, Comput. Commun. (ComCom) 138 (2019) 81–89, http://dx.doi.org/10.1016/j.comcom.2019.03.005.

[144] N.B. Truong, G.M. Lee, Y. Ghamri-Doudane, Software defined networking-based vehicular adhoc network with fog computing, in: IFIP/IEEE International Symposium on Integrated Network Management (IM), 2015, pp. 1202–1207, http://dx.doi.org/10.1109/INM.2015.7140467.

[145] L. Huang, G. Li, J. Wu, L. Li, J. Li, R. Morello, Software-defined QoS provisioning for fog computing advanced wireless sensor networks, in: IEEE SENSORS, 2016, pp. 1–3, http://dx.doi.org/10.1109/ICSENS.2016.7808814.

[146] K. Liang, L. Zhao, X. Chu, H.-H. Chen, An integrated architecture for software defined and virtualized radio access networks with fog computing, IEEE Netw. 31 (1) (2017) 80–87, http://dx.doi.org/10.1109/MNET.2017.1600027NM.

[147] S. Tomovic, K. Yoshigoe, I. Maljevic, I. Radusinovic, Software-defined fog network architecture for IoT, Wirel. Pers. Commun. 92 (1) (2017) 181–196, http://dx.doi.org/10.1007/s11277-016-3845-0.

[148] R. Vilalta, S. Vía, F. Mira, R. Casellas, R. Muñoz, J. Alonso-Zarate, A. Kousaridas, M. Dillinger, Control and management of a connected car using sdn/nfv, fog computing and yang data models, in: IEEE Conference on Network Softwarization and Workshops (NetSoft), 2018, pp. 378–383, http://dx.doi.org/10.1109/NETSOFT.2018.8460131.

[149] N. Kiran, X. Liu, S. Wang, C. Yin, Optimising resource allocation for virtual network functions in SDN/NFV-enabled MEC networks, IET Commun. (2021) http://dx.doi.org/10.1049/cmu2.12183.

[150] H.A. Al Hamid, S.M.M. Rahman, M.S. Hossain, A. Almogren, A. Alamri, A security model for preserving the privacy of medical big data in a healthcare cloud using a fog computing facility with pairing-based cryptography, IEEE Access 5 (2017) 22313–22328, http://dx.doi.org/10.1109/ACCESS.2017.2757844.

[151] W. Abdul, Z. Ali, S. Ghouzali, B. Alfawaz, G. Muhammad, M.S. Hossain, Biometric security through visual encryption for fog edge computing, IEEE Access 5 (2017) 5531–5538, http://dx.doi.org/10.1109/ACCESS.2017.2693438.

[152] B. Mukherjee, R.L. Neupane, P. Calyam, End-to-End IoT security middleware for cloud-fog communication, in: IEEE International Conference on Cyber Security and Cloud Computing (CSCloud), 2017, pp. 151–156, http://dx.doi.org/10.1109/CSCloud.2017.62.

[153] A.A. Diro, N. Chilamkurti, N. Kumar, Lightweight cybersecurity schemes using elliptic curve cryptography in publish-subscribe fog computing, Mob. Netw. Appl. 22 (5) (2017) 848–858, http://dx.doi.org/10.1007/s11036-017-0851-8.

[154] Q. Huang, Y. Yang, L. Wang, Secure data access control with ciphertext update and computation outsourcing in fog computing for Internet of Things, IEEE Access 5 (2017) 12941–12950, http://dx.doi.org/10.1109/ACCESS.2017.2727054.

[155] P. Hu, H. Ning, T. Qiu, H. Song, Y. Wang, X. Yao, Security and privacy preservation scheme of face identification and resolution framework using fog computing in internet of things, IEEE Internet Things J. (IoT-J) 4 (5) (2017) 1143–1155, http://dx.doi.org/10.1109/JIOT.2017.2659783.

[156] J. Cui, L. Wei, J. Zhang, Y. Xu, H. Zhong, An efficient message-authentication scheme based on edge computing for vehicular Ad Hoc networks, IEEE Trans. Intell. Transp. Syst. (TITS) (2018) http://dx.doi.org/10.1109/TITS.2018.2827460.

[157] S. He, B. Cheng, H. Wang, X. Xiao, Y. Cao, J. Chen, Data security storage model for fog computing in large-scale IoT application, in: IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 2018, http://dx.doi.org/10.1109/INFCOMW.2018.8406927.

[158] D. He, Y. Qiao, S. Chan, N. Guizani, Flight security and safety of drones in airborne fog computing systems, IEEE Commun. Mag. (COMMAG) 56 (5) (2018) 66–71, http://dx.doi.org/10.1109/MCOM.2018.1700916.

[159] N.H. Motlagh, T. Taleb, O. Arouk, Low-altitude unmanned aerial vehicles-based internet of things services: Comprehensive survey and future perspectives, IEEE Internet Things J. (IoT-J) 3 (6) (2016) 899–922, http://dx.doi.org/10.1109/JIOT.2016.2612119.

[160] S. Alharbi, P. Rodriguez, R. Maharaja, P. Iyer, N. Bose, Z. Ye, FOCUS: A fog computing-based security system for the Internet of Things, in: IEEE Annual Consumer Communications & Networking Conference (CCNC), 2018, pp. 1–5, http://dx.doi.org/10.1109/CCNC.2018.8319238.

[161] J. Ni, K. Zhang, Y. Yu, X. Lin, X.S. Shen, Providing task allocation and secure deduplication for mobile crowdsensing via fog computing, IEEE Trans. Dependable Secur. Comput. (TDSC) (2018) http://dx.doi.org/10.1109/TDSC.2018.2791432.

[162] P. Zhang, C. Jiang, X. Pang, Y. Qian, STEC-IoT: A security tactic by virtualizing edge computing on IoT, IEEE Internet Things J. (2020) http://dx.doi.org/10.1109/JIOT.2020.3017742.

[163] A. Razaque, M. Aloqaily, M. Almiani, Y. Jararweh, G. Srivastava, Efficient and reliable forensics using intelligent edge computing, Future Gener. Comput. Syst. 118 (2021) 230–239, http://dx.doi.org/10.1016/j.future.2021.01.012.

[164] Q. Wang, D. Chen, N. Zhang, Z. Ding, Z. Qin, PCP: A privacy-preserving content-based publish-subscribe scheme with differential privacy in fog computing, IEEE Access 5 (2017) 17962–17974, http://dx.doi.org/10.1109/ACCESS.2017.2748956.

[165] F.Y. Okay, S. Ozdemir, A secure data aggregation protocol for fog computing based smart grids, in: IEEE International Conference on Compatibility, Power Electronics and Power Engineering (CPE-POWERENG), 2018, pp. 1–6, http://dx.doi.org/10.1109/CPE.2018.8372598.

[166] A. Acar, H. Aksu, A.S. Uluagac, M. Conti, A survey on homomorphic encryption schemes: Theory and implementation, ACM Comput. Surv. 51 (4) (2018) 79, http://dx.doi.org/10.1145/3214303.

[167] X. Wang, L. Wang, Y. Li, K. Gai, Privacy-aware efficient fine-grained data access control in internet of medical things based fog computing, IEEE Access (2018) http://dx.doi.org/10.1109/ACCESS.2018.2856896.

[168] K. Fan, H. Xu, L. Gao, H. Li, Y. Yang, Efficient and privacy preserving access control scheme for fog-enabled IoT, Future Gener. Comput. Syst. 99 (2019) 134–142, http://dx.doi.org/10.1016/j.future.2019.04.003.

[169] B.S. Gu, L. Gao, X. Wang, Y. Qu, J. Jin, S. Yu, Privacy on the edge: Customizable privacy-preserving context sharing in hierarchical edge computing, IEEE Trans. Netw. Sci. Eng. (2019) http://dx.doi.org/10.1109/TNSE.2019.2933639.

[170] Y. Qu, L. Gao, T.H. Luan, Y. Xiang, S. Yu, B. Li, G. Zheng, Decentralized privacy using blockchain-enabled federated learning in fog computing, IEEE Internet Things J. 7 (6) (2020) 5171–5183, http://dx.doi.org/10.1109/JIOT.2020.2977383.

[171] B. Nour, A. Ksentini, N. Herbaut, P.A. Frangoudis, H. Moungla, A blockchain-based network slice broker for 5G services, IEEE Netw. Lett. (2019) http://dx.doi.org/10.1109/LNET.2019.2915117.

[172] M. Conti, S. Kumar, C. Lal, S. Ruj, A survey on security and privacy issues of bitcoin, IEEE Commun. Surv. Tutorials (COMST) (2018) http://dx.doi.org/10.1109/COMST.2018.2842460.

[173] X. Wang, X. Zha, W. Ni, R.P. Liu, Y.J. Guo, X. Niu, K. Zheng, Survey on blockchain for Internet of Things, Comput. Commun. (ComCom) (2019) http://dx.doi.org/10.1016/j.comcom.2019.01.006.

[174] N. Islam, Y. Faheem, I.U. Din, M. Talha, M. Guizani, M. Khalil, A blockchain-based fog computing framework for activity recognition as an application to e-Healthcare services, Future Gener. Comput. Syst. (FGCS) 100 (2019) 569–578, http://dx.doi.org/10.1016/j.future.2019.05.059.

[175] Y. Jiao, P. Wang, D. Niyato, Z. Xiong, Social welfare maximization auction in edge computing resource allocation for mobile blockchain, in: IEEE International Conference on Communications (ICC), 2018, pp. 1–6, http://dx.doi.org/10.1109/ICC.2018.8422632.

[176] N.C. Luong, Z. Xiong, P. Wang, D. Niyato, Optimal auction for edge computing resource management in mobile blockchain networks: A deep learning approach, in: IEEE International Conference on Communications (ICC), 2018, pp. 1–6, http://dx.doi.org/10.1109/ICC.2018.8422743.

[177] P. Dütting, Z. Feng, H. Narasimhan, D.C. Parkes, Optimal auctions through deep learning, 2017, arXiv preprint arXiv:1706.03459.

[178] Z. Xiong, S. Feng, D. Niyato, P. Wang, Z. Han, Optimal pricing-based edge computing resource management in mobile blockchain, in: IEEE International Conference on Communications (ICC), 2018, pp. 1–6, http://dx.doi.org/10.1109/ICC.2018.8422517.

[179] K. Suankaewmanee, D.T. Hoang, D. Niyato, S. Sawadsitang, P. Wang, Z. Han, Performance analysis and application of mobile blockchain, in: IEEE International Conference on Computing, Networking and Communications (ICNC), 2018, pp. 642–646, http://dx.doi.org/10.1109/ICCNC.2018.8390265.

[180] R. Casado-Vara, F. de la Prieta, J. Prieto, J.M. Corchado, Blockchain framework for IoT data quality via edge computing, in: Proceedings of the 1st Workshop on Blockchain-Enabled Networked Sensor Systems (BlockSys), ACM, 2018, pp. 19–24, http://dx.doi.org/10.1145/3282278.3282282.

[181] L. Zhang, Y. Zou, W. Wang, Z. Jin, Y. Su, H. Chen, Resource allocation and trust computing for blockchain-enabled edge computing system, Comput. Secur. 105 (2021) 102249, http://dx.doi.org/10.1016/j.cose.2021.102249.

[182] A.A. Abdellatif, L. Samara, A. Mohamed, A. Erbad, C.F. Chiasserini, M. Guizani, M.D. O'Connor, J. Laughton, MEdge-Chain: Leveraging edge computing and blockchain for efficient medical data exchange, IEEE Internet Things J. (2021) http://dx.doi.org/10.1109/JIOT.2021.3052910.

[183] S. Aggarwal, N. Kumar, Path planning techniques for unmanned aerial vehicles: A review, solutions, and challenges, Comput. Commun. (ComCom) (2019) http://dx.doi.org/10.1016/j.comcom.2019.10.014.

[184] R. Wang, Y. Cao, A. Noor, T.A. Alamoudi, R. Nour, Agent-enabled task offloading in UAV-aided mobile edge computing, Comput. Commun. (ComCom) (2019) http://dx.doi.org/10.1016/j.comcom.2019.10.021.

[185] N. Piovesan, A.F. Gambin, M. Miozzo, M. Rossi, P. Dini, Energy sustainable paradigms and methods for future mobile networks: A survey, Comput. Commun. (ComCom) 119 (2018) 101–117, http://dx.doi.org/10.1016/j.comcom.2018.01.005.

[186] S.K. Pasupuleti, S. Ramalingam, R. Buyya, An efficient and secure privacy-preserving approach for outsourced data of resource constrained mobile devices in cloud computing, J. Netw. Comput. Appl. 64 (2016) 12–22, http://dx.doi.org/10.1016/j.jnca.2015.11.023.

[187] M. Bahrami, M. Singhal, A light-weight permutation based method for data privacy in mobile cloud computing, in: IEEE International Conference on Mobile Cloud Computing, Services, and Engineering, 2015, pp. 189–198, http://dx.doi.org/10.1109/MobileCloud.2015.36.

[188] M. Anbarasan, B. Muthu, C. Sivaparthipan, R. Sundarasekar, S. Kadry, S. Krishnamoorthy, A.A. Dasel, et al., Detection of flood disaster system based on IoT, big data and convolutional deep neural network, Comput. Commun. (ComCom) (2019) http://dx.doi.org/10.1016/j.comcom.2019.11.022.

[189] S. Zafar, S. Jangsher, O. Bouachir, M. Aloqaily, J.B. Othman, QoS Enhancement with deep learning-based interference prediction in mobile IoT, Comput. Commun. (ComCom) 148 (2019) 86–97, http://dx.doi.org/10.1016/j.comcom.2019.09.010.