# Mobile Edge Computing: A Survey

Nasir Abbas, Yan Zhang, *Senior Member, IEEE*, Amir Taherkordi, *Member, IEEE*, and Tor Skeie

***Abstract*—Mobile edge computing (MEC) is an emergent architecture where cloud computing services are extended to the edge of networks leveraging mobile base stations. As a promising edge technology, it can be applied to mobile, wireless, and wireline scenarios, using software and hardware platforms, located at the network edge in the vicinity of end-users. MEC provides seamless integration of multiple application service providers and vendors toward mobile subscribers, enterprises, and other vertical segments. It is an important component in the 5G architecture which supports variety of innovative applications and services where ultralow latency is required. This paper is aimed to present a comprehensive survey of relevant research and technological developments in the area of MEC. It provides the definition of MEC, its advantages, architectures, and application areas; where we in particular highlight related research and future directions. Finally, security and privacy issues and related existing solutions are also discussed.**

***Index Terms*—Fog computing, Internet of Things (IoT), mobile cloud computing (MCC), mobile edge computing (MEC).**

## I. Introduction

THE PREVALENCE of mobile terminals, such as smartphones or tablet computers, has an uttermost effect on mobile and wireless networks, triggering challenges for mobile networks worldwide [1], [2]. This class of networks has to endure low storage capacity, high energy consumption, low bandwidth, and high latency [3]. Moreover, exponential growth of the emerging Internet of Things (IoT) technology is foreseen to further stumble cellular and wireless networks [4]. Mobile cloud computing (MCC), as an integration of cloud computing and mobile computing, has provided considerable capabilities to mobile devices and empowered them with storage, computation, and energy resources offered by the centralized cloud [5], [6]. However, popping up a myriad of mobile devices, MCC is encountering noticeable challenges, such as high latency, security vulnerability, low coverage, and lagged data transmission. These challenges can become more difficult to address in the case of next generation mobile networks (e.g., 5G) [7]. Moreover, MCC is not suitable for scenarios involving real-time applications and guaranteeing high quality of service. According to the recent report presented by Cisco Visual Networking Index, 11.6 billion mobile-connected devices will be used by 2020 [2]. The trend of increase in mobile devices usage is fundamentally driven by the augmentation of mobile users and mobile applications development (e.g., iPhone apps and Google apps) [8], [9].

In the era of computing paradigms, edge computing (also known as fog computing) [10], has begun to be of paramount significance, especially mobile edge computing (MEC) in mobile cellular networks. The main purpose of MEC is to address the challenges that are hailed from MCC systems. MEC empowers MCC by deploying cloud resources, e.g., storage and processing capacity, to the edge within the radio access network (RAN). This provides the end-user with swift and powerful computing, energy efficiency, storage capacity, mobility, location, and context awareness support [11], [12]. Previously, the technology at the edge of the Internet known as *cloudlet* technology has been introduced to deploy mobile cloud services; however, it was inadequate because of its limited WiFi coverage. In a highly computational environment, cloudlets can efficiently process the computationally intensive tasks offloaded from devices [12]. Alternatively, MEC is equipped with better offloading techniques that characterize the network with low-latency and high-bandwidth.

Although MEC technologies and reported research contributions are still young and limited, providing a thorough overview of the state-of-the-art in MEC development will provide useful insights to the current status of this area and help to uncover potential research directions. This basically shapes the contribution of this paper, which is surveying MEC. There exist a few MEC survey reports in [13] and [14]. However, the former mainly analyzes security threats and challenges that affect different edge paradigms, such as fog computing, MEC, and MCC. The latter provides a brief overview of different attributes of MEC and identifies the major open research challenges in MEC, while the detailed and thorough study of different design aspects and research trends is largely missing in this survey work.

This paper presents an extensive survey on MEC focusing on its general overview. Section II gives an overview of MEC encompassing definition, concepts, architectures and its advantages. Sections III and IV list MEC applications and emerging scenarios. Section V presents state-of-the-art research on MEC with respect to computational offloading, latency, storage, and energy efficiency. Then, research infrastructures are presented in Section VI which has been referred to as MEC testbeds in recent studies. Sections VII and VIII outline security and privacy issues, including security mechanisms. Finally, Section IX discusses MEC open issues. The list of

Manuscript received March 13, 2017; accepted August 22, 2017. Date of publication September 8, 2017; date of current version February 9, 2018.*(Corresponding author: Yan Zhang.)*

N. Abbas, Y. Zhang, and A. Taherkordi are with the Department of Informatics, University of Oslo, Norway (e-mail: nasirabb@student.iln.uio.no; yanzhang@ifi.uio.no; amirhost@ifi.uio.no).

T. Skeie is with the Simula Research Laboratory, 1325 Lysaker, Norway, and also with the Department of Informatics, University of Oslo, Norway (e-mail: tskeie@simula.no).

Digital Object Identifier 10.1109/JIOT.2017.2750180

TABLE I
ACRONYMS/ABBREVIATIONS

| | |
|---|---|
| 1G | First Generation |
| 2G | Second Generation |
| 3G | Third Generation |
| 4G | Fourth Generation |
| 5G | Fifth Generation |
| 5GTN | 5th Generation Test Network |
| API | Application Program Interface |
| AR | Augmented Reality |
| ASP | Application Service Provider |
| BS | Base Station |
| BSC | base station controller |
| nDCs | Nano Data Centers |
| DNS | Domain Name Server |
| DOS | Denial of Service |
| EAB | Edge Accelerated Web Browsing |
| EEG | Electroencephalogram |
| eNodeB | Evolved Node B |
| ETSI | European Telecommunications Standards Institute |
| FC | Fog Computing |
| FN | Fog Node |
| GPRS | General Packet Radio Service |
| GPS | Global Positioning System |
| IaaS | infrastructure-as-a-Service |
| IDS | Intrusion Detection System |
| IoT | Internet of Things |
| ISG | Industry Specification Group |
| LBS | Location Based Service |
| LTE | Long Term Evolution |
| M2M | Machine-to-machine |
| MCC | Mobile Cloud Computing |
| MNO | Mobile Network Operator |
| MU | Mobile Users |
| NFC | Near field communication |
| NILL | Non-Intrusive Load Leveling |
| NP-hardness | non-deterministic polynomial-time hard |
| OTT | Over-the-top |
| QoE | Quality of Experience |
| RAN | Radio Access Network |
| SRAN | Service-Aware RAN |
| SAE | System Architecture Evolution |
| SCADA | Supervisory Control Data Acquisition |
| SDCompute | Software Defined Compute |
| SDN | Software Defined Network |
| SDSec | Software Defined Security |
| SDStorage | Software Defined Storage |
| SRAN | Service-Aware RAN |
| TDMA | Time Division Multiple Access |
| UE | User Equipment |
| UMTS | Universal Mobile Telecommunication System |
| UTRAN | UMTS radio access network |
| VDTNs | Vehicular Delay-Tolerant Networks |
| WAN | Wide Area Network |
| WSAN | Wireless Sensor Actuator Network |

acronyms and abbreviations used in this paper are summarized in Table I.

## II. MEC Overview

The term MEC was standardized by European Telecommunications Standards Institute (ETSI) and Industry Specification Group (ISG). The ISG group includes Nokia Networks, Intel, Vodafone, IBM, Huawei, and NTT DOCOMO, to name a few. MEC is also acknowledged by European 5G Infrastructure Public Private Partnership as a prime emerging technology for 5G networks [15].

### A. Definition of Mobile Edge Computing

According to ETSI, MEC is defined as [15] follows.

"Mobile edge computing provides an IT service environment and cloud computing capabilities at the edge of the mobile network, within the radio access network (RAN) and in close proximity to mobile subscribers."

MEC offers cloud computing capabilities within the RAN. Allowing direct mobile traffic between the core network and the end-user, instead, MEC connects the user directly to the nearest cloud service-enabled edge network. Deploying MEC at the base station enhances computation and avoids bottlenecks and system failure [7], [16].

According to the white paper published by ETSI, MEC can be characterized by [17].

1) *On-Premises:* MEC platforms can run isolated from the rest of the network, while they have access to local resources. This is very important for machine-to-machine (M2M) scenarios. The MEC property of segregation from other networks also makes it less vulnerable.
2) *Proximity:* Being deployed at the nearest location, MEC has an advantage to analyze and materialize big data. It is also beneficial for compute-hungry devices, such as augmented reality (AR), video analytics, etc.
3) *Lower Latency:* MEC services are deployed at the nearest location to user devices, isolating network data movement from the core network. Hence, user experience is accounted high quality with ultralow latency and high bandwidth.
4) *Location Awareness:* Edge-distributed devices utilize low-level signaling for information sharing. MEC receives information from edge devices within the local access network to discover the location of devices.
5) *Network Context Information:* Applications providing network information and services of real-time network data can benefit businesses and events by implementing MEC in their business model. On the basis of RAN real-time information, these applications can estimate the congestion of the radio cell and network bandwidth. This will help them in future to make smart decisions for better delivery of services to customers.

### B. Related Concepts and Technologies

There are some terms similar to MEC, such as MCC, local cloud, cloudlets, and fog computing [18]. In the following, we carefully discuss these terms.

1) MCC generally integrates all the advantages of mobile computing, cloud computing, and mobile Internet [19]. The main focus of cloud computing is to enable isolated virtualized computing, storage and communication resources that are leveraged by end-users [20]. Some examples of cloud computing infrastructures and platforms are Amazon EC2, Microsoft Azure, Google, and Aneka. MCC enables resources on demand, such as network, server, application, storage, and computing resources in a mobile environment [21]. MCC also

focuses on resource management that could be easily manageable [20]. In an MCC infrastructure, the centralized cloud servers are located far off from end devices, therefore are less productive in computation intense environments. For example, mobile applications connected to the cloud may face network latency or disconnections while mobile applications are used.

2) *Local cloud* is administered by internal or external sources explicitly intended for a group or institution [22]. Local cloud is deployed in a local network that coordinates with its remote cloud server to promote data privacy. It is enabled by installing software on the local server that is integrated with the cloud server. However, local cloud is favorable in terms of communication delay but it is subject to some computational limitations due to its sparse resources [23].
3) *Cloudlet* is a small-box data center that is normally deployed at one wireless hop away from mobile devices, such as public places like hospital, shopping center, and office building to facilitate a convenient approach as shown in Fig. 1 [24]. Several units of multicore computers form a cloudlet that is connected to remotely located cloud servers. Cloudlet is brought as a promising solution to overcome the distant wide area network latency and cellular energy consumption problem by utilizing cellular data connectivity to near-located cloud servers [25]. The primary focus of cloudlet is to bring cloud technologies closer to the end-user, providing support to resource- and latency-sensitive applications [26]. Cloudlets utilize technologies, such as WiFi located at one hop or multiple hops away at the edge of the Internet. Therefore, it is dependent on robust and uninterrupted Internet connection. Herein, there are some security and privacy issues that involve the access privacy services, such as e-commerce websites [27].
4) *Fog computing* is also known as edge computing, supporting ubiquitous connected devices. The fog computing term was created by CISCO systems to bring cloud services to the edge of an enterprise network. In fog computing, processing is mainly carried out in the local area network and in an IoT gateway or a fog node. Fog computing offers the benefit to allow single processing devices to gather data from different sensors and act accordingly. For example, a smart robotic vacuum cleaner receives data from multiple sensors installed in a house that are capable to detect any dirt and send appropriate commands to the vacuum cleaner to react accordingly. Fog computing offers much low latency as compared to cloud computing, located far from the end-user. However, fog computing has some limitations due to its dependency on wireless connection which has to be live in order to perform complex actions. Fog computing and MEC terms are widely used interchangeably but they differ in some ways. For example, in a fog computing environment, intelligence is at the local area network level which is processed at the fog node or the IoT gateway [28]. Therefore, there is a rising trend in wireless networks for IoT and M2M communication.

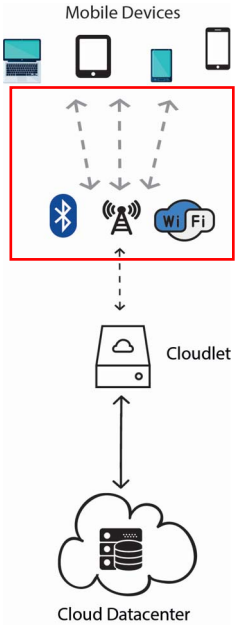



Fig. 1. Cloudlet.

However, in MEC environments, intelligence, communication capability, and processing power are pushed to the RAN, thereby MEC is becoming more popular in 4G and future 5G networks.

### C. Architectures of MEC

MEC functions are mostly found within the RAN, thereby prior to discussing MEC architectures, we need to first understand the history and general architecture of cellular network communication from a RAN perspective.

*1) History and Role of RAN in Cellular Networks:* Back in early 1980s, the first commercial cellular network (1G generation) was introduced with the compliance of analog modulation and mobility support, which later was replaced by 2G because of its digital radio signaling capability using time division multiple access (TDMA). 2G networks were known for better voice quality which was achieved by leveraging digital technology for better voice quality. Later, 3G was released with better data transfer rate and multimedia application coherence using RAN with limited data support [29]. With an accustomed support of mobile Internet using RAN long-term evolution (LTE), 4G got an edge over other wireless mobile telecommunication technologies providing the best user experience [30].

RAN is part of the cellular network communication system infrastructure, facilitating the connection between mobile phones or any wireless controlled machines with the mobile core network [31]. In traditional cellular radio systems, wireless user equipment connect through RAN to the mobile operator networks. User equipment include mobile stations, laptops, etc. RAN covers the wide geographical area divided into several cells and each cell is integrated with its base station. Base stations are typically connected to each other via microwave or landlines to the radio network controller (RNC), which is also known as the base station controller (BSC). RNC

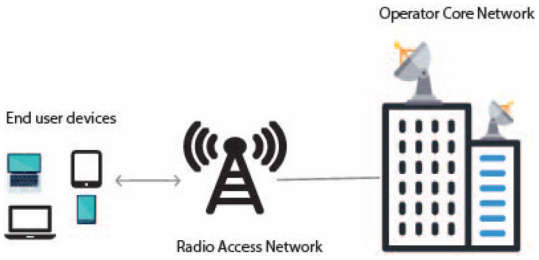



Fig. 2. Cellular architecture.

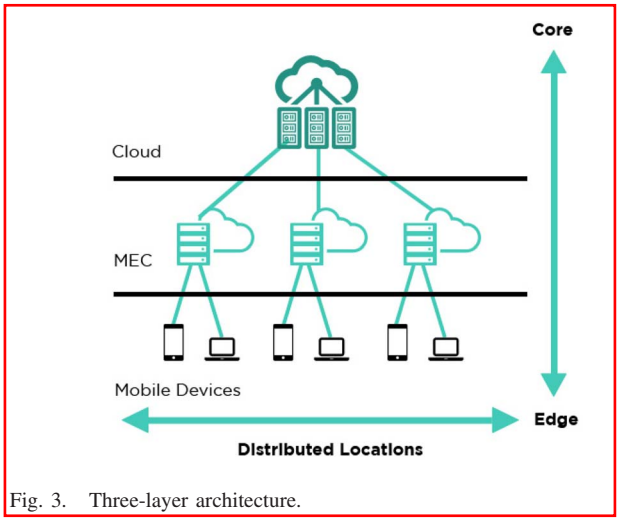



Fig. 3. Three-layer architecture.

is responsible to control the base station node and also carry out some mobile management functions. Most of the encryption is performed before sending user data to the core network. The RNCs are connected with one or two back haul networks. Cellular networks have become more efficient than before because the LTE technology provides high-speed wireless communication RANs with low-latency and high-bandwidth. System architecture evolution (SAE) of RAN LTE core conforms heterogeneous networks and legacy systems, such as air interfaces of GPRS or Universal Mobile Telecommunications (UMTS) [9]. The UMTS is a third generation system that may depend on the global system for mobile communication (GSM) developed in Europe.

The generic view of cellular networks is depicted in Fig. 2, where the core network is wire-connected (e.g., IP/Ethernet) with RAN and RAN is wireless-connected to user devices. RAN connects base station with backhaul network through the Ethernet interface which supports a high data transfer rate [32].

In the past, IP has grown from the Internet, to organization networks and increasingly adopted by the LTE network. The IP traffic between RAN and core is encapsulated with the GPRS tunneling protocol with an IPsec encryption [33]. This has prohibited IT services to be inserted at the nearest location to the end-users. Moreover, mobile operators are reluctant to deploy applications due to the risk of denial of mobile services or performance decrease.

Recently, the concept of cloud RAN (C-RAN) has been proposed by a few operators. C-RAN promises a centralized processing, collaborative radio, real-time cloud computing, and power efficient infrastructure [34]. In particular, it aggregates all base station computational resources into a central pool. In C-RAN, the radio frequency signals from geographically distributed antennas are collected by remote radio heads and transmitted to the cloud through an optical transmission network. Using C-RAN, the number of cell sites will be reduced and the user will be offered better services, while it maintains similar coverage and reduces operating expenses.

*2) Three-Layer Architecture:* MEC is a layer that resides between the cloud and mobile devices. Therefore, the infrastructure is derived as a three-layer hierarchy—the cloud, MEC, and mobile devices [35]. MEC mostly complies with cloud computing to support and enhance performance of the end devices. The formation of a three-layer service model is depicted in Fig. 3.

The general architecture of MEC is depicted in Fig. 4. As shown, different types of mobile devices and sensors in, e.g., IoT, big data, and social platforms, are connected to the core network (i.e., mobile Internet) through the edge network, i.e., the RAN and MEC, and the core network is connected to the private cloud network. With the evolution of LTE-based RAN, it has become more feasible to deploy MEC which brings cloud services near to the mobile subscribers. Therefore, as shown in the architectural model in Fig. 4, each edge platform represents an edge cloud with applications and services specific to the target mobile environment.

MEC constitutes geo-distributed servers or virtual servers with built-in IT services. These servers are implemented locally at mobile user premises, e.g., parks, bus terminals, and shopping centers [35]. MEC may utilize cellular network elements, such as the base station, WiFi access point, or femto access point (i.e., low power cellular base station). MEC may be deployed at a fixed location, for example, in a shopping center or on a mobile device located in any moving object, e.g., car or bus. MEC can be deployed at an LTE base station (eNodeB) or a multitechnology (3G/LTE) cell aggregation site. The multitechnology cell aggregation site can be located both indoor or outdoor. To push intelligence at the base station and to effectively optimize RAN services, MEC technology develops an energetic ecosystem and a new value chain that allows intelligent and smart services at nearby locations to the mobile subscribers.

To summarize, the key value proposition of MEC is that it offers cloud computing by pushing cloud resources, such as compute, network, and storage to the edge of the mobile network in order to fulfil application requirements that are compute hungry (e.g., games applications), latency-sensitive (e.g., AR applications) and high-bandwidth demanding (e.g., mobile big data analytics).

### *D. Advantages of MEC*

As already discussed in the previous sections, there are several benefits associated with MEC which are turning out to be promising for both mobile network operators (MNOs) and application service provider (ASP). In addition, they are beneficial to content providers, over-the-top (OTT) players, network equipment vendors, and middleware

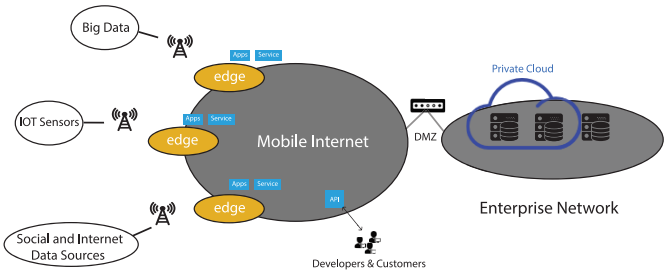



Fig. 4. MEC architecture.

providers [9], [36]. MEC concept focuses on important metrics, such as delay and high-bandwidth that are accomplished by limiting data movement to MEC servers than to centralized servers with severe latency cost. Moreover, power consumption is also one of the main concerns. Computational tasks are migrated to external resource-rich systems to increase the battery lifetime of user equipment. In addition, distributed virtual servers provision scalability and reliability.

With respect to the actors (MNOs, ASPs and end-users), MEC benefits include [9], [37] the following.

1) MNOs could enable RAN access to third party vendors to deploy their applications and services in a more flexible and agile manner. These enabling services could generate revenue by charging based on the services used, such as storage, bandwidth, and other IT resources. OTT services and DVR services offered by cable operators may likely be faster since their services could reside in MEC servers.
2) ASPs could gain profit by an MEC-enabled infrastructure-as-a-service (IaaS) platform at the network edge which makes ASPs services scalable along with high bandwidth and low latency. ASPs could also get real-time access to the radio activity that may develop more capable applications. RAN is revamped into service-aware RAN (SRAN) which provides the location information of the subscriber, cell load, and network congestion.
3) *End-users* could experience fast computational applications through offloading techniques that are handled by MEC servers within RAN. In addition, tight RAN assimilation and physical close servers could improve the user quality of experience (QoE), such as high throughput browsing, video caching, better DNS, etc.

## III. Applications

Although the MEC architecture is a new revenue stream for mobile operators that has not matured sufficiently, we witness a few application areas adopting edge computing (e.g., fog computing) as it has been focused by [15] and [38]. Some recognized applications include AR and content delivery.

### A. Augmented Reality

In the era of mobile technology, AR applications have recently adopted mobile technology, such as Layar, Junaio, Google Goggles, and Wikitude [39]. AR enables real environment user experience by combining real and virtual objects existing simultaneously [40], [41]. Recent AR applications have become adaptive in sound and visual components, such as news, TV programs, sports, object recognition, games, etc. [42]. However, AR systems usually demand high computing power for task offloading, low latency for better QoE, and high bandwidth that is conducive to sustaining interminable IT services.

Edge computing infrastructures have been recognized to be a niche for latency-sensitive applications in the AR domain [43]. They empower AR systems, for example by maximizing throughput by pushing intelligence to the edge of the network instead of relying on the core network. Therefore, offloading computation-intensive tasks at the nearest cloudlet is more optimized and efficient, enhancing user experience.

One example of AR applications is brain computer interaction that works by detecting human brainwaves [38]. The data is received by EEG Bio-sensors in real-time acquiring large computational tasks handled by MEC and cloud computing platforms.

### B. Content Delivery and Caching

The edge computing technology plays a key role in website performance optimization, such as caching HTML content, reorganizing Web layout and resizing Web components. The user makes HTTP requests that pass through the edge server. This server handles user requests by performing number of tasks to load webpages on the user device interface. These requests and responses are time efficient as the edge server is deployed close to the edge devices. The edge computing infrastructure is time efficient as compared to the traditional Internet infrastructures where user requests are handled by the servers that are distantly placed at the service provider side. In addition, edge computing also analyses network performance during on and off peak hours. For example, under congested network conditions where several users are streaming video at the same time, the graphics resolution is decreased to minimal to accommodate every user averting any denial of service (DOS) or jitter.

## IV. Emerging Application Scenarios

It is important to stay ahead of the curve to apprehend mobile technology trends. In this section, emerging application scenarios of MEC are presented which are recently discussed in the ETSI white paper [15], such as video analytics and mobile big data. Several research papers [10], [18], [44], [45] have referred to MEC scenarios in connected vehicles, smart grid and wireless sensor and actuator networks (WSANs). Furthermore, in [46], the application area is expanded to smart building control and software-defined network (SDN), as well as to ocean monitoring [47].

### A. Healthcare

Science and technology in health domain is a substantial research area for many researchers [48]. Like other industries, healthcare can also be aided by edge computing, e.g.,

patients suffering from strokes fall. According to the stroke statistics, someone in the U.S. has a stroke about once every 40 s [49]. Falls are common among stroke patients who suffer mostly from hypoglycemia, hypotension, muscle weakness, etc. According to recent research, one third of the strokes could possibly be averted by early mitigating the fall incidents [50]. In order to detect and prevent fall, a large body of research has been carried out, for example, by introducing human computer interaction devices, such as smartphone, smart watch, and Google glass, but certain limitations still exist.

Recently, researchers have proposed a smart healthcare infrastructure called U-fall, that exploits smartphones by engaging edge computing technology. U-fall is based on a fall detection algorithm that is designed using acceleration magnitude values and nonlinear time series analysis [38], [48]. U-fall senses motion detection with the help of smart device sensors, such as gyroscopes and accelerometers. U-fall intelligently maintains integrity between the smartphone and the cloud server to ensure real-time detection. In addition, the proposed infrastructure is capable to deliver accurate results which make it more reliable and dependable.

Furthermore, the three-tier architecture that includes role model, layered-cloud architecture, and MEC can help health advisers to assist their patients, independent of their geographical location. MEC enables smartphones to collect patient physiological information, e.g., pulse rate, body temperature, etc., from smart sensors and send it to the cloud server for storage, data sync, and sharing. Health advisers having access to the cloud server can immediately diagnose patients and assist them accordingly [51].

### *B. Video Analytics*

Surveillance cameras in old times were used to stream data back to the main server and then the server decided how to perform data management. Due to the growing ubiquity of surveillance cameras, the traditional client-server architecture might not be able to stream video coming from million of devices and therefore, it will stress the network. In this scenario, MEC will be beneficial by implementing intelligence at the device itself which is programmed to send data to the network, when there is a motion detection. In addition, MEC-enabled surveillance cameras can be beneficial for several applications, such as traffic management applications which can detect traffic jam or an accident on the basis of traffic patterns. The application can also be helpful for face recognition, for example, if someone commits a crime then his photograph can be transferred to these intelligent cameras to trace the culprit [52], [53].

### *C. Mobile Big Data Analytics*

Mobile phone technology is valued a growth-engine for small, medium and large enterprises, and also has widespread social connotation. The ubiquity of mobile phones and their big data coming from applications and sensors, such as GPS, accelerometer, gyroscope, microphone, camera, and bluetooth are stressing the network bandwidth [54]. Big data consists of large and complex data sets that is generated by data processing applications, sensors, devices, video, and audio channels, and Web and social media [55], [56]. These data sets may be structured or nonstructured and may not be possible to process them by a single machine [57]. Big data is of paramount importance to businesses because it extracts analytics and useful information that may benefit to different business segments [58]. Big data analytics is a process of extracting meaningful information from raw data which could be helpful for marketing and targeted advertising, customer relations, business intelligence, context-aware computing, health care, etc. [59], [60].

Implementing MEC near the mobile devices can elevate big data analytics with the help of network high bandwidth and low latency. For example, instead of using the typical path from an edge device to the core network, big data can be collected and analyzed at the nearest MEC environment. The result of big data analytics can then be passed to the core network for further processing. This scenario will perhaps also accommodate data coming from several IoT devices for big data analytics [61].

### *D. Connected Vehicles*

Vehicles are facilitated with an Internet access that allows them to connect with other vehicles on the road. The connection scenario can either be vehicle-to-vehicle, vehicle to access point or access point to access point. Deploying MEC environments along side the road can enable two-way communication between the moving vehicles. One vehicle can communicate with the other approaching vehicles and inform them with any expected risk or traffic jam, and the presence of any pedestrians and bikers. In addition, MEC enables scalable, reliable, and distributed environments that are synced with the local sensors [62].

### *E. Smart Grid*

A smart grid infrastructure is an electrical grid that consists of several components, such as smart appliances, renewable energy resources, and energy efficiency resources. Smart meters that are distributed over the network are used to receive and transmit measurements of the energy consumption [63]. All the information collected by the smart meter is supervised in supervisory control and data acquisition (SCADA) systems that maintain and stabilize the power grid. Moreover, distributed smart meters and micro grids, integrated with MEC, can support SCADA systems. For example, in this scenario, MEC will balance and scale the load according to the information shared by other micro grids and smart meters.

### *F. Wireless Sensor and Actuator Networks*

WSANs are sensors that are used for surveillance, tracking, and monitoring of physical or environment situations, e.g., light intensity, air pressure, and temperature [64]. MEC-enabled actuators autonomously manage measurement process by developing an active feedback loop system. For example, air vent sensors manage air pressure flowing in and out of the mine to save miners from any emergency. These sensors

consume very less energy and bandwidth with the help of MEC.

### G. Smart Building Control

Smart building control systems consist of wireless sensors that are deployed in different parts of buildings. Sensors are responsible for monitoring and controlling building environments, such as temperature, gas level or humidity. In a smart building environment, sensors installed with MEC become capable of sharing information and become reactive to any abnormal situation. These sensors can maintain building atmosphere on the basis of collective information received from other wireless nodes. For example, if humidity is detected in the building, MEC can react and perform actions to increase air in the building and blow out the moisture.

### H. SDNs

SDN are an innovation to computer networking that separates control layer and the data layer [65]. Data layer contains user-generated messages and is responsible to forward them using the forwarding tables prepared by the control layer [66]. This is managed by a centralized control system. The MEC concept along with SDN can make centralized control more efficient and reliable, e.g., in vehicle-to-vehicle connectivity the ratio of packet loss can be resolved.

### I. Ocean Monitoring

Scientists are researching to cope with any ocean cataclysmic incidents and know the climate changes in advance. This can help to react quickly and mitigate to prevent any disastrous situation. Sensors deployed at some locations in the ocean transmit data in great quantity which requires large computational resources [47]. The data handled by the cloud may introduce delays in the transmission of live forecast. In this scenario, MEC can play a vital role to prevent any data loss or delay in sensor data transmission.

## V. State-of-the-Art Related Research

In this section, we present several research efforts carried out in the area of MEC recently.

### A. Computational Offloading

In computer science, computation offloading is the process of migrating computing tasks to external sources, such as clouds, grids, or clusters [67]. Computation offloading is a solution to enhance the capacity of mobile devices by transferring computation to higher resourceful servers that are located at a different location [68]. The emergence of resource-demanding applications, such as 3-D games will continue to demand more mobile resources. Improvement of mobile devices and networks will still not be able to cope up with the trend in demand. Therefore, mobile devices will always have to compromise with their limited resources, such as resource-poor hardware, insecure connections and energy-driven computing tasks [69]. For example, editing video clips on a mobile phone requires a large amount of energy and computation which is provided with some limitations as compared to desktop or laptop. To deal with these constraints, many researchers have studied computation offloading to resource-rich platforms, such as the cloud [70]–[72].

In 2015, Takahashi *et al.* [73] proposed edge accelerated Web browsing (EAB) prototype designed for Web application execution using a better offloading technique. The purpose of EAB is to improve user experience by pushing application offloading to the edge server which is implemented within the RAN. EAB-frontend at the client-side retrieves the rendered Web content which is processed in the EAB server, whereas, audio and video streams travel through the EAB-backend and are decoded depending on the capabilities of the client hardware.

In 2016, Chen *et al.* [74] designed an efficient computation offloading model using a game theoretic approach in a distributed manner. Game theory is a persuasive tool that helps simultaneously connected users to make the correct decision when connecting a wireless channel based on the strategic interactions. If all user devices offload computation activities using the same wireless channel, it might cause signal interference with each other and wireless quality reduction. Specifically, the game theory targets the NP-hard problem of computation offloading incurred by multiuser computation offloading and provides a solution by attaining Nash equilibrium of multiuser computation offloading game.

In 2015, Sardellitti *et al.* [75] proposed an algorithm-based design, called successive convex approximation (SCA). This algorithm optimizes computational offloading across densely deployed multiple radio access points. The authors considered the MIMO multicell communication system where several mobile users request for their computational tasks to be carried at the central cloud server. They first tested a single user offloading computational task on the cloud server which resulted in the nonconvex optimization problem. In the multiuser scenario, the SCA-based algorithm attained local optimal solution of the original nonconvex problem. According to the formulation results, authors claimed their algorithms to be surpassed disjoint optimization schemes. Moreover, they stated that the proposed SCA design is more suitable for applications acquiring high computational tasks and minimizes energy consumption.

In 2016, Zhang *et al.* [76] proposed the contract-based computation resource allocation scheme. This scheme improves the utility of vehicular terminals which intelligently utilize services offered by MEC service providers under low computational conditions. The MEC provider receives the payment from vehicles on the basis of the computation task they offloaded to the MEC servers. Using a wireless communication service, information of the contract and payment information is broadcasted to the vehicles on the road.

In 2015, Habak *et al.* [77] proposed the femto-cloud system which forms a cloud of orchestrated co-located mobile devices that are self-configurable into a correlative mobile cloud system. A femto-cloud client computing service is installed on each mobile device to calculate device computing capability and capacity for sharing with other mobile devices, and energy information. Mobile properties are built and maintained inside

a user profile that is shared in a mobile cluster connected to a cloudlet or a control device that is available in a WiFi network. Intensive computational tasks in the form of codes are sent to cloudlets to leverage the computational capacity of other connected mobile devices. The femto-cloud model is designed to reduce the computational load from the centralized location and bring it to the edge of the mobile network.

### B. Low Latency

MEC is one of the promising edge technologies that improves user experience by providing high bandwidth and low latency.

In 2016, Abdelwahab *et al.* [78] proposed REPLISOM which is a edge cloud architecture and LTE enhanced memory replication protocol to avoid latency issues. LTE bottleneck occurs due to allocating memory to a large number of IoT devices in the backend cloud servers. These devices offload computational tasks by replicating and transmitting tiny memory objects to a central cloud which makes IoT to be scalable and elastic. The LTE-integrated edge cloud provides its compute and storage resources at the edge to resource-intensive services. Thus, the proposed REPLISOM reduces the stress of LTE by intelligently scheduling memory replication events at the LTE-edge to resolve any conflicts during the memory replication process for the radio resources.

In 2015, Nunna *et al.* [79] proposed a real-time context-aware collaboration system by combining MEC with 5G networks. By integrating MEC and 5G, it empowers real-time collaboration systems utilizing context-aware application platforms. These systems require context information combined with geographical information and low latency communication. The 4G network might not be capable to fulfill such requirements, instead 5G networks and MEC are proficient to utilize contextual information to provide real-time collaboration. The above suggested model is beneficial for scenarios such as life remote robotic tele-surgery and road accident that demand high bandwidth and ultralow latency.

In 2016, Kumar *et al.* [80] proposed a vehicular delay-tolerant network (VDTN)-based smart grid data management scheme. The authors investigated the use of VDTNs to transmit data to multiple smart grid devices exploring the MEC environment. With the use of a store-and-carry forward mechanism for message transmission, the possible network bottleneck and data latency is avoided. Due to the high mobility of vehicles, a smart grid environment supported by MEC is used to monitor large data sets transmitted by several smart devices. According to the data movement, these devices make computation charging and discharging decisions with respect to message transmission delay, response time and high network throughput for movable vehicles.

### C. Storage

Limited storage resources of end devices tend to affect user experience. End-users may utilize MEC resources to overcome their device storage limitation.

In 2016, Jararweh *et al.* [12] proposed a software defined system for MEC (SDMEC). The proposed framework connects software defined system components to MEC to further extend MCC capabilities. The components jointly work cohesively to enhance MCC into the MEC services. Working with SDN, software defined compute (SDCompute), software defined storage (SDStorage), and software defined security (SDSec) are the prime focus of the proposed framework which enables applications requiring compute and storage resources. Applications like traffic monitoring, content sharing, and mobile gaming will benefit from SDMEC.

### D. Energy Efficiency

As previously mentioned, the MEC architecture is designed to reduce energy consumption of user devices by migrating compute intensive tasks to the edge of the network.

In 2014, Gao [81] proposed a opportunistic peer-to-peer MCC framework. The probabilistic framework is comprised of peer mobile devices that are connected via their short-range radios. These mobile devices are enabled to share both energy and computational resources depending on their available capacity. He proposed the probabilistic method to estimate the opportunistic network transmission status and ensure the resultant computation is timely delivered to its initiator. The purpose of the proposed framework is to facilitate warfighters at the tactical edge in a war zone. This framework is beneficial for situation awareness or surrounded ground environment understanding, with the help of data processed by *in-situ* (on site) sensors. The preambled novel framework thus efficiently shares computational tasks by migrating workloads among warfighters mobile hand held devices, perhaps taking an account of timeliness of computational workload for successive resultant migration.

In 2015, Beck *et al.* [82] proposed ME-VoLTE, which is an architecture that integrates MEC to voice over LTE. The encoding of video calls is offloaded to the MEC server located at the base station (eNodeB). The offloading of video encoding through external services helps escalating battery lifetime of the user equipment. Encoding is high computational-intensive and hence is very power consuming. In the proposed system, encoding techniques are wisely used to stream video on the MEC server. MEC transcodes video by using a special codec program before responding to the user device request. This phenomenon significantly increases data transmission and enhances power management.

In 2015, El-Barbary *et al.* [25] proposed DroidCloudlet which is based on commodity mobile devices. DroidCloudlet is legitimized with resource-rich mobile devices that take the load of resource-constraint mobile devices. The purpose of the proposed architecture is to enhance mobile battery lifetime by migrating data-intensive and compute-intensive tasks to rich-media. DroidCloudlet works as a client device or as a server device running an application that supplements resource-poor devices by offering their available resources. One of the devices takes the role of an agent which is responsible for coordinating resources with other groups of devices.

In 2016, Jalali *et al.* [83] proposed a flow-based and time-based energy consumption model. They conducted number of experiments for efficient energy consumption using centralized nano data centers (nDCs) in a cloud computing environment. The authors claim that nDCs energy consumption is not yet been investigated. Therefore, several models were presented to perform energy consumption tests on both shared and unshared network equipment. In this paper, it concludes that nDCs may lead to energy savings if the applications, especially IoT applications generate and process data within user premises.

### E. Summary

In this section, we presented the relevant state-of-the-art research results in the MEC area. Among the discussed research focuses, *computational offloading*, *low latency*, and *energy efficiency* have received more attention by the MEC community. Considering the former, two predominant categories of approaches have been proposed to enable computational offloading in MEC network models.

1) Algorithmic solutions such as those based on the game theory and SCA [74], [75].
2) Network architecture-based solutions, such as cloud of co-located mobile devices [77].

With respect to low latency, early approaches basically rely on the wireless network technologies for latency reduction, e.g., through integrating MEC systems with LTE or 5G. Recently, domain-specific network technologies such as VDTNs have been used to mitigate the latency in MEC systems. The state-of-the-art in MEC-based energy efficiency is, in most cases, addressed indirectly through computational offloading mechanisms, such as in [25] and [82]. Other existing approaches have attempted to address this issue through proprietary network architectures, such as peer-to-peer mobile networks [81] and centralized nDCs [83].

## VI. Research on Infrastructure

There are a few contributions on the MEC infrastructure which has been partly discussed in [15] and [17]. In this section, we explore existing MEC infrastructures with respect to their deployment scenarios and developed test beds.

### A. Deployment Scenarios

As mentioned earlier, MEC can be flexibly and intelligently deployed at different sites, including UMTS RAN (UTRAN), LTE E-UTRAN Node B, 3G RNC and multiradio access technology. An MEC deployment may use the shared or dedicated network functions virtualization architecture.

According to the first release of MEC by Industry Specification Group (ISG), the implementation scenarios can either be at the outdoor environment, such as LTE and 3G sites or the indoor environment, such as shopping malls and hospitals.

1) *MEC in Outdoor Scenarios:* Several ways are possible to implement MEC in outdoor scenarios, for example, macro cells vendors insert virtualization environment into a RAN. This scenario helps operators to deliver network features with high value services. Moreover, it improves QoE by providing low latency, pushes more intelligence to the edge and provides better computation offloading. The infrastructure where MEC is closely integrated with RAN, gives a better network traffic analysis, radio network status, and device location services.
2) *MEC in Indoor Scenarios:* In WiFi or 3G/4G access points, MEC can be deployed through light weight virtualization. Its deployment in M2M environments can monitor temperature, humidity, air conditioning, etc. with the help of connected sensors at various indoor locations. MEC can also be beneficial in case of any emergency situation, such as in any hazardous situation in a residential building environment where it can help people to evacuate the building with the help of AR services.

### B. MEC Testbeds

This section lists some recent testbeds that are developed and tested by implementing MEC platforms.

*1) 5th Generation Test Network:* The 5th generation test network (5GTN) architecture was developed and successfully tested at Oulu, Finland, which is based on LTE and LTE-advanced technology [84]. It opens an opportunity for application developers to develop their applications in a test environment before they are brought to the market. The introduced testbed is composed of different environments, one is located at the Technical Research Centre of Finland (VTT's) 5G laboratory and the other one is at the University of Oulu's Centre for Wireless Communications (CWC). The CWC network is opened for public users, whereas VTT's network is in a more secured and private environment. Both networks are integrated with the help of carrier-grade technology offering a real-time environment. The private network is connected to 5G test laboratories located in different parts of Europe. The purpose is to stretch 5G network functionality. The CWC network was targeted for any mobile user of any mobile operator. The key purpose is to give access to the university students and visitors with high-nature 5G experience. MEC functionality is based on a Nokia provided solution that is operative in an AirFrame cloud environment and can be tested in the 5GTN architecture. It will allow the third-parties service providers to test their applications in an MEC-5G.

*2) Industrial Testbeds:* Nokia and China mobile successfully tested advance mobile solutions for utmost mobile data capacity and real-time video [85]. The testbed was deployed in a car race stadium where 11 707 active users were simultaneously connected with small cells and 6195 users with macro cells. In total, 95 LTE small cells were installed having 2.6 TDD, 2.3 TDD, and 1.8 FDD specifications at the ultradense distance of 10–15 m. The platform was built for MEC with airframe radio cloud platform for MEC and Airscale WiFi with flexi zone controllers. The system successfully delivered high performance HD videos on user mobile panels offering multiscreen view. Similarly, another testbed application was created by Nokia and Chunghwa Telecom implemented at a baseball stadium which gives a live TV coverage like view

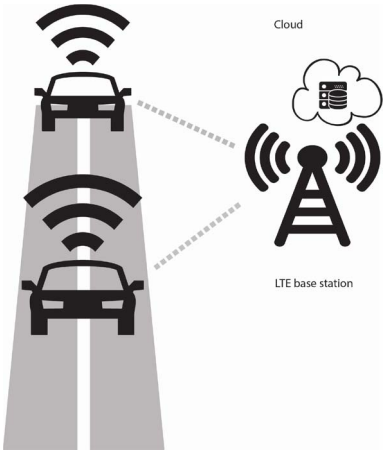



Fig. 5. Vehicular communication system.

and live experience of match atmosphere simultaneous at the same time [86]. The MEC environment was created with the help of Nokia Flexi Zone base stations that use 30 MHz of LTE spectrum. Spectators are able to see four video feeds at the same time that are on a split mobile screen. MEC offers ultralow latency which is required for live video streaming by moving compute power to process the videos at the nearest place to the subscribers.

Nokia and its partners delivered an intelligent car-to-car infrastructure communication system using operators live LTE network [87]. Vehicles connection is facilitated by different cloudlets deployed on the Nokia MEC platform at mobile base stations as shown in Fig. 5. These cloudlets were able to deliver end-to-end latency below 20 ms. First tested use case was emergency brake or slowing down car prior to any upcoming emergency. Vehicles can communicate almost in real-time with the vehicles that are even beyond sight. The second tested use case was cooperative passing assistant that also utilizes cloudlets deployed at the LTE base stations. Vehicles changing lanes are alarmed with the critical distance between them. On the basis of distance and car velocity, the situation is computed by the cloudlets and later signaled to vehicles with guidance of possible actions to avoid any risks.

## VII. Security and Privacy Issues

This section studies security and privacy issues in the context of different architectural elements of MEC [13], [88]–[90].

### A. Security Concerns

The components of CIA triad, confidentiality, integrity, and availability makeup a model design for information security [91]. There are several aspects of trust that need considerations in the MEC infrastructure.

1) *Confidentiality:* There are several applications hosted at the edge of the network providing their services to mobile users, e.g., location-awareness. In spite of the fact that these applications are beneficial but they also pose confidential risks. For example, at the application layer there is no rule defined to separate user identity from its geo-location [92]. Therefore, new protocols are required to be preambled. The user information is vulnerable between MEC and cloud communication channels. Intercepting the communication stream, such as packet sniffing, will exploit location-based attacks on end devices.
2) *Integrity:* The MEC ecosystem incorporates multiple actors, such as end-users, service providers, and infrastructure providers [13]. This causes several security challenges. Cloud servers efficiently enable compute nodes to authenticate them to administrative servers in data centers due to isolated environments but is less suitable in an open environment. For example, MEC nodes under a multimanagement domain will be difficult to share their identification with cloud servers. This scenario can cause several attacks, such as man-in-the-middle attack in which the attacker can authenticate themselves to the central cloud systems and later with end devices to steal their secret information.
3) *Availability:* Due to less isolated environment, MEC system may suffer DOS attacks that could be application- or packet-based [17]. On a single node, these attacks might not be much hazardous but if the correlative attacks occur simultaneously at multiple geo-locations, it can lead to serious implications. For example, compromised sensors in the industrial sector will make a ripple effect globally. Such attacks are difficult to mitigate, as MEC systems are directly connected to the end devices and there is no way of detecting malicious network activity.

*1) Network Security:* As the preponderance of various communication networks, such as mobile core networks or wireless networks, network security is a very important element in MEC environments. In the traditional network security environment, the network administrator defines network security policies which isolate network traffic. However, the deployment of MEC at the Internet edge, stresses the network management policy which may be vulnerable to various attacks, such as DOS which may damage MEC and cause useless heavy network traffic. This kind of attack is limited to MEC nodes and not much effective to the back-haul network since the back-haul network is more secured. Attackers can also launch traffic injection or eavesdropping attacks that can takeover the network or a quantum of a network. Hackers hijacking the network stream can launch attacks to affect MEC system performance. Man-in-the-middle attack is likely to be effective when intercepting data communication. Attackers can successfully manipulate the data traveling from the cloud to the user and vice versa. It is difficult to mitigate such attacks because deploying and dropping virtual machines make it cumbersome to maintain the blacklist. Han *et al.* [93] proposed a measurement-based approach to prevent user connection with rogue gateways by observing the round-trip time between the user and the DNS server.

*2) Core Network Security:* It should be noted that all edge paradigms may be supported by the core network and most of the core network security is enabled by mobile core networks or a central cloud. The security of cloud services is mostly managed by third party suppliers, such as Amazon, Microsoft,

and Google. However, it is not possible to completely rely on their security mechanisms. In addition, there is a high risk for user's personal and sensitive information which can be stolen by malicious entities. Edge devices exchange information with each other and may bypass the central system's security mechanism. This makes security vulnerable and hackable. This type of security issue will not affect the whole ecosystem and will be limited due to its decentralized nature. There is also a possibility of the system data to be changed and provide false information, if the services are hijacked. The level of this effect will be limited but may cause DOSs. If the core infrastructure is compromised then it can sabotage some elements of the core system. Core network elements that are compromised can disrupt the lower level infrastructure. Attackers may have full access to the information and may tamper the network data flow.

*3) MEC Server Security:* MEC at the edge comprises of several virtualized servers providing intelligent IT services. However, these services are liable to external security threats, for example, physical access to the data center is less protected or guarded. Attackers breaching security channels can physically damage IT resources. This particular attack is limited to a specific geographical location and may not be very critical. Moreover, stream of information to and from the local scope of data center can be stolen from malicious actors, such as users and ASPs. In addition, design flaws, configuration errors, insufficient security training or abusing one's own privileges may be an alarming risk to the security of data center systems. Being newly preambled in the technology world, MEC lacks some security expertise for adequate system security. Once the login access has been granted to the MEC system resources, the attacker can abuse system integrity or can execute DOS attacks, man-in-the-middle attacks, etc. The services are discontinued or interrupted as a result of such security breaches. Another security issue is the compromise of an entire data center. In this type of attack, the whole data center is hijacked through a single or a combination of different attacks. The attacks might be privilege escalation or a fake infrastructure. A compromised data center has a large impact over geographical locations which may result in high scale damage.

*4) Virtualization Security:* In core mobile edge data centers, several network instances co-exist sharing network instances. If one resource is compromised, it can affect the whole virtualized infrastructure. An attacker may misuse and exploit system resources that have been conceded. DOS attacks are most likely to happen. MEC virtualized systems can completely drain the resources that serve computational, storage, and network tasks. Users connecting to MEC virtual servers may face denial of requests and DOSs. Furthermore, malicious antagonists can misuse virtual resources and not only affect the system itself but also IoT devices that are connected to it. For instance, any IoT device that is in the range of the radio network and is vulnerable can be hacked and sabotaged. One of the common security concerns is privacy leakage. Several APIs implemented in the MEC environment are responsible to deliver information of the physical and logical infrastructure. However, these APIs are most likely to be less protected against any malevolent activity. Several attacks can be escalated, e.g., malicious virtual machines hosted in a data center can advance to other virtual machines or other data centers. Users moving across different geographical locations can escalate such attacks to other MEC virtualized servers. The virtual machine itself, affected by an attacker, can become a hostile and launch attacks on other virtual machines hosted on the same system.

*5) End Devices Security:* End-user devices can potentially be harmful to affect some elements of the ecosystem. However, the impact could be narrow due to limited user device surroundings. User devices act as a carrier in a distributed environment. In addition, there could be rogue users that can intrude the system and perform some malicious activities. For example, they can inject false values or information to the system. A device can be reconfigured and set to send fake information, such as wrong surveillance camera information or incorrect data announcements by vehicles. Moreover, there are some scenarios where devices can participate in service manipulation. For example, any compromised device connected in a cluster environment can change and control services in that cluster.

### *B. Security Mechanisms*

Security breaches may cause potential harmful problems within the system. Therefore, it is very important to implement appropriate security mechanisms and safeguard the MEC resources from any intrusion. In this section, we present existing security mechanisms for MEC.

*1) Identification and Authentication:* In a cloud computing environment, data centers are mostly hosted by cloud service providers, whereas in all edge paradigms, providers may be hosted by several providers depending on their choices. For example, cloud service providers may extend their IT services to the edge using existing infrastructures. MEC resource providers may differ with the extended cloud infrastructure and the end-user may want to use limited cloud resources depending on their budget and lease their resources in the local cloud. In order to integrate all these services, proper identification and authentication is required. Every entity in the ecosystem, such as end devices, virtual machine services, the cloud and MEC infrastructure service providers, and ASPs should be able to identify and mutually authenticate each other.

In [94], a user-friendly solution is introduced to provide a secure authentication in a local ad-hoc wireless network. The connected devices share only limited public information that enables them to exchange authenticated key protocols. Similarly, NFC also enables a secure authentication method in a cloudlet scenario [95]. NFC applications based on cloudlets enable authentication by NFC-equipped end devices. Moreover, it is also of prime importance to have a continuous connectivity of user devices with their respected cloud servers. Stand-alone authentication is introduced for a scenario if there is temporary disconnection between MEC and the cloud server [89]. If the connection is fragile then stand-alone authentication would be able to authenticate users with the cloud servers. With the evolution of biometric authentication, such as face recognition, eye recognition, and finger print,

it will be very helpful to introduce biometric authentication systems in MEC.

*2) Network Security Mechanisms:* Network security is one of the prime concern for the MEC concept due to the predominance of the network infrastructure. Attackers are involved more in launching attacks, such as man-in-the-middle and DOS to sabotage the network environment. Thus, it is very crucial to deploy a comprehensive security mechanism. Intrusion detection and prevention is an important prerequisite before designing the MEC infrastructure. Several network entities could be vulnerable to any threats, hence these entities should be monitored from internal or external threats. In such cases, the edge infrastructure should be in charge of monitoring its network and equally coordinate with surrounded and core networks. Intrusion detection systems (IDSs) can be employed in the MEC data center to monitor and analyze system logs for any unauthorized access. It can also be employed at the MEC network side to detect and prevent the network from any attacks, such as man-in-the-middle attack, DOS, and port scanning. A Cloudlet that is located at one hop away from mobile devices can efficiently be meshed to form a security framework to detect any intrusion [96]. Cloudlets can serve as a proxy for distant cloud servers in case of any unavailability issue due to certain attacks. Moreover, by implementing SDN, it is easy to reduce network cost and scale network resources. SDN can isolate network traffic and segregate malicious data. A proposed access control scheme based on OpenFlow is useful for multiple security requirements [97]. For example, having direct access to the network components will make it easier to monitor and detect any abnormal activity in the network traffic.

*3) Virtualization Security Mechanisms:* Virtualization technology is one of the foundation for the edge paradigm and thus it is of paramount importance to be secured. Malicious elements that get access to virtual servers may hijack the entire edge data center. Virtualized servers and their hosted physical servers can be protected through hypervisor hardening, network abstractions, and isolation policies [98].

*4) Data Security:* In an edge paradigm, user data is outsourced to the MEC server that gives access control to mobile users. This introduces some challenges, such as data integrity and authorization, for example, outsourced data can be modified or disappeared, and uploaded data can be accessed for malicious activity. Moreover, data owners and data servers possess dissimilar identities and business interests that make the scenario more vulnerable. Appropriate auditing methods can be used to audit data storage to confirm that data is properly resided in the cloud [99].

*5) Data Computation Security:* Securing data computation is another important issue that has to be addressed. There are two major aspects to secure any computation that is outsourced, including computation verification and data encryption. Verifiable computing allows the computing node to offload some functions to other servers that could not be trusted, but it enables the maintenance of the results that are verifiable. Other servers perform a check on the given function and confirm the correctness of computation. There should be a mechanism through which the user is allowed to verify computational accuracy. In [100], a verifiable computing protocol is proposed to return a computational-sound, noninteractive proof. Data encryption is another security mechanism. The data that is sent from user devices need to be protected and encrypted before outsourced to MEC servers. One of the popular services is keyword search which means to search keywords from encrypted data files. In [101], a statistical measuring approach is proposed to search through a secured searchable index. The index is secured through a one-to-many order-preserving mapping approach.

### C. Privacy Issues

Due to close proximity to the end-user, privacy preserving, such as data, usage, and location may be challenging in MEC. User privacy breaches may become worse if the attacker gains personal information, such as the credit card information, personal emails, etc. Data privacy or information privacy of the user have a risk of being accessed. It could be even worse if the attacker gets access to the user's sensitive information.

Aggregation schemes, such as homomorphic encryption can enable privacy-preserving aggregation at gateways to secure user information [102]. An attacker may retrieve user information by learning the usage pattern of the user device while accessing MEC. For example, in a home smart-grid environment, meter reading, such as the presence and absence of the user at home and user in-house behavior can help the attacker to perform any malicious or criminal activities. Nonintrusive load leveling (NILL) has been introduced to encounter these types of issues [103]. However, it cannot be implemented in MEC environments due to untrusted third parties, e.g., the lack of a duplicate battery to perform NILL. One possible way to counter this kind of privacy is creating dummy tasks and performing multiple offloadings to different locations. This can therefore hide the original tasks by hiding behind these fake ones.

Another privacy issue is the user location. The global positioning system (GPS) is very useful for users to benefit from geo-location services. Mobile users use location-based services for GPS navigation. However, such services endure certain privacy issues, for example, users who share their location information with location-based services. The user device connected to the nearest MEC will give an indication to the attacker that which MEC location the compute device is near to, as shown in Fig. 6. In order to secure location information, there are several ways to confuse the attacker. For example, the MobiShare system is a flexible and secure mechanism for sharing geo-location information and it has a good support for location-based applications [104].

Moreover, the edge paradigm in general, and MEC in particular can be used to improve the privacy level of certain services, such as crowd sourcing. The state-of-the-art privacy solutions are not particularly suitable for crowd sourced location-based services. Abdo *et al.* [105] proposed a solution to deploy a crowd-sourcing platform in a trusted edge data center to protect the anonymity of the participants of certain location-based services.

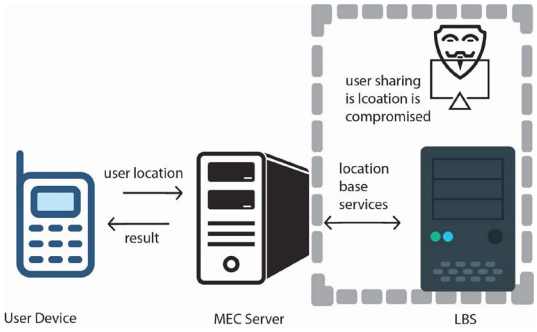



Fig. 6. Architecture of location sharing.

## VIII. Other Open Issues

As a recent technology platform, not much research has been specifically advocated to MEC. There are some issues in MEC that need to be addressed before its commercial deployments. This section discusses and identifies the open issues that are investigated by different researchers in the development of MEC.

### A. Security

Security is one of the main concerns for technology advisers to secure MEC deployments. There are some security mechanisms that are applicable to MEC, as discussed in the previous section. However, there are still some issues that need proper research studies. For example, computational-intensive applications outsource their computation to MEC servers. Computation tasks are performed through wireless medium opening up the risk of intrusion. Moreover, different users connected to the common physical server also raise security issues [106]. The application data movement is possible through encryption and decryption strategies but it affects application performance.

### B. Resource Optimization

Promoting cloud infrastructures to the network edge, MEC incorporates less resources than the cloud. Computational offloading is supported by applications and virtualized MEC servers. However, computational tasks carry extra overload due to heterogeneous processor architectures. For example, mobile smart phones have mostly ARM and x86 architectures, hence they need translation or emulation [107]. Therefore, an optimized solution for enhancing performance of intrinsic limited resources is required [108].

### C. Transparent Application Migration

As mentioned previously, user applications are transported to MEC servers for execution. It is very vital to transparently migrate these applications for usability of delay-sensitive mobile applications, such as real-time applications [109]. Poor compute performance and delay in service provisioning deteriorate the emergence of mobile applications [110]. Application migration is a software level solution that can be achieved by proposing solutions to optimize cloud resources utilization at the edge [111].

### D. Pricing

MEC environments involve several actors that quote different prices for their services. These actors have different payment methods, different customer management models, and different business policies. Therefore, it raises several questions: 1) what will be the mutually agreed price; 2) what will be the mode of payment; and 3) who will process customer payment. For example, a game application on the user device has to utilize cloud resources, the mobile network and game services. The user has to pay for the game which should be divided equally or as per mutual contract to all the entities involved. This can be argued that agreeing to the pricing may be difficult among different entities.

### E. Web Interface

Currently, the interface used to access MEC and the cloud is the Web interface which is not sufficient for user experience. The Web interface is generally not designed for mobile devices and hence have compatibility issues. Generally, Web interfaces are not suitable for MEC due to their overhead problem. Therefore, standard protocols are required for smooth communication between the user, MEC and the cloud. The latest version of HTML5 is designed specifically for advanced devices, such as mobile or smart phones. However, performance and test-based research is needed to make HTML5 ready for MEC.

### F. Other Issues

Many issues are already discussed in the previous sections, but in addition, there are some other issues which are also vital to strengthen the MEC framework. A comprehensive scientific research study is required to avoid any security issues that can damage the system.

1) *Openness of the Network:* Mobile networks have complete authority over the network but in the case of MEC it will be very crucial to open the network for third party vendors due to possible security risks.
2) *Multiservices and Operations:* ASPs, OTT, network vendors, and content providers require access to MEC data centers. This scenario causes complexity for seamless integration with third-party services.
3) *Robustness and Resilience:* Deploying resources at MEC is very important to enable robustness of MEC servers.
4) *Security and Privacy:* User privacy and its data security may be exposed while integrating mobile services with MEC. Prior to the MEC deployment, there should be an assurance that the infrastructure is well protected.

## IX. Conclusion

MEC has a great potential to be the future edge technology offering bandwidth, battery life and storage to the resource-constraint mobile devices. MEC trends to provide elastic resources at the end of the network toward applications demanding computational-intensive tasks with high bandwidth and ultralow latency, especially in 5G networks. MEC deployment can build an ecosystem involving third-party partners, content providers, application developers, OTT players, network vendors, and multiple mobile operators. This

paper has presented a thorough study on the recent research and technological development in the area of MEC and its application domains, research challenges, and open issues.

## REFERENCES


[1] E. Cau *et al.*, "Efficient exploitation of mobile edge computing for virtualized 5G in EPC architectures," in *Proc. 4th IEEE Int. Conf. Mobile Cloud Comput. Services Eng. (MobileCloud)*, Oxford, U.K., Mar. 2016, pp. 100–109.

[2] Cisco Systems. *Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2015–2020 White Paper*. Accessed: Aug. 22, 2016. [Online]. Available: http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.html

[3] G. Orsini, D. Bade, and W. Lamersdorf, "Computing at the mobile edge: Designing elastic android applications for computation offloading," in *Proc. 8th IFIP Wireless Mobile Netw. Conf. (WMNC)*, Munich, Germany, Oct. 2015, pp. 112–119.

[4] E. Borgia, R. Bruno, M. Conti, D. Mascitti, and A. Passarella, "Mobile edge clouds for information-centric IoT services," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, Messina, Italy, Jun. 2016, pp. 422–428.

[5] M. A. Marotta *et al.*, "Managing mobile cloud computing considering objective and subjective perspectives," *Comput. Netw.*, vol. 93, pp. 531–542, Oct. 2015. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128615003667

[6] H. T. Dinh, C. Lee, D. Niyato, and P. Wang, "A survey of mobile cloud computing: Architecture, applications, and approaches," *Wireless Commun. Mobile Comput.*, vol. 13, no. 18, pp. 1587–1611, 2013. [Online]. Available: http://dx.doi.org/10.1002/wcm.1203

[7] Y. Jararweh *et al.*, "The future of mobile cloud computing: Integrating cloudlets and mobile edge computing," in *Proc. 23rd Int. Conf. Telecommun. (ICT)*, Thessaloniki, Greece, May 2016, pp. 1–5.

[8] S. Kitanov, E. Monteiro, and T. Janevski, "5G and the fog 2014—Survey of related technologies and research directions," in *Proc. 18th Mediterranean Electrotech. Conf. (MELECON)*, Limassol, Cyprus, Apr. 2016, pp. 1–6.

[9] M. T. Beck, M. Werner, S. Feld, and S. Schimper, "Mobile edge computing: A taxonomy," in *Proc. 6th Int. Conf. Adv. Future Internet*, 2014, pp. 48–54.

[10] K. Kai, W. Cong, and L. Tao, "Fog computing for vehicular ad-hoc networks: Paradigms, scenarios, and issues," *J. China Univ. Posts Telecommun.*, vol. 23, no. 2, pp. 56–65, 2016.

[11] S. Yi, C. Li, and Q. Li, "A survey of fog computing: Concepts, applications and issues," in *Proc. Workshop Mobile Big Data (Mobidata)*, Hangzhou, China, 2015, pp. 37–42. [Online]. Available: http://doi.acm.org/10.1145/2757384.2757397

[12] Y. Jararweh *et al.*, "SDMEC: Software defined system for mobile edge computing," in *Proc. IEEE Int. Conf. Cloud Eng. Workshop (IC2EW)*, Berlin, Germany, Apr. 2016, pp. 88–93.

[13] R. Roman, J. Lopez, and M. Mambo, "Mobile edge computing, fog *et al.*: A survey and analysis of security threats and challenges," *Future Gener. Comput. Syst.*, Nov. 2016. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167739X16305635

[14] A. Ahmed and E. Ahmed, "A survey on mobile edge computing," in *Proc. 10th Int. Conf. Intell. Syst. Control (ISCO)*, Coimbatore, India, 2016, pp. 1–8.

[15] Y. C. Hu, M. Patel, D. Sabella, N. Sprecher, and V. Young, "Mobile edge computing—A key technology towards 5G," ETSI, Sophia Antipolis, France, White Paper, vol. 11, 2015.

[16] D. Satria, D. Park, and M. Jo, "Recovery for overloaded mobile edge computing," *Future Gener. Comput. Syst.*, vol. 70, pp. 138–147, May 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167739X16302096

[17] M. Patel *et al.*, "Mobile-edge computing—Introductory technical white paper," White Paper, Mobile-Edge Computing (MEC) Industry Initiative, 2014.

[18] S. Yi, Z. Hao, Z. Qin, and Q. Li, "Fog computing: Platform and applications," in *Proc. 3rd IEEE Workshop Hot Topics Web Syst. Technol. (HotWeb)*, Washington, DC, USA, 2015, pp. 73–78.

[19] P. Asrani, "Mobile cloud computing," *Int. J. Eng. Adv. Technol.*, vol. 2, no. 4, pp. 606–609, 2013.

[20] D. Huang, "Mobile cloud computing," *IEEE COMSOC Multimedia Commun. Tech. Committee E-Lett.*, vol. 6, no. 10, pp. 27–31, Oct. 2011.

[21] P. M. Mell and T. Grance, "The NIST definition of cloud computing," Nat. Inst. Stand. Technol., Gaithersburg, MD, USA, Tech. Rep. 800-145, 2011.

[22] T. Brummett, P. Sheinidashtegol, D. Sarkar, and M. Galloway, "Performance metrics of local cloud computing architectures," in *Proc. IEEE 2nd Int. Conf. Cyber Security Cloud Comput. (CSCloud)*, New York, NY, USA, Nov. 2015, pp. 25–30.

[23] T. Zhao, S. Zhou, X. Guo, Y. Zhao, and Z. Niu, "A cooperative scheduling scheme of local cloud and Internet cloud for delay-aware mobile cloud computing," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, San Diego, CA, USA, Dec. 2015, pp. 1–6.

[24] Y. Liu, M. J. Lee, and Y. Zheng, "Adaptive multi-resource allocation for cloudlet-based mobile cloud computing system," *IEEE Trans. Mobile Comput.*, vol. 15, no. 10, pp. 2398–2410, Oct. 2016.

[25] A. E.-H. G. El-Barbary, L. A. A. El-Sayed, H. H. Aly, and M. N. El-Derini, "A cloudlet architecture using mobile devices," in *Proc. IEEE/ACS 12th Int. Conf. Comput. Syst. Appl. (AICCSA)*, Nov. 2015, pp. 1–8.

[26] T. Verbelen, P. Simoens, F. De Turck, and B. Dhoedt, "Cloudlets: Bringing the cloud to the mobile user," in *Proc. 3rd ACM Workshop Mobile Cloud Comput. Services (MCS)*, 2012, pp. 29–36. [Online]. Available: http://doi.acm.org/10.1145/2307849.2307858

[27] Z. Pang, L. Sun, Z. Wang, E. Tian, and S. Yang, "A survey of cloudlet based mobile computing," in *Proc. Int. Conf. Cloud Comput. Big Data (CCBD)*, Shanghai, China, Nov. 2015, pp. 268–275.

[28] A. Taherkordi and F. Eliassen, "Poster abstract: Data-centric IoT services provisioning in fog-cloud computing systems," in *Proc. IEEE/ACM 2nd Int. Conf. Internet Things Design Implement. (IoTDI)*, Pittsburgh, PA, USA, 2017, pp. 317–318.

[29] R. Q. Hu, *Heterogeneous Cellular Networks*. New York, NY, USA: Wiley, 2013.

[30] A. H. Khan, M. A. Qadeer, J. A. Ansari, and S. Waheed, "4G as a next generation wireless network," in *Proc. Int. Conf. Future Comput. Commun. (ICFCC)*, Kuala Lumpar, Malaysia, Apr. 2009, pp. 334–338.

[31] CommVerge. (2016). *Radio Access Network (RAN) Optimization*. Accessed: Sep. 19, 2016. [Online]. Available: http://www.commverge.com/Solutions/SubscribersServicesManagement/RANOptimization/tabid/174/Default.aspx

[32] C.-K. Park, "Performance for radio access network in mobile backhaul network," *J. Inst. Internet Broadcast. Commun.*, vol. 12, no. 6, pp. 297–302, 2012.

[33] Brocade. (2016). *Brocade and the Mobile Edge*. Accessed: Oct. 3, 2016. [Online]. Available: https://www.brocade.com/content/dam/common/documents/content-types/solution-brief/brocade-and-the-mobile-edge-sb.pdf

[34] J. Wu, Z. Zhang, Y. Hong, and Y. Wen, "Cloud radio access network (C-RAN): A primer," *IEEE Netw.*, vol. 29, no. 1, pp. 35–41, Jan./Feb. 2015.

[35] T. H. Luan, L. Gao, Z. Li, Y. Xiang, and L. Sun, "Fog computing: Focusing on mobile users at the edge," *CoRR*, abs/1502.01815, 2015.

[36] N. Zhong. (2015). *Mobile Edge Computing: Unleashing the Value Chain*. Accessed: Oct. 7, 2016. [Online]. Available: http://dashif.org/wp-content/uploads/2015/08/6d-Mobile-Edge-Computing-Unleashing-the-value-chain.pdf

[37] J. Sharpe. (2015). *How Mobile Edge Computing Is Helping Operators Face the Challenges of Today's Evolving Mobile Networks*. Accessed: Oct. 3, 2016. [Online]. Available: http://eecatalog.com/intel/2015/08/17/how-mobile-edge-computing-is-helping-operators-face-the-challenges-of-todays-evolving-mobile-networks/

[38] A. V. Dastjerdi, H. Gupta, R. N. Calheiros, S. K. Ghosh, and R. Buyya, "Fog computing: Principles, architectures, and applications," in *Internet of Things: Principles and Paradigms*. San Mateo, CA, USA: Morgan Kaufmann, 2016, ch. 4, pp. 61–75.

[39] T. Olsson and M. Salo, "Online user survey on current mobile augmented reality applications," in *Proc. 10th IEEE Int. Symp. Mixed Augmented Reality (ISMAR)*, Basel, Switzerland, Oct. 2011, pp. 75–84.

[40] T. Piumsomboon, A. Clark, M. Billinghurst, and A. Cockburn, "User-defined gestures for augmented reality," in *Proc. CHI Extended Abstracts Human Factors Comput. Syst. (CHI EA)*, Paris, France, 2013, pp. 955–960. [Online]. Available: http://doi.acm.org/10.1145/2468356.2468527

[41] R. Azuma *et al.*, "Recent advances in augmented reality," *IEEE Comput. Graph. Appl.*, vol. 21, no. 6, pp. 34–47, Nov./Dec. 2001.

[42] S. Yuen, G. Yaoyuneyong, and E. Johnson, "Augmented reality: An overview and five directions for AR in education," *J. Educ. Technol. Develop. Exchange*, vol. 4, no. 1, pp. 119–140, 2011.

[43] R. Buyya and A. V. Dastjerdi, *Internet of Things: Principles and Paradigms*. Cambridge, MA, USA: Elsevier, 2016.

[44] Y. Wang, T. Uehara, and R. Sasaki, "Fog computing: Issues and challenges in security and forensics," in *Proc. IEEE 39th Annu. Comput. Softw. Appl. Conf. (COMPSAC)*, vol. 3. Taichung, Taiwan, 2015, pp. 53–59.

[45] N. Peter, "Fog computing and its real time applications," *Int. J. Emerg. Technol. Adv. Eng.*, vol. 5, no. 6, pp. 266–269, 2015.

[46] I. Stojmenovic and S. Wen, "The fog computing paradigm: Scenarios and security issues," in *Proc. Federated Conf. Comput. Sci. Inf. Syst. (FedCSIS)*, Warsaw, Poland, 2014, pp. 1–8.

[47] E. Ahmed and M. H. Rehmani, "Mobile edge computing: Opportunities, solutions, and challenges," *Future Gener. Comput. Syst.*, vol. 70, pp. 59–63, May 2017.

[48] Y. Cao, S. Chen, P. Hou, and D. Brown, "Fast: A fog computing assisted distributed analytics system to monitor fall for stroke mitigation," in *Proc. IEEE Int. Conf. Netw. Archit. Stor. (NAS)*, Boston, MA, USA, Aug. 2015, pp. 2–11.

[49] A. S. Go *et al.*, "Heart disease and stroke statistics—2014 update: A report from the American heart association," *Circulation*, vol. 129, no. 3, pp. e28–e292, 2014.

[50] P. A. Heidenreich *et al.*, "Forecasting the future of cardiovascular disease in the united states: A policy statement from the American heart association," *Circulation*, vol. 123, no. 8, pp. 933–944, 2011.

[51] V. Stantchev, A. Barnawi, S. Ghulam, J. Schubert, and G. Tamm, "Smart items, fog and cloud computing as enablers of servitization in healthcare," *Sensors Transducers*, vol. 185, no. 2, pp. 121–128, 2015.

[52] K. Hong, D. Lillethun, U. Ramachandran, B. Ottenwälder, and B. Koldehofe, "Mobile fog: A programming model for large-scale applications on the Internet of Things," in *Proc. 2nd ACM SIGCOMM Workshop Mobile Cloud Comput. (MCC)*, Hong Kong, 2013, pp. 15–20. [Online]. Available: http://doi.acm.org/10.1145/2491266.2491270

[53] ITS International. (2009). *Computer Technology Increasingly Aids Traffic Management*. Accessed: Sep. 10, 2016. [Online]. Available: http://www.itsinternational.com/categories/detection-monitoring-machine-vision/features/computer-technology-increasingly-aids-traffic-management/

[54] J. K. Laurila *et al.*, "The mobile data challenge: Big data for mobile computing research," in *Proc. Pervasive Comput.*, 2012, pp. 1–8.

[55] Wikipedia. (2016). *Big Data—Wikipedia, the Free Encyclopedia*. Accessed: Sep. 12, 2016. [Online]. Available: https://en.wikipedia.org/w/index.php?title=Big_data&oldid=739099684

[56] R. Misra, B. Panda, and M. Tiwary, "Big data and ICT applications: A study," in *Proc. 2nd Int. Conf. Inf. Commun. Technol. Competitive Strategies (ICTCS)*, Udaipur, India, 2016, pp. 1–6. [Online]. Available: http://doi.acm.org/10.1145/2905055.2905099

[57] TDWI. (2011). *Big Data Analytics*. Accessed: Sep. 12, 2016. [Online]. Available: https://tdwi.org/portals/big-data-analytics.aspx

[58] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2347–2376, 4th Quart., 2015.

[59] M. A. Alsheikh, D. Niyato, S. Lin, H.-P. Tan, and Z. Han, "Mobile big data analytics using deep learning and apache spark," *IEEE Netw.*, vol. 30, no. 3, pp. 22–29, May/Jun. 2016.

[60] P. Russom *et al.*, "Big data analytics," TDWI Best Pract., Renton, WA, USA, Tech. Rep., pp. 1–35, 2011.

[61] A. Taherkordi, F. Eliassen, and G. Horn, "From IoT big data to IoT big services," in *Proc. Symp. Appl. Comput. (SAC)*, Marrakech, Morocco, 2017, pp. 485–491.

[62] S. K. Datta, C. Bonnet, and J. Haerri, "Fog computing architecture to enable consumer centric Internet of Things services," in *Proc. Int. Symp. Consum. Electron. (ISCE)*, Madrid, Spain, 2015, pp. 1–2.

[63] R. Mahmud, R. Vallakati, A. Mukherjee, P. Ranganathan, and A. Nejadpak, "A survey on smart grid metering infrastructures: Threats and solutions," in *Proc. IEEE Int. Conf. Electro/Inf. Technol. (EIT)*, Dekalb, IL, USA, May 2015, pp. 386–391.

[64] P. Kułakowski, E. Calle, and J. L. Marzo, "Performance study of wireless sensor and actuator networks in forest fire scenarios," *Int. J. Commun. Syst.*, vol. 26, no. 4, pp. 515–529, 2013. [Online]. Available: http://dx.doi.org/10.1002/dac.2311

[65] S. Shin and G. Gu, "Attacking software-defined networks: A first feasibility study," in *Proc. 2nd ACM SIGCOMM Workshop Hot Topics Softw. Defined Netw. (HotSDN)*, Hong Kong, 2013, pp. 165–166. [Online]. Available: http://doi.acm.org/10.1145/2491185.2491220

[66] R. Jain and S. Paul, "Network virtualization and software defined networking for cloud computing: A survey," *IEEE Commun. Mag.*, vol. 51, no. 11, pp. 24–31, Nov. 2013.

[67] X. Ma, Y. Zhao, L. Zhang, H. Wang, and L. Peng, "When mobile terminals meet the cloud: Computation offloading as the bridge," *IEEE Netw.*, vol. 27, no. 5, pp. 28–33, Sep./Oct. 2013.

[68] K. Kumar, J. Liu, Y.-H. Lu, and B. Bhargava, "A survey of computation offloading for mobile systems," *Mobile Netw. Appl.*, vol. 18, no. 1, pp. 129–140, 2013. [Online]. Available: http://dx.doi.org/10.1007/s11036-012-0368-0

[69] D. Kovachev, T. Yu, and R. Klamma, "Adaptive computation offloading from mobile devices into the cloud," in *Proc. IEEE 10th Int. Symp. Parallel Distrib. Process. Appl.*, Leganés, Spain, Jul. 2012, pp. 784–791.

[70] M. A. Hassan, M. Xiao, Q. Wei, and S. Chen, "Help your mobile applications with fog computing," in *Proc. 12th Annu. IEEE Int. Conf. Sens. Commun. Netw. Workshops (SECON Workshops)*, Seattle, WA, USA, Jun. 2015, pp. 1–6.

[71] M. Satyanarayanan, P. Bahl, R. Caceres, and N. Davies, "The case for VM-based cloudlets in mobile computing," *IEEE Pervasive Comput.*, vol. 8, no. 4, pp. 14–23, Oct. 2009.

[72] K. Kumar and Y.-H. Lu, "Cloud computing for mobile users: Can offloading computation save energy?" *Computer*, vol. 43, no. 4, pp. 51–56, Apr. 2010.

[73] N. Takahashi, H. Tanaka, and R. Kawamura, "Analysis of process assignment in multi-tier mobile cloud computing and application to edge accelerated Web browsing," in *Proc. 3rd IEEE Int. Conf. Mobile Cloud Comput. Services Eng. (MobileCloud)*, San Francisco, CA, USA, Mar. 2015, pp. 233–234.

[74] X. Chen, L. Jiao, W. Li, and X. Fu, "Efficient multi-user computation offloading for mobile-edge cloud computing," *IEEE/ACM Trans. Netw.*, vol. 24, no. 5, pp. 2795–2808, Oct. 2016.

[75] S. Sardellitti, G. Scutari, and S. Barbarossa, "Joint optimization of radio and computational resources for multicell mobile-edge computing," *IEEE Trans. Signal Inf. Process. Over Netw.*, vol. 1, no. 2, pp. 89–103, Jun. 2015.

[76] K. Zhang, Y. Mao, S. Leng, A. Vinel, and Y. Zhang, "Delay constrained offloading for mobile edge computing in cloud-enabled vehicular networks," in *Proc. 8th Int. Workshop Resilient Netw. Design Model. (RNDM)*, Halmstad, Sweden, Sep. 2016, pp. 288–294.

[77] K. Habak, M. Ammar, K. A. Harras, and E. Zegura, "Femto clouds: Leveraging mobile devices to provide cloud service at the edge," in *Proc. IEEE 8th Int. Conf. Cloud Comput.*, New York, NY, USA, Jun./Jul. 2015, pp. 9–16.

[78] S. Abdelwahab, B. Hamdaoui, M. Guizani, and T. Znati, "Replisom: Disciplined tiny memory replication for massive IoT devices in LTE edge cloud," *IEEE Internet Things J.*, vol. 3, no. 3, pp. 327–338, Jun. 2016.

[79] S. Nunna *et al.*, "Enabling real-time context-aware collaboration through 5G and mobile edge computing," in *Proc. 12th Int. Conf. Inf. Technol. New Gener. (ITNG)*, Las Vegas, NV, USA, Apr. 2015, pp. 601–605.

[80] N. Kumar, S. Zeadally, and J. J. P. C. Rodrigues, "Vehicular delay-tolerant networks for smart grid data management using mobile edge computing," *IEEE Commun. Mag.*, vol. 54, no. 10, pp. 60–66, Oct. 2016.

[81] W. Gao, "Opportunistic peer-to-peer mobile cloud computing at the tactical edge," in *Proc. IEEE Mil. Commun. Conf.*, Baltimore, MD, USA, Oct. 2014, pp. 1614–1620.

[82] M. T. Beck, S. Feld, A. Fichtner, C. Linnhoff-Popien, and T. Schimper, "ME-VoLTE: Network functions for energy-efficient video transcoding at the mobile edge," in *Proc. 18th Int. Conf. Intell. Next Gener. Netw. (ICIN)*, Paris, France, Feb. 2015, pp. 38–44.

[83] F. Jalali, K. Hinton, R. Ayre, T. Alpcan, and R. S. Tucker, "Fog computing may help to save energy in cloud computing," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 5, pp. 1728–1739, May 2016.

[84] E. Piri *et al.*, "5GTN: A test network for 5G application development and testing," in *Proc. Eur. Conf. Netw. Commun. (EuCNC)*, Athens, Greece, 2016, pp. 313–318.

[85] *Small Cells Deliver Cost-Effective Capacity and Coverage, Indoors and Outdoors*, NOKIA, Espoo, Finland, 2016, accessed: Nov. 27, 2016. [Online]. Available: https://networks.nokia.com/products/small-cells

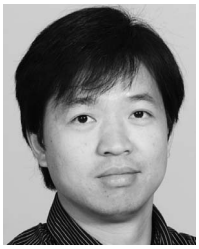
[86] *Small Cells Mobile Edge Computing Cover All the Bases For Taiwan Baseball Fans*, NOKIA, Espoo, Finland, 2016, accessed: Nov. 27, 2016. [Online]. Available: https://blog.networks.nokia.com/small-cells/2016/09/14/small-cells-mobile-edge-computing-cover-bases-taiwan-baseball-fans/

[87] *Connected Cars Use Case for Mobile Edge Computing*, NOKIA, Espoo, Finland, 2016, accessed: Nov. 27, 2016. [Online]. Available: https://networks.nokia.com/solutions/mobile-edge-computing

[88] S. Yi, Z. Qin, and Q. Li, "Security and privacy issues of fog computing: A survey," in *Proc. Int. Conf. Wireless Algorithms Syst. Appl.*, Qufu, China, 2015, pp. 685–695.
[89] I. Stojmenovic, S. Wen, X. Huang, and H. Luan, "An overview of fog computing and its security issues," in *Concurrency and Computation: Practice and Experience*. New York, NY, USA: Wiley, 2015, vol. 28, no. 10.
[90] H. Li, G. Shou, Y. Hu, and Z. Guo, "Mobile edge computing: Progress and challenges," in *Proc. 4th IEEE Int. Conf. Mobile Cloud Comput. Services Eng. (MobileCloud)*, Oxford, U.K., Mar. 2016, pp. 83–84.
[91] Y. Cherdantseva and J. Hilton, "A reference model of information assurance & security," in *Proc. Int. Conf. Availability Rel. Security*, 2013, pp. 546–555.
[92] J. Somorovsky *et al.*, "All your clouds are belong to us: Security analysis of cloud management interfaces," in *Proc. 3rd ACM Workshop Cloud Comput. Security Workshop*, Chicago, IL, USA, 2011, pp. 3–14.
[93] H. Han, B. Sheng, C. C. Tan, Q. Li, and S. Lu, "A timing-based scheme for rogue AP detection," *IEEE Trans. Parallel Distrib. Syst.*, vol. 22, no. 11, pp. 1912–1925, Nov. 2011.
[94] D. Balfanz, D. K. Smetters, P. Stewart, and H. C. Wong, "Talking to strangers: Authentication in ad-hoc wireless networks," in *Proc. Netw. Distrib. Syst. Security Symp.*, 2002, pp. 23–35.
[95] S. Bouzefrane, A. F. B. Mostefa, F. Houacine, and H. Cagnon, "Cloudlets authentication in NFC-based mobile computing," in *Proc. 2nd IEEE Int. Conf. Mobile Cloud Comput. Services Eng. (MobileCloud)*, Oxford, U.K., 2014, pp. 267–272.
[96] M. Satyanarayanan *et al.*, "An open ecosystem for mobile-cloud convergence," *IEEE Commun. Mag.*, vol. 53, no. 3, pp. 63–70, Mar. 2015.
[97] F. Klaedtke, G. O. Karame, R. Bifulco, and H. Cui, "Access control for SDN controllers," in *Proc. 3rd Workshop Hot Topics Softw. Defined Netw.*, Chicago, IL, USA, 2014, pp. 219–220.
[98] G. Pék, L. Buttyán, and B. Bencsáth, "A survey of security issues in hardware virtualization," *ACM Comput. Surveys*, vol. 45, no. 3, p. 40, 2013.
[99] K. Yang and X. Jia, "Data storage auditing service in cloud computing: Challenges, methods and opportunities," *World Wide Web*, vol. 15, no. 4, pp. 409–428, 2012.
[100] R. Gennaro, C. Gentry, and B. Parno, "Non-interactive verifiable computing: Outsourcing computation to untrusted workers," in *Proc. Annu. Cryptol. Conf.*, Santa Barbara, CA, USA, 2010, pp. 465–482.
[101] C. Wang, N. Cao, K. Ren, and W. Lou, "Enabling secure and efficient ranked keyword search over outsourced cloud data," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 8, pp. 1467–1479, Aug. 2012.
[102] R. Lu, X. Liang, X. Li, X. Lin, and X. Shen, "EPPA: An efficient and privacy-preserving aggregation scheme for secure smart grid communications," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 9, pp. 1621–1631, Sep. 2012.
[103] S. McLaughlin, P. McDaniel, and W. Aiello, "Protecting consumer privacy from electric load monitoring," in *Proc. 18th ACM Conf. Comput. Commun. Security*, Chicago, IL, USA, 2011, pp. 87–98.
[104] W. Wei, F. Xu, and Q. Li, "MobiShare: Flexible privacy-preserving location sharing in mobile online social networks," in *Proc. IEEE INFOCOM*, Orlando, FL, USA, 2012, pp. 2616–2620.
[105] J. B. Abdo, T. Bourgeau, J. Demerjian, and H. Chaouchi, "Extended privacy in crowdsourced location-based services using mobile cloud computing," *Mobile Inf. Syst.*, vol. 2016, 2016, Art. no. 7867206.
[106] M. Sookhak, H. Talebian, E. Ahmed, A. Gani, and M. K. Khan, "A review on remote data auditing in single cloud server: Taxonomy and open issues," *J. Netw. Comput. Appl.*, vol. 43, pp. 121–141, Aug. 2014.
[107] J. Shuja, A. Gani, A. Naveed, E. Ahmed, and C.-H. Hsu, "Case of ARM emulation optimization for offloading mechanisms in mobile cloud computing," *Future Gener. Comput. Syst.*, vol. 76, pp. 407–417, Nov. 2017.
[108] E. Ahmed, A. Gani, M. Sookhak, S. H. Ab Hamid, and F. Xia, "Application optimization in mobile cloud computing: Motivation, taxonomies, and open challenges," *J. Netw. Comput. Appl.*, vol. 52, pp. 52–68, Jun. 2015.
[109] E. Ahmed, A. Gani, M. K. Khan, R. Buyya, and S. U. Khan, "Seamless application execution in mobile cloud computing: Motivation, taxonomy, and open challenges," *J. Netw. Comput. Appl.*, vol. 52, pp. 154–172, Jun. 2015.
[110] E. Ahmed, S. Khan, I. Yaqoob, A. Gani, and F. Salim, "Multi-objective optimization model for seamless application execution in mobile cloud computing," in *Proc. 5th Int. Conf. Inf. Commun. Technol. (ICICT)*, Karachi, Pakistan, 2013, pp. 1–6.
[111] E. Ahmed *et al.*, "Network-centric performance analysis of runtime application migration in mobile cloud computing," *Simulat. Model. Pract. Theory*, vol. 50, pp. 42–56, Jan. 2015.

**Nasir Abbas** received the master's degree in network and system administration from the Department of Informatics, University of Oslo, Oslo, Norway, in 2017.

He has performed research on OpenStack and Amazon Web services cloud computing to build and maintain entire IT infrastructures. His current research interests include cloud computing for which he had attended several conferences on cloud technologies, edge computing, 5G networks, mobile cloud computing, wireless networks, radio access network, network functions virtualization, and Internet of Things.



**Yan Zhang** (M'05–SM'10) received the Ph.D. degree from the School of Electrical and Electronics Engineering, Nanyang Technological University, Singapore.

He is a Full Professor with the Department of Informatics, University of Oslo, Oslo, Norway. His current research interests include next-generation wireless networks leading to 5G, and green and secure cyber-physical systems, such as smart grid, healthcare, and transport.

Dr. Zhang is an Associate Technical Editor for *IEEE Communications Magazine*, an Editor for the IEEE TRANSACTIONS ON GREEN COMMUNICATIONS AND NETWORKING, the IEEE COMMUNICATIONS SURVEYS AND TUTORIALS, the IEEE INTERNET OF THINGS JOURNAL, and an Associate Editor for IEEE ACCESS. He serves as the Chair for a number of conferences including IEEE GLOBECOM 2017, IEEE VTC-Spring 2017, IEEE PIMRC 2016, IEEE CloudCom 2016, IEEE ICCC 2016, IEEE CCNC 2016, IEEE SmartGridComm 2015, and IEEE CloudCom 2015. He serves as a TPC member for numerous international conference including IEEE INFOCOM, IEEE ICC, IEEE GLOBECOM, and IEEE WCNC. He is an IEEE Vehicular Technology Society (VTS) Distinguished Lecturer. He is also a Senior Member of IEEE ComSoc, IEEE CS, IEEE PES, and IEEE VTS. He is a Fellow of the IET.

**Amir Taherkordi** (M'16) received the Ph.D. degree from the Department of Informatics, University of Oslo, Oslo, Norway, in 2011.

He is a Researcher with the Networks and Distributed Systems Group, Department of Informatics, University of Oslo. He possesses experience from several Norwegian and EU research projects. His current research interests include distributed computing, software engineering, middleware engineering, embedded systems, software architecture, programming abstractions, service distribution, and middleware systems for Internet of Things (IoT).

Dr. Taherkordi was selected as a Young Talented Researcher by the Norwegian Research Council in 2017 to work on a novel IoT service computing model for future fog-cloud computing systems.

**Tor Skeie** received the M.S. and Ph.D. degrees in computer science from the University of Oslo, Oslo, Norway, in 1993 and 1998, respectively.

He is a Professor with the Simula Research Laboratory, Lysaker, Norway, and the University of Oslo. His current research interests include scalability, effective routing, fault tolerance, and quality of service in switched network topologies. He is also a Researcher in the Industrial Ethernet area. The key topics here have been the road to deterministic Ethernet end-to-end and how precise time synchronization can be achieved across switched Ethernet. He has also contributed to wireless networking, hereunder quality of service in WLANs, and cognitive radio.