Survey on Multi-Access Edge Computing for Internet of Things Realization

Pawani Porambage, *Student Member, IEEE*, Jude Okwuibe, *Student Member, IEEE*, Madhusanka Liyanage, *Member, IEEE*, Mika Ylianttila, *Senior Member, IEEE*, and Tarik Taleb, *Senior Member, IEEE*

***Abstract*—The Internet of Things (IoT) has recently advanced from an experimental technology to what will become the backbone of future customer value for both product and service sector businesses. This underscores the cardinal role of IoT on the journey toward the fifth generation of wireless communication systems. IoT technologies augmented with intelligent and big data analytics are expected to rapidly change the landscape of myriads of application domains ranging from health care to smart cities and industrial automations. The emergence of multi-access edge computing (MEC) technology aims at extending cloud computing capabilities to the edge of the radio access network, hence providing real-time, high-bandwidth, low-latency access to radio network resources. IoT is identified as a key use case of MEC, given MEC's ability to provide cloud platform and gateway services at the network edge. MEC will inspire the development of myriads of applications and services with demand for ultralow latency and high quality of service due to its dense geographical distribution and wide support for mobility. MEC is therefore an important enabler of IoT applications and services which require real-time operations. In this survey, we provide a holistic overview on the exploitation of MEC technology for the realization of IoT applications and their synergies. We further discuss the technical aspects of enabling MEC in IoT and provide some insight into various other integration technologies therein.**

***Index Terms*—Multi-access edge computing (MEC), Internet of Things (IoT), 5G, edge computing, virtualization, network architecture, latency, reliability.**

I. Introduction

OVER the last four decades, the Internet has evolved from peer-to-peer networking to World-Wide-Web, and mobile-Internet to the Internet of Things (IoT) (Figure 1). IoT emerged as a huge paradigm shift by connecting a versatile and massive collection of smart objects to the Internet. With IoT, people and things are able to connect at any time to any place with anything and anyone, ideally using any path or network and any available services [1]. From the user and application points of view, fifth generation (5G) wireless networks will be highly capable mobile networks with high bandwidth (e.g., 10 Gbps), very low latency (e.g., 1 ms), and low operational cost which will lead to highly improved quality of service and quality of experience. Another significant advancement of the Internet will be the Tactile Internet; which is a highly advanced use case of human-to-machine and machine-to-machine interaction characterized by ultra low latency with extremely high availability, reliability and security.

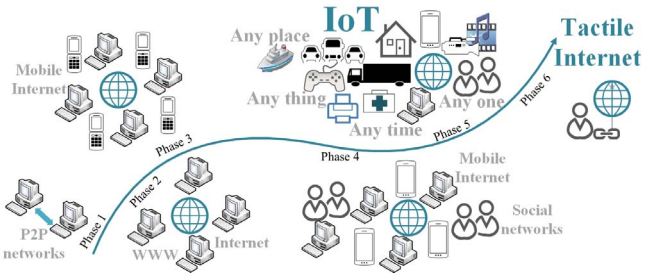

Fig. 1. Evolution of the Internet.

IoT system is poised to induce a significant surge in demand for data, computing resources, as well as networking infrastructures in order to accommodate the anticipated myriads of interconnected devices. Meeting these extreme demands will necessitate a modification to existing network infrastructures as well as cloud computing technologies.

Mobile Edge Computing was introduced by the European Telecommunications Standards Institute (ETSI) Industry Specification Group (ISG) as a means of extending intelligence to the edge of the network along with higher processing and storage capabilities [2]. From 2017, the ETSI industry group renamed it to Multi-Access Edge Computing (MEC), since the benefits of MEC technology reached beyond mobile and into Wi-Fi and fixed access technologies. Nevertheless, the name change conveniently allows ETSI to retain the MEC acronym, which has become widely recognized among stakeholders in the industry.

The underlying principle of MEC is to extend cloud computing capabilities to the edge of cellular networks. This will

Manuscript received February 2, 2018; revised May 16, 2018; accepted June 18, 2018. Date of publication June 21, 2018; date of current version November 19, 2018. This work was supported in part by the Infotech Doctoral Program of UniOGS and four research projects—6Genesis Flagship under Grant 318927, Secure Connectivity of Future Cyber-Physical Systems, Towards Digital Paradise, and Micro-Operator Concept for Boosting Local Service Delivery in 5G, and in part by the Academy of Finland and TEKES, Finland. *(Corresponding author: Pawani Porambage.)*

P. Porambage, J. Okwuibe, M. Liyanage, and M. Ylianttila are with the Center for Wireless Communications, University of Oulu, 90570 Oulu, Finland (e-mail: pawani.porambage@oulu.fi; jude.okwuibe@oulu.fi; madhusanka.liyanage@oulu.fi; mika.ylianttila@oulu.fi).

T. Taleb is with the Department of Communications and Networking, Aalto University, 06220 Espoo, Finland, and also with the Department of Computer and Information Security, Sejong University, Seoul 143-747, South Korea (e-mail: tarik.taleb@aalto.fi).

Digital Object Identifier 10.1109/COMST.2018.2849509

TABLE I
HIGH LEVEL COMPARISON OF EDGE COMPUTING PARADIGMS

	MEC	**Fog computing**	**Cloudlet**	**MCC**
Initial promotion	ETSI (2014)	Cisco (2011)	Carnegie Mellon Uni. (2013)	Aepona (2010)
Objective	Bring cloud computing capabilities closer to User Equipment (UE)			
Infrastructure owners	Telecom operator	Private entities / individuals		
Node location	Radio network controller or macro base station	Any strategic location between end user device and cloud		
SW architecture	Mobile orchestrator based	Fog abstraction layer based	Cloudlet agent based	Service oriented
Service accessibility	Direct access from the closest UE			Via Internet connection
Latency and jitter	Low			High
Context awareness	High	Medium	Low	High
Storage capacity and computation power	Limited			High
Relevance to IoT	High			Low

minimize network congestion and improve resource optimization, user experience and the overall performance of the network. By leveraging on the Radio Access Networks (RANs), MEC will improve heavily on latency and bandwidth utilization, making it easier for both application developers and content providers to access network services. Several technologies are identified as enabling technologies for MEC realization, these include Software Defined Networking (SDN), Network Function Virtualization (NFV), Information Centric Networking (ICN) and Network Slicing.

A. Role of MEC for IoT

Generally, cloud computing enables the outsourcing of storage and processing functionalities of IoT data to a third party in order to ease the hazel involved in self-management and data protection. However, the centralized nature of conventional cloud servers may face several challenges such as the single point of failure, lack of location awareness, reachability, and latencies associated with typical Wide Area Networks (WANs). On the other hand, many IoT applications need to be served with decentralized systems which need mobility management, geo-distribution, location awareness, scalability, and ultra-low latency. Mission critical communication IoT use cases need latency as low as 1 ms and reliability as high as 99.99 %. For instance factory automation applications may typically require a reliability of 10^{-9} packet loss rate and a latency range of 250 μs to 10 ms [3]. Therefore, the conjugation of IoT applications and centralized cloud servers may introduce several limitations and vulnerabilities. In addition, the rapid growth of IoT devices and big data sets may also create cumbersome traffic on telecommunications networks.

Edge computing was conceived in a bid to fill the gap between the centralized cloud and IoT devices. Apart from MEC, there are other edge computing paradigms such as Mobile Cloud Computing (MCC), fog computing, and cloudlets. They tend to coexist with MEC in many technical contexts, hence the tendency for a misappropriation of these technologies given that they all have similar origin. However, these technologies are intrinsically different and each of them comes with its unique value proposition to both existing and future mobile networks as summarized in Table I.

ETSI has identified IoT as one of the key use cases of MEC [2]. MEC has opened many new frontiers for network

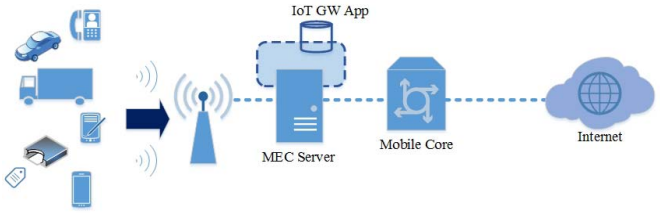

Fig. 2. IoT gateway service scenario [2].

operators, service and content providers to deploy versatile and uninterrupted services on IoT applications. MEC and IoT facilitate each other with mutual advantages. MEC empowers tiny IoT devices with significant additional computational capabilities through computation offloading. Similarly, IoT expands MEC services to all types of smart objects ranging from sensors and actuators to smart vehicles. As shown in Figure 2, MEC servers can perform as gateway nodes which can aggregate and process the small data packets generated by IoT services before they reach the core network. As summarized in [4], the three key benefits of the collaboration between IoT and MEC are: 1) lowering the amount of traffic passing through the infrastructure; 2) reducing the latency for applications and services; and 3) scaling network services diversely. Among these, the most significant is the low latency introduced by MEC due the reduced physical and virtual communication distance.

B. Paper Motivation

At present, IoT has become a fairly mature technology. As a result, the recent decade has seen a plethora of surveys published in multiple research areas on IoT including enabling concepts [5], visions and challenges [6], technologies [7], standardization [8], architecture [9], security [10], [11], privacy [12], trust [13], Social Internet of Things (SIoT) [14], communication [15], context awareness [16], and future directions [6], [17]. Few other papers are focused on the combined aspects of IoT research and their potential application scenarios [7], [18]–[20]. Some of these surveys were published during the time when IoT was more of a visionary paradigm than a real world platform. Many future research possibilities discussed in those papers have already been achieved and commercialized with high market values. However, there

TABLE II
SUMMARY OF IMPORTANT SURVEYS ON MEC

Aspect	Ref.	Main contribution	Relevance to IoT
Research directions	[22]	An elaboration of edge-centric vision and its future research challenges.	No explicit focus on IoT.
	[23]	A comprehensive overview on sate-of-the-art and future research directions for MEC.	Concisely describes how MEC can improve latency and support big data handling in different IoT deployments.
	[24]	A presentation of MEC related definitions, applications, opportunities, and research challenges.	Provides no detailed description on IoT. Identifies IoT data handling as a key use case of MEC.
	[25]	A concise tutorial of three edge computing technologies, including MEC, cloudlets, and fog computing.	Describes the exploitation of edge computing technologies for IoT with respect to standardization efforts, principles, architectures, and applications.
	[26]	A comprehensive survey of relevant research and technological developments in the area of MEC.	Identifies MEC services for IoT big-data analytics.
Taxonomy	[27]	A taxonomy of MEC based on different aspects including its characteristics, access technologies, applications, and objectives.	Classifies MEC applications as computational offloading, collaborative computing, memory replication in IoT and content delivery.
	[28]	A classification of applications deployed in MEC systems.	No explicit focus on IoT.
Architecture and Computation Offloading	[29]	A detailed study on decision on computation offloading, allocation of computing resources, and mobility management along with a summary of MEC use cases and standardization efforts.	Describes MEC acting as an IoT gateway.
Virtualization	[4]	A survey of 5G network edge cloud architecture and orchestration with a summary of MEC virtualization technologies including Virtual Machines (VMs), SDN, NFV and network slicing.	Explains how MEC platform can encompass a local IoT gateway functionality capable of performing data aggregation and big data analytics for application domains.
	[30]	An investigation on how to exploit SDN for enabling edge computing.	Discuses SDN scenarios based on IoT and edge Computing, and the future research.
	[31]	An elaboration of network slicing from an E2E perspective on principles, enabling technologies and solutions.	Describes the role of massive IoT as a key use case of 5G and network slicing.
Communication	[32]	An comprehensive survey on joint radio-and-computational resource management in MEC systems.	Briefly introduces the role of MEC in IoT.
	[33]	A comprehensive survey of issues on computing, caching and communication techniques in MEC.	Describes specific applications and use cases of MEC in IoT including healthcare, wireless sensor systems, smart grid, smart home, and smart city.
MEC-IoT	[21]	An overview about the role of MEC in IoT use cases.	Provides examples of MEC deployments for IoT cases: Security, safety, and data analytics; Vehicle to infrastructure communication; Computation offloading to edge cloud.
Security	[34]	A discussion of the security threats and challenges in the edge paradigms, along with the promising solution for each specific challenge.	No explicit discussion on IoT. Briefly discusses how IoT will benefit from edge computing and related security threats.

is yet to be a sufficient number of publications on MEC technology, given that is relatively a novel technology which lies at the intersection of mobile cloud computing and wireless communication. In Table II, we summarize the recently published surveys on MEC. These articles are focused on MEC taxonomy, future research directions, and more specific MEC attributes such as communication, computation offloading, security, and virtualization. These studies are quite shallow in addressing the MEC integration with IoT, they are mostly focusing on the requirements and usability of MEC in IoT applications. In this short magazine article [21], the authors discuss the examples of MEC deployment, with special reference to IoT use cases.

To the best of our knowledge there is not a single survey which addresses broader range of areas about MEC and its influence on IoT realization. Since both MEC and IoT are very essential to the realization of 5G, it is vital to express their associativity in terms of application scenarios and key technical attributes. Our goal is to broaden the horizons of potential inter-dependencies of MEC and IoT technologies and their related applications in future 5G and beyond.

Furthermore, in our previous survey [4], we discuss the role of MEC in 5G network edge cloud architecture and orchestration. There we do not explicitly address the integration of MEC for the realization of IoT and related applications. In addition to MEC integration technologies like SDN, NFV, and network slicing discussed in [4], we consider ICN in this work. Therefore, this survey sets to provide a comprehensive overview of the state-of-the-art technologies which are required for the complementary integration of MEC with IoT. In this survey, our contributions manifold into three main categories:

1) Providing a comprehensive survey on the exploitation of MEC technology for the realization of different IoT applications.
2) Presenting a holistic overview of related works and the future research directions in areas of scalability, communication, computation offloading, resource allocation, mobility management, security, privacy, and trust management of MEC-IoT integration.
3) Providing a concise summary of the state-of-the-art MEC integrating technologies for IoT and related projects.

TABLE III
SUMMARY OF IMPORTANT ACRONYMS

Acronym	Definition	Acronym	Definition
3GPP	Third Generation Partnership Project	5G	Fifth Generation Wireless Network
AI	Artifical Intelligence	AR	Augmented Reality
BLE	Bluetooth Low Energy	CaPC	Cloud-aware Power Control
CPS	Cyber Physical System	C-RAN	Cloud Radio Access Network
D2D	Device-to-device	DDoS	Distributed Denial of Service
DoS	Denial of Service	E2E	End-to-end
EC	Edge Computing	eMBB	enhance Mobile Broadband
EMM	Energy-aware Mobility Management	eNodeB	Evolved Node B
ETSI	European Telecommunications Standards Institute	EU	European Union
FiWi	Fiber-enable Wireless	F-RAN	Fog Radio Access Network
GDPR	General Data Protection Regulation	ICN	Information Centric Networking
ICT	Information Communication Technology	IIoT	Industrial Internet of Things
IoT	Internet of Things	ISG	Industry Specification Group
KDN	Knowledge-Defined Networking	LPWAN	Low-power Wide Area Network
LTE	Long Term Evolution	M2M	Machine-to-machine
MANO	Management and Orchestration	MCC	Mobile Cloud Computing
MEC	Multi-Access Edge Computing	MIFaaS	Mobile-IoT-Federation-as-a-Service
MitM	Man-in-the-Middle	mmW	millimeter-Wave
MR	Mixed Reality	NB-IoT	Narrow-band IoT
NFV	Network Function Virtualization	PbD	Privacy by Design
QoE	Quality of Experience	QoS	Quality of Service
RAN	Radio Access Networks	RAT	Radio Access Technology
RFID	Radio-Frequency Identification	RNC	Radio Network Controller
SCeNB	Small Cell eNodeBs	SDLB	Software Load Balancer
SDN	Software Defined Networking	SDP	Software Defined Privacy
SIoT	Social Internet of Things	TDMA	Time-division Multiple Access
UAV	Unmanned Aerial Vehicles	UE	User Equipment
V2V	Vehicle to Vehicle	V2X	Vehicle to Everything
VANET	Vehicular Ad-hoc Network	VM	Virtual Machine
VNF	Virtual Network Function	VR	Virtual Reality
VRARA	Virtual Reality/Augmented Reality Association	WAN	Wide Area Networking
WAP	Wireless Access Point	WIoT	Wearable Internet of Things
WLAN	Wirless Local Area Networking	WSN	Wireless Sensor Network

C. Paper Organization

The rest of the paper is organized as follows: Section II summarizes the well-known IoT applications that require a noteworthy assistance of MEC like edge computing technologies. Section III is particularly focused on technological aspects of MEC enabled IoT systems in terms of scalability, communication, computation offloading, resource management, mobility management, security, privacy, and trust management. Each technical aspect is described with its requirements and related works. Sections IV and V respectively summarize the related work on different MEC integration technologies and the proceeding research projects in the respective areas. Section VI describes the lessons learned and the future research directions. Finally, Section VII concludes the paper. We provide the definitions of frequently used acronyms in Table III.

II. IOT AND MEC APPLICATION SCENARIOS

This section focuses on how IoT can leverage MEC technology in various application scenarios. IoT itself is a classic application of MEC where the key value proposition of MEC is exemplified in a variety of application scenarios (Figure 3). These values become evident in the utility factor measured by the end user experience while using such IoT related services.

Table IV and V respectively show the characteristics of different IoT applications and how each application benefits from MEC-IoT integration. In addition, Table VI summarizes the reviewed state-of-the-art applications in MEC-IoT domains.

A. Smart Home and Smart City

One of the pioneering applications of the IoT technology has been in the areas of home automation and consumer electronics [39]. Several smart home applications that are built on the basis of IoT concept are already available in most consumer markets. These range from the simple thermostat sensors to other more sophisticated automation systems like smart metering, smart heating and lighting, cleaning services, and home entertainment systems. That notwithstanding, the amount of data that would be generated on a typical IoT network like the smart home is expected to be huge. Hence transferring such data to the centralized cloud servers will be impractical with most pre-MEC techniques. As a solution, MEC leverages specialized and reliable local services for processing and storage capabilities for the large IoT traffic created within a building. The conventional gateways which allow IoT applications to run on the centralized cloud can be empowered with MEC-server functionalities [40], [41]. This extends gateway functionalities to the edge of the network with reduced communication latency. Since such appliances are statically deployed in smart home or smart building environments, the cooperation with MEC servers will offer some other features such as easy instantiation, relocation, privacy preservation, and upgrading when necessary [21], [42].

Correspondingly, IoT technology has advanced from home to community, and even city scale applications. We see numerous future promises for public safety, health care,

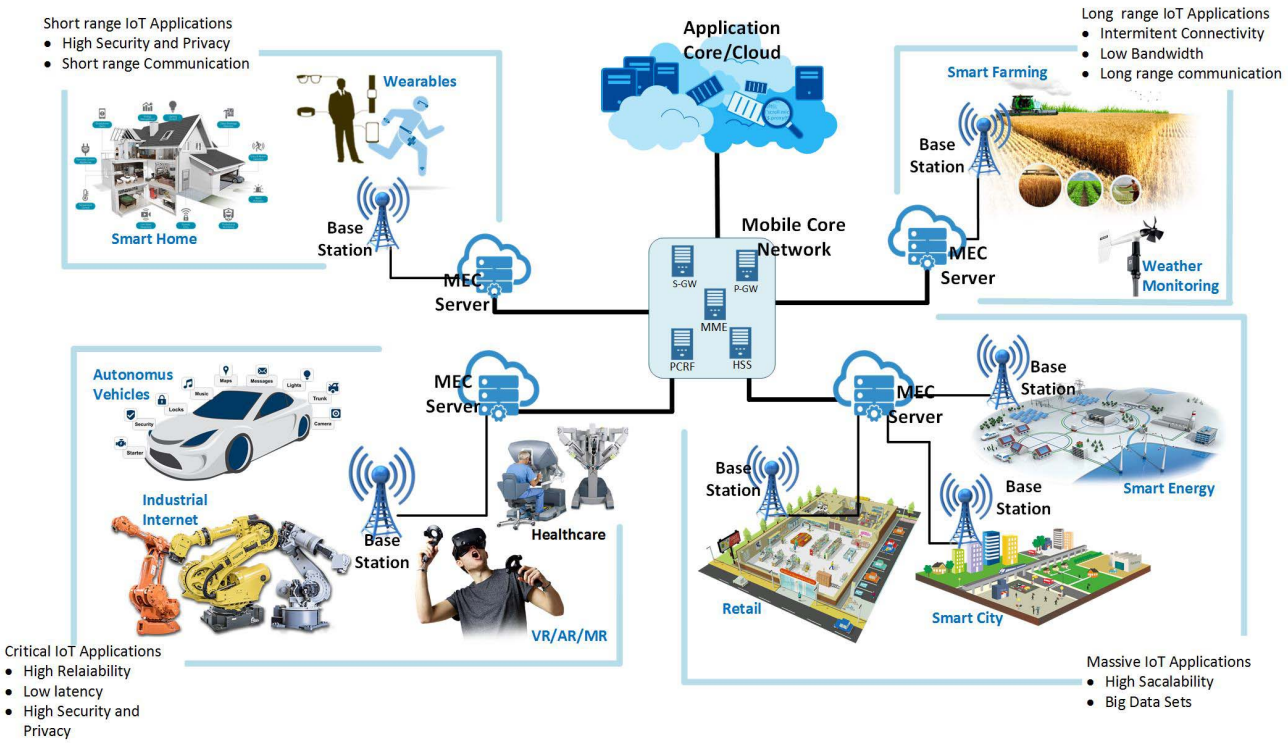

Fig. 3. IoT and MEC application scenarios.

TABLE IV
CHARACTERISTICS OF DIFFERENT IOT APPLICATION

IoT Application	Data type	Data Capacity	Backhaul Connectivity	Expected latency	Number of IoT Devices
Smart home	Stream / Historical data	$\geq$ 10 MB of data per household per day	Realtime	1 ms -1000 s	$\geq$10-100 per house
Smart city	Stream / Massive data	$\geq$10-100 million GB of data per city per day	Realtime	$\leq$1ms	$\geq$1000-1million per city
Remote surgery [35]	Stream data	$\geq$1.5 million per year	Realtime	$\leq$200 ms	$\geq$10-100 per surgery
Remote consultancy	Stream data	$\geq$ 500 million visits per year	Realtime	1 ms-100 s	1-10 per appointment
Autonomous vehicles	Stream / Massive data	$\geq$ 100 GB per vehicle per day	Realtime	$\leq$1 ms	50-200 per vehicle
AR [36]	Stream / Massive data	$\geq$1 GBps	Realtime	$\leq$1 ms	$\geq$0.2 million globally
VR [36]	Stream / Massive data	$\geq$1 GBps	Realtime	$\leq$1ms	$\geq$0.2 million globally
Gaming [36]	Stream / Massive data	$\geq$10 Mbps	Realtime	$\leq$10 ms	$\geq$1 billion globally
Retail [37]	Stream / Historical data	100 Mbps - 1 Gbps	Realtime/ Intermittent	$\leq$1 ms	$\geq$100-1000 per shop
WIoT	Stream data	$<$ 1 GB per device	Intermittent	Several Hours	$\geq$1-10 per person
Farming	Historical data	$\geq$ 1 GB per farm	Intermittent	Several hours	100-100,000 per farm
Smart energy	Stream / Massive data	$\geq$ 100,000 GB per day	Realtime/ Intermittent	1ms - 10 mins	$\geq$ 1 billion per grid
Industrial Internet [38]	Stream / Massive data	$\geq$ 100,000 GB per day	Realtime	$\leq$1 ms	$\geq$ 1 million per factory

utility, tourism, and the transport sectors. Enormous IoT data traffic produced in smart cities can be ideally processed at the edge of the network providing low latency and location awareness [43], [44]. In particular, a video cameras (i.e., deployed for surveillance) connected with a Long Term Evolution (LTE) network can convey video streams to the MEC server for real-time processing and anomaly detection [21]. Collaborative edge paradigms that connect multiple MEC servers (i.e., dedicated for different services) will advocate the applications which need to process geographically distributed data. For instance, a connected health care application requires to collaborate with entities from multiple domains such as hospital, pharmacy, insurance, logistics, and government [45].

TABLE V
MEC AND IOT BENEFITS FOR EACH APPLICATION

Required characteristics of MEC and IoT	**Description**	Smart home	Smart city	Remote surgery	Remote health consultancy	Autonomous vehicles	Augmented Reality (AR)	Virtual Reality (VR)	Gaming	Retail	Wearable IoT	Farming	Smart energy	Industrial Internet
Low Latency	Optimize to process a very high volume of data messages with minimal delay		✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	
Increased Bandwidth	Ability move a large set amount of data rapidly	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓
Content Awareness	Adaptation of network characteristics according the local services requirements	✓	✓	✓			✓	✓	✓	✓	✓	✓	✓	
Low power devices	Support for low power devices which has limited transmission powers					✓	✓	✓			✓	✓	✓	✓
Fixed wireless support	Operation of wireless systems used to connect two fixed locations with a wireless link	✓	✓	✓			✓		✓	✓	✓	✓	✓	✓
Fast inter-RAT handoff	Speed up the handover takes place between different RATs	✓	✓	✓			✓	✓	✓	✓	✓			
Caching	Keeping frequently accessed information in a location close to the requester	✓	✓				✓	✓	✓	✓	✓			
Edge Analytics	An automated analytical computation is performed on data at a sensor, network switch or other device instead of waiting for the data to be sent back to a centralized data store.	✓	✓	✓			✓	✓	✓	✓	✓			✓
Application virtualization between edge and cloud	On demand application and service migration from centralized cloud to the edge cloud		✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓
Private or local network	Limit the communication and data exchanges to a certain network segment	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓
Security	Provide localized security		✓		✓		✓		✓			✓	✓	✓
Privacy	Provide localized Privacy		✓	✓	✓	✓	✓		✓		✓			
Fast Mobility	Enable the ability to move or be moved fast within the network or network coverable area		✓	✓		✓	✓		✓		✓	✓	✓	

B. Healthcare

Mobile health and telemedicine are identified as important use cases of 5G. Wearable low power IoT medical sensors for monitoring health related data and tracking records are now popular in public healthcare facilities [46]. Although IoT technologies are widely adopted in the health sector [47], their performance goals will not be achievable without edge computing solutions like MEC [37], [48], [49]. For instance, humanoid robots sitting next to an elderly person may need tactile feedback in 1ms latency for his or her care taking services. Mission critical use cases like remote surgeries require ultra-low latency, uninterrupted communication links, and collaborations among surgeons present in different locations. Remote patient monitoring is another use case which enables consultants in major cities to interact with patients residing far away from the medical facility. The frequent updates of health records for an elderly person or someone with a chronic disease needs to proceed ubiquitously and securely. With such potential use cases and scenarios, the role of MEC in health and social assistance industries becomes more evident [37].

Some research works have already been published about the cooperation between edge computing and IoT in the healthcare sector. Singh *et al.* [50] describe a military healthcare service platform based on hierarchical IoT architecture and a semantic edge network model. The hierarchical IoT architecture can collect the vital health parameters of the soldiers, their weapon status, as well as their geographical locations. The control center of the battlefield performs the role of edge component which can process and store large amount of health data sent over an SDN-based network. The preliminary network architecture proposed in [51] provides real-time context-aware collaboration for remote robotic tele-surgeries. Big data analytics performed by edge computing are also important in e-Healthcare applications [52]. Rahmani *et al.* [53] introduces the smart gateway concept for an IoT-based remote health monitoring system. Here they exploit edge computing nodes to update the centralized cloud based on the medical data generated by the IoT sensors. Their geo-distributed network of smart e-Health gateways provides local data processing for real-time notification for medical practitioners, secure and privacy preserved data gathering, patients' mobility, network interoperability, and energy efficient communication.

C. Autonomous Vehicles/IoT Automotive

5G is a key enabler of V2X (Vehicle to Everything) concept which covers Vehicle to Vehicle (V2V), vehicle to

infrastructure, vehicle to device, vehicle to pedestrian, vehicle to home and vehicle to grid [54]. In the context of IoT Automotive, V2X requires critical communication infrastructure where reliability and ultra low latency are crucial factors [55]. Use cases in these categories include autonomous and semi-autonomous driving, vehicle maintenance, and in vehicle infotainment. In order to operate an efficient and reliable vehicular network, several features have to be improved, these include real-time traffic monitoring [56], [57], continuous sensing in vehicles [58], [59], support for Infotainment applications [60] and improved security [61]. However, these features cannot be served by current mobile networks [62]. In this vein, upcoming 5G mobile systems are expected to offer a higher level of flexibility, leveraging the emerging technologies related to network softwarization [63]. In this context, V2X combined with MEC provides a viable and cost-effective solution that can accelerate development of V2X and IoT automotive systems [64].

It is important to improve the performance of RAN technologies to enable IoT automatization. MEC will play a vital role here also. For instance, MEC technologies may fulfill the latency, reliability, and throughput requirements in V2X channel modeling of mmWave communication [65]. Moreover, the placement of the MEC server within the RAN provides flexible network services for the vehicle and to efficiently control the radio network resources [66]. It is also possible to design a time-predicted handover mechanism for vehicles by leveraging road side information at MEC server in order to meet the demand for high mobility and reliability in vehicular networks [66].

In addition, ICN-MEC integration can also tackle existing technical challenges such as massive mobility of vehicles, scalability, deployment strategies, service orchestration, massive data handling, fast big data processing, as well as ensuring security and privacy [67].

Unmanned aerial vehicles (UAVs) or drones are another type of autonomous vehicles which are capable of sensing its environment and navigating without human inputs. UAV use cases include but not limited to, public safety, smart agriculture, surveillance, and environmental monitoring [68]. In order to maximize the flight time, the UAV battery life should be essentially conserved by minimizing the overhead onboard. When the required processing power exceeds the available resources on UAV, the application data can be offloaded to MEC. Accompanying the advanced RATs, MEC will facilitate the offloading process from UAV due to its expected wide deployment in the network [68].

D. Gaming, AR and VR

Mixed reality (MR) combines virtual reality (VR) and augmented reality (AR) technologies thereby enabling humans to interact more naturally with the virtual worlds based on data aggregated by IoT devices [69]. With IoT, AR technologies are able to benefit directly from the high end interconnection of objects that characterizes the IoT environment through which users can extend their interactions from the real world to the virtual world [2], [70]. Convergence of VR and IoT can occur in many ways such as telepresence, tourism industry, smart transportation networks, and robotic assisted surgeries. Exclusive AR and VR experiences with the delivery of 360° navigable videos will be offered by enhanced mobile broadband connections with low latency and high reliability for mission-critical services. With present-day network standards, this might be impossible to achieve, however with the predicted characteristics of 5G such as 20 Gbps peak data rate and 1 ms round-trip over-the-air latency, this becomes more easily achievable. As identified by ETSI, MEC will be an ideal solution for low-latency offload services in AR and VR applications that combine computer generated data with physical reality [71]. While operating VR devices over wireless links and deploying the VR control center at MEC server, the tracking accuracy can be increased with round trip latency of 1 ms and high reliability [72]. Migrating computationally intensive tasks to edge servers will increase the computational capacity of VR devices and save their battery-life. Furthermore, MEC will allow VR devices to access cloud resources in an on-demand fashion [73].

MEC platforms provide high capacity and low latency wireless coverage for large venues like stadiums or smart cities with a massive density of users to enjoy the AR and VR experience. For instance, inside a smart building with a network of cameras, obtaining raw video frames and preparing the processed frames for display can be performed locally with the help of edge computing. Furthermore, tracking the local position of the user or object, building a model of the environment, and identifying known objects in the environment can be offloaded to the edge cloud. Similarly, in order to get absolute experience of VR glasses, the response time should be extremely low. When the user moves his head, he may experience delay if the glasses need to access remote data centers. Therefore, the expected interaction time between machines and humans needs to be less than 1 ms. When the latency of a VR application is more than 1 ms, the user will experience cyber sickness which will be interrupting the real VR experience. MEC servers in the nearest proximity will be able to serve such applications with ultra low latency. Future games will be played beyond the entertainment purposes on top of VR and AR applications which would require the minimum possible latency. Pokmon Go and Ingress are two examples of successful games that combine AR and sensor information such as user location.

E. Retail

The second largest MEC use case is expected to be in the retail businesses [37]. Currently, IoT has dominated retail market applications in many ways including digital signage, supply chain management, intelligent payment solutions, smart vending machines, shelves, doors, resource management, streaming, and safety. The high class retail stores which use facial recognition systems need high definition cameras that generate huge volumes of data requiring powerful servers within the premises. Therefore, the on-site MEC servers will assist to process these kind of large data sets produced by IoT devices in a retail market. Big data analytics

in shopping centers can further exploit the collaborative processing between edge and cloud computing [52]. Installation of MEC in a retail market also provides high speed mobile coverage throughout the store. WiFi access points that are maintained per store can be connected to the MEC server to provide WiFi connectivity for store customers as needed. The enabling of MEC will also omit load balancing, Wi-Fi controllers, or policy engines required in the wide area networks in the store. Although not many academic published research works are explicitly focusing on MEC and IoT [74], they have become enormously reputed and commercialized technologies in the industry and the business sectors.

F. Wearable IoT (WIoT)

During the previous years, wearable technology has evolved tremendously from walkman to step trackers, smart watches to smart glasses. The development of low power wireless technologies such as BLE (Bluetooth Low Energy) fuels the development of wearable devices. Present-day wearables span from low-end devices such as health and fitness trackers to high-end devices such as VR/AR helmets and smart watches. It is expected that wearables will become the worlds best-selling consumer electronics product after smartphones with a global availability of more than 929 million devices by 2021 [75]. With the new application domains and enabling services, wearable devices will demand more sophisticated communication infrastructures. For instance, VR/AR wearables are demanding gigabit/s throughput network connectivity to run their applications. On the other hand, dense deployment of wearable devices in smart cities will increase the network traffic on communication networks. Thus, the next generation communication networks should be able to provide the gigabit experience for the anticipated ultra dense wearable devices [76].

Although cloud computing has enabled wide range of new networking services, it cannot alone fulfill the upcoming requirements for the future wearable ecosystem. Mainly, the centralized cloud data centers fails due to long End-to-End (E2E) latency. Delay-sensitive wearable applications such as VR perceptual stability requires ultra low delay. In this context, MEC has the potential to solve the limitations in current cloud based systems, by combining cloud and MEC infrastructures. This will enable providers deploy storage, computing, and caching capabilities in close proximity with such wearable devices [76].

G. IoT in Mechanized Agriculture

In order to meet the demands for future food production, the agricultural sector will require some major evolution where IoT will be integrated in various production, management, and analytical processes [77], [78]. The present-day agricultural sector has been slow to adopting the emerging Machine-to-Machine (M2M) and IoT technologies when compared with other sectors like smart cities and the medical fields [79].

Precision farming and smart agriculture can be achieved using autonomous vehicles (tractors), remote monitoring, and real-time analytics. It is reported that farmers are increasingly turning to agricultural drones and satellites to survey their lands and generate crop data. IoT sensors may provide information about crop yields, rainfall, pest infestation, and soil nutrition which are invaluable to production and can improve farming techniques over time. Although low latency is not a critical requirement in smart farming environment, management of large data sets will be a key requirement to consider. MEC servers located on-site can assist high tech farming by collecting and analyzing big data on agriculture in order to maximize efficiency. Likewise, without moving everyday farming applications to a remote cloud, MEC platforms can benefit in terms of data access, synchronization, storage and other overhead costs the farmer might normally incur.

The use of IoT-based automated data collection and monitoring systems in poultry houses can be used to increase work efficiency and service quality, and get a deeper understanding of chicken nurturing [80]. Sensing technologies can be used in carbon dioxide and luminosity sensing, these are important parameters in large scale poultry houses. Gas sensors can be used to get all necessary information to prevent chicken infertility due to problems such as low carbon dioxide levels. Luminosity senors can help to maintain the proper luminosity level for optimum productivity. Similar to smart farms, low latency is not a critical requirement in smart poultry houses [80]. However, it is critical to manage large data sets where on-site MEC servers can be used. In addition, sharing the data between poultry houses and storing legacy data in centralized servers are important in identifying abnormal incidents in the farm [81]. With the use of MEC, poultry houses can work with intermittent connectivity to the centralized clouds. In that case, MEC servers can temporarily hold the data until farms are connected with the centralized clouds.

H. Smart Energy

The smart grid system is an Information Communication Technology (ICT)-enabled energy generation, transmission and distribution network. It has capabilities to continuously sense, analyze, and monitor both energy flow and energy transportation infrastructure. Such features are enabled by adding digital controls and enabling network monitoring and telecommunication capabilities. As a result, a smart grid does not only provide two-way flows of electrical power, but also enables real-time, automated, bidirectional flow of information. Adding such smartness to the aging energy infrastructure will foster a more efficient energy system.

IoT is considered as the foundation for realizing intelligence capabilities in smart grid systems. IoT integrates the Internet-connectivity into all kinds of grid components such as transformers, breakers, switches, meters, relays, intelligent electronic devices, capacitor banks, voltage regulators, cameras and many more. These IoT devices are then used to capture the data required to enable automations. IoT-enabled smart grids provide several benefits such as reduced capital expenditure, optimized renewable capacity, lowered maintenance costs and enhanced customer engagement. On one hand, the transformation of an electrical grid into a smart system requires nearly every device and piece of equipment to have

TABLE VI
THE REVIEWED STATE-OF-THE-ART MEC INTEGRATION IN DIFFERENT IOT APPLICATIONS

Ref.	Description	Smart Home	Smart City	Healthcare	IoT Automotive	Gaming, AR, VR	Retail	Wearable IoT	Smart Agriculture	Smart Energy	Industrial Internet
[40]	Preliminary design of deploying MEC server functionalities in a smart home to realize IoT gateway with direct M2M interaction in LTE networks	✓									
[41]	Introduce Gateway-as-a-Service for heterogeneous IoT devices on top of the virtualization technologies in edge computing.	✓							✓		
[44]	Propose an autonomic creation of MEC services to enhance QoS of video streaming in smart cities.		✓								
[50]	Propose a semantic edge-based IoT architecture for military health services in battlefield.			✓							
[51]	Provide a conceptual MEC based architecture for mission-critical context aware collaboration in remote surgeries.			✓							
[53]	Describe and implement a smart e-Health gateway at the edge of the network suitable for ubiquitous healthcare systems.			✓							
[64]	Analysis on research and engineering challenges co-existence of cloud, edge computing and data caching strategies at the edge for vehicular networks.				✓						
[82]	Discuss the design aspects for the radio access in 5G V2X.				✓						
[65]	Discuss the benefits of merging MEC and mmWave technologies for 5G applications.				✓	✓					✓
[66]	Propose a novel MEC-based architecture for future cellular vehicular networks.				✓						
[67]	Discuss the benefits of combining ICN and MEC in the context of connected vehicle environments.				✓						
[52]	Propose a framework for big data analytics between edge and cloud computing platforms.			✓		✓					
[74]	Design and implement a fog computing based framework that support sharing and reusing contextual data across services in smart city and retail stores.		✓				✓				
[83]	Present a usecase of MEC for Tactile Internet based 5G gaming application.					✓					
[84]	A demonstration of MEC for Tactile Internet based 5G gaming application.					✓					
[76]	Discuss the role of MEC in 5G WIoT communication and its challenges.			✓				✓			
[68]	Propose an UAV-based IoT platform for a crowd surveillance use case.				✓				✓		
[78]	Develop and test a ubiquitous sensor network platform for crop lands automation maintenance in precision agriculture.								✓		
[70]	Present a serverless edge computing architecture that enables the offloading of mobile computation with low latency and high throughput, using a mobile AR application.					✓					
[85]	Discuss the benefits of MEC and edge computing (EC) to enhance the security of smart grids.									✓	
[86]	Present a method to optimize the EC based video streaming schemes for Industrial IoT.										✓
[87]	Present the use of edge computing to provide elastic resources and services to enable microdatabases architecture for IIoT.										✓
[88]	Propose a fog-based communication architecture for Industry 4.0 applications.										✓
[73]	Describe research directions and enablers of wireless interconnected VR systems.					✓					
[89]	Design an optimization framework for VR/AR communication via small-cell cooperation.					✓					

built-in, secure, interconnected intelligence. On the other hand, an efficient system is required to manage the generated data, i.e., transferring, storing, and analyzing such huge amounts of data which are collected from these smart devices. Therefore, cloud computing is a viable solution to these IoT-based smart grids [90].

Generally, smart grids are spanning over large geographical areas. They often confront bandwidth bottlenecks and communication delays due to poor network connectivity and vast number of devices generating data. Thus, the traditional centralized cloud architecture is not suitable for the domain of the smart grid since it relies heavily on centralized processing [91]. Many delay sensitive smart grid applications, such as fault detection, isolation and service restoration or Volt/VAR optimization cannot tolerate round trip delay to access centralized cloud systems. MEC is identified as the viable cloud computing option to address these limitations. MEC allows the computation to be performed closer to the data source. Moreover, the potential attack points for the grid is increasing with the growth of ubiquitous sensor deployment. Every smart IoT device can be vulnerable to potential attacks. MEC provides the opportunity to enforce security mechanism closer to the end devices. As such, even if an attacker gains access to an endpoint device, the attack gets no further information beyond the local network segment since MEC has capabilities to notice the intrusion and cease the accessibility [85].

I. Industrial Internet

The Industrial Internet of Things (IIoT), also known as Industry 4.0 [92] is an application of IoT in the domain of

manufacturing. IIoT incorporates numerous advanced communication and automation technologies such as M2M communication, machine learning and big data analytics to improve intelligence and the connectivity [93]. For instance, IIoT networks can connect all of the employees data and processes from the factory floor and forward them to the executive offices. Thus, decision makers or employees can create a full and accurate view of their manufacturing process by using IIoT network, hence improving their ability to make more informed decisions. IIoT also helps the exploitation as well as implementation of new intelligent technologies to accelerate the innovation and transformation of the factory workforce [92].

Primarily, IIoT is seen as a way to improve operational efficiency. However, IIoT provides a wide range of other benefits such as improving connectivity, efficiency, scalability, time savings, as well as cost savings for manufacturing processes with the maximum use of smart machines [92], [94]. In general, these smart machines operate with higher accuracy, greater efficiency and constant working capabilities than humans [95]. Thus, IIoT has great potential for improving quality control, sustainability and overall supply chain efficiency.

MEC will play a vital role in enabling future IIoT applications [96] by addressing the shortcomings of M2M communication (e.g., latency, resilience, cost, peer-to-peer, connectivity, security) in IIoT domain [97], [98]. Current market trends already show that edge computing will represent many implementation scenarios for IIoT. For instance, real-time edge analytics and enhanced edge security are two key drivers in the creation of new IIoT deployments. Thus, the addition of MEC in IIoT networks will fuel the evolution of IIoT as well as create new business applications [99].

One way to optimize the use of conventional edge computing in video streaming schemes for IIoT is presented in [86]. By using machine learning algorithms, edge computing can process the sensor data before transmitting to the cloud. This mitigates against the degradation of service quality of the video streaming. Aggregation of all the sensor data to a single data center increases latency and raises performance concerns in IIoT domain. In order to solve this issue, a microdatabase architecture is proposed for the Industrial Internet [87]. It holds the data close to the industrial processes, but also makes it available near the applications that can benefit from the data. Edge computing also provides elastic resources and services to enable micro-database architecture [87]. A fog-based communication architecture for Industry 4.0 applications is proposed in [88]. This approach will substantially minimize the energy consumption of the IoT nodes. Edge computational capabilities are further used to predict future data measurements and reduce the throughput from IoT devices to the control unit.

III. Technical Aspects of MEC Enabled IoT

To realize the MEC exploitation for IoT applications, the key value propositions are mostly seen from the technical parameters such as scalability, communication, computation offloading and resource allocation, mobility management, security, privacy, and trust management. This section describes the state-of-the-art of each of these technical parameters, hence giving a clear background against which the benefits of MEC can be envisioned.

A. Scalability

1) Requirements: When it comes to actual deployment of MEC platform for IoT systems, scalability is a key factor to consider. The compatibility of MEC servers to multiple network environments is one of the factors that will drive its large scale adoption in future networks [100]. The IoT environment will consist of hundreds of billions of sensors, actuators, Radio-Frequency Identification (RFID)-tagged objects, software, vehicles, and embedded systems all interconnected in a huge network of cyber-physical systems. At a utility scale consideration, these devices will be working in close collaboration to deliver the expected services in technologies like the smart grids, virtual power plants, smart homes, intelligent transportation and smart cities. That being said, the role of scalability to the realization of such a hyper-connected IoT environment becomes more obvious. The IoT environment will require a dynamic range of capabilities in the network space if such large numbers of devices are to be supported effectively.

2) Related Work: Currently, MEC servers have been confirmed to be compatible with LTE macro base station (eNodeB) sites, 3G Radio Network Controller (RNC) site, multi-Radio Access Technology (RAT) cell aggregation site, and at the edge of the core network [2]. Such multi-RAT cell aggregation schemes can be implemented indoor or outdoor settings depending on the requirements. This invariably enables MEC to be applied to many different possible scenarios. The larger the deployment scenarios for MEC the more the range of capabilities it can handle, this also translates to higher scalability for MEC-enable technologies like IoT.

Designing an edge cloud network implies that an optimal location for citing the cloud facility is first determined. Ceselli *et al.* [105] present a design optimization scheme for the MEC architecture based on link-path formulation supported by heuristics in order to optimize the computation time for the scheme. In this approach, consideration is given to both users and VMs mobility. Hence, an optimal point to install the MEC server is determined through a tread-off between installation cost and the quality of service to be delivered. Table VII compares the reviewed state-of-the-art scalability feature in MEC enabled IoT.

B. Communication

1) Requirements: There are three main categories for the communication concerns about MEC [100]: Wireless access while offloading to the mobile edge host; Backhaul access while offloading to a remote cloud server; Communication among IoT devices, mobile edge host, and remote cloud servers when they collaboratively execute multiple jobs. The first and the second categories are the most renowned on behalf of the MEC servers which are the small scale data centers deployed by the network operators and can be co-located with the Wireless Access Points (WAPs). In the IoT supportive MEC systems, the consumer devices may communicate with

TABLE VII
COMPARISON OF THE REVIEWED STATE-OF-THE-ART SCALABILITY FEATURE IN MEC ENABLED IOT

Ref.	Description	IoT application /domain /feature	Addressing	Search
[101]	Discusses the challenges in searching imposed by the burgeoning field of IoT.	General IoT		✓
[94]	Examines a variety of popular and innovative IoT solutions in terms of context-aware technology perspectives, to serve as a conceptual framework for context-aware product development and research in the IoT paradigm	General IoT solutions.	✓	
[102]	Proposes an innovative distributed architecture combining machine-to-machine industry-mature protocols (i.e., MQTT and CoAP) in an original way to enhance the scalability of gateways for the efficient IoT-cloud integration	IoT cloud integration.	✓	✓
[103]	Studies an implementation of edge computing, which exploits transparent computing to build scalable IoT platforms using transparent computing.	Wearable IoT	✓	
[104]	Introduces a lightweight edge gateway for the IoT architecture using container-based virtualization techniques.	General IoT		✓

the MEC servers either directly or with the support of neighboring devices using Device-to-Device (D2D) communication. For the third category, WAPs enable access to the remote data centers in the central cloud through backhaul links.

In order to reap the maximum advantage of computation offloading leveraged at the edge servers, MEC systems need efficient communication channels. Unlike the wired connections in the conventional grid computing and cloud computing, the wireless access links between the mobile devices and cloud computing resources in the edge computing paradigm can be unstable. Sudden service outages may occur with the interruption of access links. The inherent challenges with wireless communication channels like multi-path fading, interference, and spectrum shortage should always be taken into account for the design of MEC systems to seamlessly integrate computation offloading and radio resource management [32]. Moreover, both wireless and backhaul access links have limited capacities which should be properly shared among mobile devices in a similar way as sharing the computing resources of the MEC server. Hence, having a cooperative scheme for the joint allocation of communication and computation resources is important for the successful deployment of MEC [100]. Redesigning both communication and networking protocols to integrate communication infrastructures in MEC and IoT systems is a challenging task. The key focus should be on improving the computation efficiency with respect to data transmission.

Another major requirement is to maintain interoperability while addressing heterogeneous communication technologies that have to be utilized in IoT and MEC paradigms in 5G. There are plenty of radio technologies that facilitate IoT Low-Power Wide Area Networks (LPWANs) (e.g., WCDMA, LTE, narrowband IoT (NB-IoT), Wi-Fi, Bluetooth, Zigbee, SIGFOX and LoRA). The choice of these LPWAN technologies may create trade-offs among signal strength, operational range, throughput, and power consumption. With the arrival of 5G, the convergence of these communication technologies needs to be achieved since one network will not be fitting based on those trade-offs.

2) Related Work: Recently, Fog-Radio Access Network (F-RAN) was introduced by Peng *et al.* [106] to consolidate the heterogeneous networks into a single network architecture with 5G even though they do not operate in the same bands to gain high spectral and operating and energy efficiency. Well known Cloud Radio Access Network (C-RAN) architecture can perform cooperative transmission across multiple edge nodes with centralized cloud computing servers via fronthaul links [107]. Although, C-RAN provides high spectral efficiencies due to the enhanced interference management capabilities with the centralized baseband processing at the cloud, it has potentially large latencies. F-RAN is proposed for 5G MEC deployments as an advanced socially aware mobile networking architecture to provide high spectral efficiency while maintaining high energy efficiency and low latency [106], [107]. Precoding design, resource block allocation, user scheduling, and cell association are jointly designed for radio resource allocation in F-RANs in order to optimize spectral and energy efficiencies, and latency performances [108]. Rimal *et al.* [109] propose a unified Time-Division Multiple Access (TDMA) based resource management scheme for offloading traffic over Fiber-enabled Wireless (FiWi) access networks.

In the envisioned 5G systems and MEC architecture, both backhaul and wireless access links can be facilitated by millimeter-Wave (mmW) spectrum [110]. The use of mmW spectrum will enable high data rate access to MEC functionalities with low latency. On the other hand, MEC provides local computation power usefully for optimizing the performance of mmW communications. Barbarossa *et al.* [111], [112] address the joint optimization of communication/computation resources with mmW communication. They have taken the advantage of blocking probabilities by considering intermittency of mmW multi-link communications.

An open source LPWAN infrastructure called OpenChirp is discussed in [113]. OpenChirp, which is developed using LoRWAN, allows multiple users to provision and to manage battery-powered transducers across large areas like campuses, industrial zones, or cities. As pointed out in [30] and [114], SDN plays a vital role in improving MEC type technologies by removing the technical shortcomings in edge computing implementations. The authors summarize the work performed for implementing MEC based on NFV and SDN where the SDN controller manages the communication between MEC servers which form a data center at the edge. Table VIII summarizes the reviewed state-of-the-art communication issues and solutions in MEC enabled IoT.

TABLE VIII
COMPARISON OF THE REVIEWED STATE-OF-THE-ART COMMUNICATION ISSUES AND SOLUTIONS IN MEC ENABLED IOT

Ref.	Description	IoT application /domain /feature	Comm. network architecture	Comm. resource allocation
[109]	Performance analysis of radio resource allocation in F-RANs for edge cache and adaptive model selection to improve spectral efficiency and energy efficiency.	Low latency and high reliability		✓
[112], [113]	Use of mmWave spectrum for high data rate access to MEC servers and backhaul links.	Low latency and high reliability		✓
[114]	An open source LPWAN infrastructure which allows multiple users to provision and manage battery-powered transducers across large areas.	LPWAN infrastructure	✓	
[42]	A virtualized edge computing architecture with a proxy VM migration scheme to minimize traffic in the core network.	IoT big data streams	✓	
[115]	Proposed network architecture includes multi-interface wireless access network (e.g., FiWi), heterogeneous backhauling, distributed cloudlets, hierarchical structure of a cloudlet, and the SDN based mobile core network.	IoT big data streams	✓	
[110]	A novel unified resource management scheme for Ethernet-based FiWi networks that jointly allocates bandwidth for transmissions of both conventional broadband traffic and MEC data in a TDMA fashion.	Mission-critical IoT		✓
[116]	Introduce Mobile-IoT-Federation-as-a-Service (MIFaaS) to enable dynamic cooperation among private/public local clouds of IoT devices at the edge of the cellular infrastructure. The selection of the best configuration of federated IoT cloud platforms are modeled as a coalition formation problem.	Cellular IoT		✓
[117]	Allocation of radio resources in a joint LTE and NB-IoT system based of MIFaas paradigm [116]. Discovered that in handling high-end IoT data traffic, a combination between NB-IoT and LTE is essential in providing the needed high data rate and low latency.	Mission-critical IoT		✓
[118]	Integration of D2D communications into edge computing environment reduce transmission delay and traffic load across the network.	Mission-critical IoT		✓
[119]	Use the theories of stochastic geometry, queueing, and parallel computing for provisioning and planning MEC networks.	Communication latency	✓	

C. Computation Offloading and Resource Allocation

1) Requirements: Computation offloading is the most prominent and widely discussed feature of MEC that empowers resource-constrained IoT devices with augmented computational capabilities [29], [33]. This will not only prolong the battery life of the IoT sensor nodes, but also reduce E2E latency needed to run sophisticated applications. In the first place, UE has to decide whether to execute the relatively simple tasks locally or offload to the MEC servers (i.e., task model for binary offloading) [32]. Secondly, the decision of computation offloading to the MEC servers can be performed fully or partially. In the partial offloading, a subset of computations is executed locally while the rest is offloaded to the MEC server by considering several factors such as users or application preferences (e.g., application buffer state), radio and backhaul connections quality (i.e., between UE and MEC servers), UE capabilities, or cloud capabilities, and availability [29].

The sole objective of the offloading policies need to be the minimization of execution delay. Other critical concerns are to define the dependency of offloadable components of the applications based on their ability to partition data (e.g., real-time user input has to be processed at UE without offloading) and to predict the execution time of multiple tasks. The execution order or routines have to be carefully formulated since certain outcomes can be the inputs of other tasks. As pointed out in [32], the task models for partial offloading can be represented by task-call graphs with sequential, parallel, and general dependencies.

Although in MEC, computation offloading enables powerful cloud services at the edge level, the insufficient battery energy at the tiny IoT devices may incur new challenges. In applications like IoT surveillance or remote asset management, the nodes are typically hard to reach. Those applications may also require to offload data more frequently in small chunks by consuming more energy. Therefore, it is necessary to consider not only the trade-off between energy consumption and execution delay in both full and partial offloading scenarios in MEC, but also the trade-off between computation energy and transmission energy consumption in order to extend battery life.

The joint computation and communication resource allocation should be properly addressed in order to get the maximum utilization of available resources. Single MEC server will be allocated for the applications which cannot be partitioned. The resources in multiple MEC servers are allocated for the offloaded applications that can be split into several parts. When a job arrives at the MEC server, if there are enough resources, the scheduler has to allocate the VM for further processing. If there are no sufficient computation resources, it delegates the task to the centralized cloud. MEC servers also have to allocate computation and communication resources for user application jobs and MEC service jobs. User mobility, network topology, network scalability, and load balancing are some other factors to be considered in order to define fare resource utilization policies on MEC servers. Specifically when IoT gateways share limited bandwidth among multiple IoT devices which can handle video, audio or bio-medical signals, the allocation of bandwidth will become challenging [119]. The low power wireless technologies (e.g., BLE, ZigBee, low power Wi-Fi, and LPWAN standards like LoRA or SigFox) used in IoT networks have limited bandwidth. When the IoT devices access the MEC server, which is acting as the IoT gateway, they have

to utilize either of those low-power wireless connections that have low bandwidth.

2) Related Work: In the comprehensive survey presented in [29], the existing work that addresses MEC computation offloading decisions have been nicely summarized based on full and partial offloading types. These solutions are proposed either to minimize the execution delay or to balance the trade-off between energy consumption and latency. Moreover, [29] provides an overview of the latest research works that address the allocation of computation resources for the data or application which it decides to offload in MEC systems. However, this analysis does not address the explicit applicability of computation offloading and resource allocation in IoT supportive MEC systems.

A preliminary study on how computation offloading and bandwidth allocation can be performed in MEC supportive IoT networks is presented in [119]. Due to the discrete and coarse-grained offloading levels on the IoT end nodes, the gateway (i.e., MEC server) bandwidth will be under-utilized. This phenomenon is termed fragmentation. Based on the received transmission rates and power consumption parameters of IoT devices, the gateway runs an iterative algorithm to optimally allocate bandwidth in such a way as to optimize the battery life of the devices. The implementation of the algorithm for a health monitoring application shows more than 40% improvement in using gateway bandwidth and up to 1.5 hour improvement in battery life of IoT devices. Replisom [120] designed by Abdelwahab *et al.*, is a model for computation offloading for massive IoT applications where the replicated memory objects produced by IoT devices are offloaded to the LTE-aware edge cloud. Replisom protocol relies on D2D communication for effectively scheduling the memory replication occasions to resolve interference and scarcity in radio resources as a large number of devices simultaneously transmit their memory replicas.

Furthermore, with the advent of mobile device performance and D2D communication technologies, computation offloading can be performed at the mobile devices. As shown in [128], a collection of co-located mobile devices can be utilized to provide cloud services at the edge instead of using MEC servers. Such an offloading mechanism will allow the very constrained tiny IoT devices to outsource the computation intensive tasks to the high performing mobile devices in the closest proximity. Few research efforts were performed to derive computation offloading strategies in MEC that support user mobility. Chen *et al.* [129] propose a hybrid computation offloading mechanism for edge computing considering the hardware heterogeneity of the mobile devices, various users requirements on Quality of Experience (QoE) and the heterogeneity status of the network.

The requests for computation offloading generated by end devices have to be handled by the software load balancer according to the availability of the MEC servers and resources. Yu *et al.* [121] proposes a softwarized load balancer technique called SDLB for edge computing based on the minimal perfect hashing algorithm. Their scalable and dynamic load balancer SDLB is derived based on POG data structure and able to support about one million update requests per second. Vilalta *et al.* [122] propose a virtualized network architecture with intelligent resource allocation capabilities for NFV, MEC and IoT services. This so called TelcoFog architecture provides seamless and unified control for the complete visibility, computation, and allocation of both cloud and network resources through different network segments (access, aggregation, and transport) assuming heterogeneous access and transport technologies (e.g., Wi-Fi, packet switching, optical transmission).

The game theoretic approach is also designed for selecting the most appropriate wireless channels to transmit offloading data in a multi-user multi-channel MEC systems [130], [131]. In [132], the MEC server makes the offloading decisions and physical resource block allocation to the UEs using the graph coloring method. Furthermore, Bouet and Conan [123] propose a graph-based algorithm that takes into account, the maximum MEC server capacity, provides a partition of geographic area, and consolidates as many communications as possible at the edge. The offloading architecture proposed in [124], addresses the scaling of offloading support to large-scale IoT environments. Their application level task scheduler uses horizontal scaling to allocate the available resources in the edge cloud. Moreover, content caching strategy is also considered in some work for the optimized joint computation and communication resource allocation [125]. Table IX summarizes the reviewed state-of-the-art computation offloading and resource allocation features in MEC enabled IoT.

D. Mobility Management

1) Requirements: A more general concept in cellular and IP networks is mobility management for moving users. Since earlier generations of mobile cellular networks, mobility management has been the ultimate way of ensuring that mobile services are delivered to subscribers wherever they are within the coverage areas of the service provider. The cellular network is a radio network that consists of multiple base stations; each base station is designated to provide mobile services within a particular cell, and hence combining several base stations enables the service provider to cover wider geographical locations. In LTE, mobility management advanced significantly through the introduction of moving networks, seamless roaming, and vertical handovers which is enabled when the UE changes the serving eNB/SCeNB.

In the case of MEC, mobility management is particularly crucial, given that when mobile UEs move far away from the computing node, then there is the possibility of degrading the QoS due to latency. A severe degradation could lead to a complete disconnection of a UE from the MEC network. In MEC-enabled IoT, a large majority of the nodes will be mobile nodes, hence the goal is to exploit MEC services to offer an ultra-reliable mobility management scheme for IoT applications. In traditional mobile networks, the key issues with mobility management are mainly connectivity, location management, routing group formation, seamless mobility, mobility context management, and migration among others. Among these issues, seamless mobility tends to be the most trivial. There is a need for mobile devices to have uninterrupted access

TABLE IX
COMPARISON OF THE REVIEWED STATE-OF-THE-ART COMPUTATION OFFLOADING AND RESOURCE ALLOCATION FEATURES IN MEC ENABLED IOT

Ref.	Description	IoT application /domain /feature	Computation Offloading	Comp. Resource Allocation
[120]	Management of computation offloading in a local IoT network with the efficient utilization of IoT gateway bandwidth constraints.	IoT-gateway	✓	
[121]	Replicated memory objects produced by IoT devices are offloaded to the LTE-aware edge cloud based on D2D communication.	Massive-IoT	✓	
[122]	Proposes a portable MEC load balancer which is scalable, software based, memory efficient and adaptive to device heterogeneity. The design takes the advantages of SDN and POG data structure.	IoT big data streams		✓
[123]	Defines an architecture to allocate cloud and edge resources for deploying NFV, MEC, and IoT services on top of a telecom operator's network.	Low latency		✓
[124]	Propose a MEC clustering algorithm to consolidate the maximum communications at the edge which stands for the spatial temporal dynamics of the traffic.	IoT big data streams		✓
[125]	Defines a scalable offloading architecture and a simulator with multi-tenancy ability and dynamic horizontal scaling based on Amazon Autoscale service-oriented architecture.	Massive-IoT	✓	✓
[126]	Formulate the computation offloading decision, resource allocation, and content caching in wireless cellular networks with mobile edge computing as an optimization problem and solve it applying alternating direction method of multipliers based distributed algorithm.	Cellular IoT	✓	✓
[127]	Introduces asymptotically optimal offloading schedules, which are tolerant to partial out-of-date network knowledge and stochastically maximize a time-average network utility balancing system throughput and fairness.	Massive IoT	✓	✓
[128]	Develop a toolkit for modeling and simulation of resource management techniques in the IoT, edge and fog computing environments	General IoT		✓

to information, communication, monitoring and control when, where and how they want, regardless of the device, service, network or location. For the MEC architecture, using such traditional approach to mobility management will certainly lead to a degraded performance in the overall MEC network; one key reason for this shortfall is due to the co-provision of radio access and computing services of the MEC-enabled base stations.

2) Related Work: Several mobility management policies have been proposed for the MEC architecture [29], [133]–[135]. Sun *et al.* [133] developed a novel user-centric Energy-aware Mobility Management (EMM) scheme based on Lyapunov optimization and multi-armed bandit theories. The EMM scheme works in an online fashion without using future system state information is hence able to manage the imperfect system state information. The goal of EMM is to optimize the offloading delay that results from both radio access and computation, under the long-term energy consumption constraint of the user. Here, the experiment results showed that the proposed algorithms can optimize the delay performance while approximately satisfying the energy consumption budget of the user. However a major issue with this algorithm is that it will not be effective for a high mobility scenario where a connected node will move in a great deal during the processing of a task, and such high mobility scenario is a typical feature of the IoT networks.

Mach and Becvar [29] presented a user-oriented use case of MEC from the perspective of computational offloading and mobility management. They first discuss the power control approach where the mobility management entity regulates the transmission power of the eNB/SCeNB, which is mostly used in scenarios where the UEs mobility is confined within a given space such as an office room [29], [136], [137]. The principle of this approach is depicted in Figure 4. Accordingly, the MEC services are extended to slowly moving IoT devices

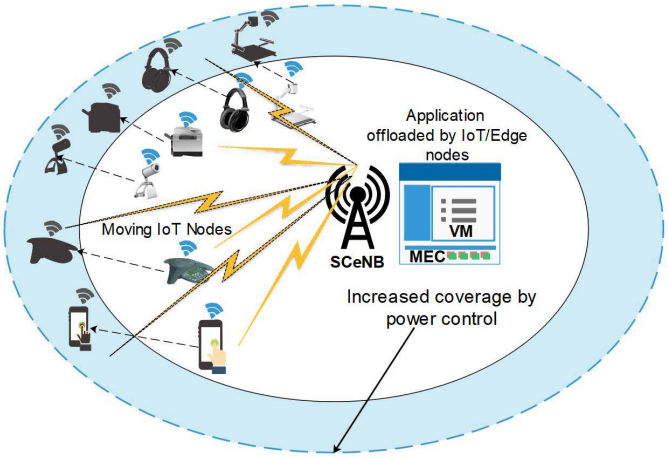

Fig. 4. CaPC Power Control Principle [29].

within a given space by adjusting the transmission power of the serving and/or neighboring SCeNBs. This Cloud-aware Power Control (CaPC) algorithm is mostly suitable for managing the offloading of real-time applications where delay requirements are strict. It allows the MEC system to handle higher amounts of offloaded applications within specific latency constraint. Typically, increasing the transmission power of SCeNB will momentarily increase the coverage region of MEC signals, hence allowing IoT nodes to move beyond the default coverage region for the duration of the power boost. This will help to avoid the need for handover as much as possible, especially in cases where the moving distance of the IoT device is relatively small. The moving IoT devices are able to roam certain distance away from the coverage region of MEC services just by adapting the transmission power of the eNB/SCeNB, without discontinuity in service and handovers.

Another scenario is when the IoT node decides to initiate an offload either within the coverage region increased by power

control or as it roams beyond. Two possible procedures could be used in this case; one is by performing a VM migration, i.e., migrating a VM from the less effective to a more effective computing node, and two is by path selection, i.e., selecting a new path for communication between the computing node and the IoT device. The need for VM migration arises when the IoT node roams beyond the region extended by the power control mechanism. In that case, the risk of service discontinuity and poor QoS factors tend to be higher, hence there is a need to strategically design the VM migration process. Analysis of the influence of such migration on the performance of a typical IoT node is described in [138], using the Markov chain analytical models. Based on the outcome of the analysis, when VM migration is not implemented, the probability that the edge device will connect to the optimal MEC decreases with the increase in hops between the eNB and the UE. Meanwhile there is also an additional delay that occurs in when VM migration is not used. In addition to the literature mentioned in [29], Table X summarizes the reviewed state-of-the-art mobility management in MEC enabled IoT.

E. Security

1) Requirements: Integrating MEC capabilities to the IoT systems come with an assurance of better performance in terms of quality of service and ease of implementation. This however, raises concerns in both research and the industry first on the heterogeneity of connected devices, and second on the potential repercussions of such architectural modification on the overall security of MEC-enabled systems. Typical security threats in these areas are Denial of Service (DoS) attacks, Man-in-the-Middle (MitM) attacks and malicious node problems [34], [143]. More detailed descriptions of these threats are presented in [34].

IoT systems in general inherit most of the security vulnerabilities commonly found on sensor networks, mobile communication networks and the Internet as a whole. Thus making security one of the application challenges of IoT in present and future networks. Such security vulnerabilities in IoT networks include DoS/Distributed DoS (DDoS) attacks, forgery/middle attack, heterogeneous network attacks, application risk of IPv6, Wireless Local Area Networking (WLAN) application conflicts also affect the transport security of IoT [144].

Here we define the possible security attacks in the context of MEC-enabled IoT environment. Security threats are mostly targeted towards the MEC nodes, e.g., MEC server and other IoT nodes. In DoS attacks, the adversaries tend to attack critical networking or computing resources by sending requests at rates that are beyond the handling capacity of such networking or computing equipment, hence inundating such facility and preventing other users or nodes from getting access to the resources offered. DoS attacks could happen in the form of DDoS or wireless jamming and could be launched on both the virtualization and network infrastructures.

MitM happens when an adversary interposes between two nodes or entities and secretly relaying or altering the communication between such parties, common example is the MitM attack between a server and a client. For the MEC-enabled IoT scenario, the most vulnerable location for MitM attack is the infrastructure layer where the malicious attacker tries to hijack certain segments of the network and begins to launch attacks like eavesdropping and phishing on connected devices. As claimed in [145] MitM attacks can be launched between 3G and WLAN networks. Such attacks would be even more threatening for the MEC-enabled IoT scenario, given that MEC relies heavily on virtualization, hence launching a MitM attack on multiple VMs could very easily affect all other elements on both sides of the attack.

VM Manipulation is a typical attack for all virtualized and edge computing systems. In MEC-enabled IoT system, VM manipulation is mainly targeted towards the virtualization infrastructures. In this case, the attacker is more likely to be a malicious insider with enough privileges or a VM that has escalated privileges. The adversary in such attack begins to launch multiple attacks to the VMs running inside it. When VM manipulation attack is launched, the affected VMs are further exposed to numerous other potential attacks like logic bombs.

2) Related Work: On the application layer, security threats are mostly in the context of information access and user authentication. Others include possibility of tracking and destroying data streams, tampering with the stability of the IoT platform, attacking the middleware layer and/or management platform [146], [147]. Given that IoT will further converge peoples everyday life activities and devices on the network, the need for faster access to data which is largely addressed by introducing MEC to the IoT system, must be balanced by a robust and highly reliable security technology in addition to creating more security awareness for users and application developers.

The architecture proposed in [144] has three key layers namely perception, transportation and application. The authors have identified different potential security vulnerabilities on each layer. For the perception layer, potential security vulnerabilities are mainly on the RFID, the wireless sensor networks, and the RFID sensor networks. For the transport layer, security vulnerabilities are mainly found at the access network, the core network, and the local network. Here, vulnerabilities can also be unique to the different access technologies, i.e., for 3G access network, Ad-Hoc network, and Wi-Fi. On the application layer, vulnerabilities exist for the application support layer as well as for specific IoT applications.

F. Privacy

1) Issues and Challenges: The early designs of IoT systems were largely closed, homogeneous and single-purpose with limited functionality, geographic scope and scale. In contrast, the present-day IoT systems are much larger and spanning across countries or continents, making them to comply with the varying rules and regulations. Similarly, in health care [148] type of applications, which invade personal spaces, privacy is becoming a significant concern [10], [12]. Governing organizations like European Commission have recognized that privacy in the processing of personal data and the confidentiality of communications as fundamental rights that

TABLE X
SUMMARY OF THE REVIEWED STATE-OF-THE-ART MOBILITY MANAGEMENT IN MEC ENABLED IOT

Ref.	Description	IoT application /domain /feature	Mobility Management	Flow Scheduling
[134]	Develop a user-centric energy-aware mobility management (EMM) scheme, to optimize the delay due to both radio access and computation, under the long-term energy consumption constraint of the user.	General IoT	✓	
[140]	Present UbiFlow, the first software-defined IoT system for ubiquitous flow control and mobility management base don distributed controller in multinetworks.	Software defined IoT	✓	✓
[141]	Explores how Named Data Networking, a proposed future Internet architecture, can address the challenges of interoperability in IoT networks.	IoT applications		✓
[142]	Analyzed distributed mobility management for future IoT sensor networks.	IoT sensors	✓	✓
[143]	Propose a location-aware load prediction at edge data centers which supports user mobility.	General IoT	✓	

should be protected [149]. In an IoT application, when the data sharing principle is leveraged by a cloud based system, that could raise a lot of privacy concerns. The potential use of data for unpredicted future applications may compromise privacy.

MEC enables caching, data processing and analytics to be done closer the source of the data and reduces the burden on centralized cloud servers and core networks [22]. Importantly, this will support differentiated privacy since raw, unprocessed data does not have to be stored or processed by a centralized cloud systems which can be located in distance. Only the processed and selected data are needed to reach the centralize cloud for further processing [10], [12]. For instance, the image processing of car number plate recognition can be done in the edge without transferring the location information to the centralized cloud servers. Such MEC based local processing protects the privacy of data without leaving the jurisdiction of the user. Moreover, the decentralized approach reduces the impact of data breaches such as Sony breach [150] and OPM (Office of Personnel Management) breach [151]. MEC approach also enable the possibility to implement specific or local privacy policies [152], contrary to the uniform privacy policies applied in centrally managed public cloud. In some IoT applications such eHealth services (for instance, mental and abortion clinics) local privacy polices with edge intelligence is required to meet the required privacy protection which cannot be met by only using a centralized approach [152].

The requirements in privacy protection are identified based on the generic and the regulatory objectives. First, it is required to harmonize the privacy of digital services at global level by promoting the digital single market. All relevant directives and legislative instruments should be encouraged to enable cross border policies. Then, it is necessary to balance the interests in protecting privacy and in fostering the global use of services.

Second, the privacy legislation should be done at a global level to ensure their compatibility with new technologies such as MEC. Different jurisdictions should cooperate together to develop inter-operable privacy requirements and facilitate the flow of information with the required level of privacy protection. For instance, the "Safe Harbor" agreement between U.S. and EU, requires U.S. companies to obey EU regulations so that EU companies can store and process data in U.S. data centers [153].

Third, it is necessary to foster interoperability and data portability to support the adaptation of new technologies. For instance, it can be done by avoiding mandated standards or preferences which could prevent interoperability. Moreover, it is necessary to promote the on-going interoperability efforts in the industries, this will be useful in defining uniform and global privacy policies. Finally, it is required to define one framework with a set of data protection laws which can be used across the border and they should be simple enough to be set up globally. This framework should be based on the concept of accountability and the laws should also support self-regulatory codes and mechanisms.

2) Related Work: Security and privacy challenges in MEC like edge computing paradigms are surveyed in [34] and [154]. A partially distributed approach that allows edge intelligence that can meet the privacy requirements of IoT use cases such as eHealth services is presented in [152]. The possibility of exploiting edge computing to solve the problem of loss of privacy by releasing personal and social data to centralized services such as e-commerce sites, rating services, search engines, social networks, and location services are presented in [22]. Possibilities of improving the data privacy of IoT data by using edge computing is presented in [45].

G. Trust Management

1) Requirements: Trust is a rather complex property to define, it is closely associated with the overall security of any network or platform. Trust is significant in critical 5G use cases like remote surgeries, emergency autonomous vehicles, factory automation, and tele-operated driving (e.g., drones). In these scenarios, latency and reliability are highly regarded. Although trust is an equally important property similar to security and privacy in IoT and MEC, it is hardly addressed lately in research works [34]. The need to implement the appropriate trust management scheme is very essential when it comes to IoT technologies. This is because IoT devices offload their delay critical applications to the edge cloud which is normally out of the direct control of the client.

According to Yan *et al.* [13], the key challenges of trust management in IoT are not only limited to system security robustness and privacy preservation. Trust relationships have to be sustained among all IoT system entities including the enabling technologies such as MEC. Data perception trust

determines the reliability of data sensing and collection in the IoT perception layer. Data fusion and mining trust explains the efficiency and trustworthiness of big data handling in the IoT network layer. Enabling secure data transmission and communication while maintaining the quality of IoT services and identity trust are other important aspects of IoT trust. It is equally important to apply a more generic trust management framework for IoT since it is a collaboration of multiple technologies and systems. The utilization of tamper resistive secure elements will enable the trust in the end user devices with physical protections to prevent the compromising of cryptographic security parameters. However, due to limited resources in many tiny IoT devices, the integration of such trust enabling devices will also be challenging. Above all, the most significant is the realization of human-computer trust interaction which requires more attention to the subjective properties of IoT users at the application layer.

In cloud computing, trust is targeted towards long-term underlying properties or infrastructure (persistent trust), and such trust can be specific to context-based social and technological mechanisms (dynamic trust). Moreover, when edge cloud computing is collaborating with IoT, it introduces more trust related objectives such as maintaining the trust for computation offloading IoT services or collected data to the edge cloud and the cooperative trust among edge servers. The edge servers should ensure the trustworthiness of end users and IoT devices, which acquire the resources from the edge cloud. Likewise, the edge servers should also assure their reliability and trustworthiness to the end users/devices and other edge servers for providing guaranteed services. More importantly, the efficient resource sharing among the edge servers has to be accomplished based on a proper trust management framework.

2) Related Work: The comprehensive literature surveys in [10] and [13] summarize the recent research works on IoT trust. Accordingly, the researchers have addressed IoT trust in multiple perspectives including trust evaluation, trust framework, data perception trust, identity trust and privacy preservation, transmission and communication trust, secure multi-party computation, user trust, and application trust. Existing IoT trust evaluation mechanisms are mathematically formed and have considered different trust metrics like social trust and QoS trust using both direct observations and indirect recommendations. Most of the trust frameworks proposed in IoT address security and privacy in IoT data transmission and communications. In [157], a preliminary design of a holistic solution with trust and security-by-design for cyber physical systems based on IoT and cloud architectures is presented. They have taken the initiative to develop and demonstrate a trustworthy-by-design autonomic security framework based on SDN/NFV and IoT networks.

In many previous literatures, data perception trust is addressed in the context of security and privacy, mainly by mitigating security attacks on data aggregation and processing, as well as exploiting some key management techniques [13]. Some recent literatures have also addressed data protection and performance improvement at the edge computing servers by trust management among fog servers [158]. Furthermore, trust is paramount to the effectiveness of node interaction in SIoT where the objects are building up a social network and becoming more autonomous [14]. Table XI summarizes the reviewed state-of-the-art security, privacy, and trust management in MEC enabled IoT.

IV. Integration Technologies

The realization of MEC for IoT is fueled by several integrating technologies such as SDN, NFV, ICN and Network Slicing. This section provides a high level overview of the role of each technology in MEC-IoT environment and the related works.

A. Network Function Virtualization

NFV is a network concept which proposes to use virtualization technologies to manage core networking functions using a software based approach [159]. NFV has been proven as one of the key enablers for not only the development of 5G but also MEC-IoT integration [160]. Specifically, MEC reuses the NFV virtualization infrastructure and the NFV infrastructure management to the largest extent possible [161].

Both MEC and NFV technologies can be used together in environments such as 5G mobile networks to elevate computing capacity to meet the increased networking demands. MEC architecture is also based on a virtualized platform quite similar to NFV architecture. Both technologies feature stackable components and each has a virtualization layer.

According to ESTI [2], it is beneficial to reuse the infrastructure and infrastructure management of NFV to the largest extent possible, by hosting both Virtual Network Functions (VNFs) and MEC applications on the same platform, computing experience is enhanced. The use of NFV will equally increase the scalability of MEC application. NFV can improve the scalability by dynamically scaling up/down the network resources depending on demand.

Several NFV-MEC ingratiation research works have been proposed recently. In [161], NFV-enabled MEC scheme is proposed to optimize the placement of resources among NFV-enabled nodes to support low latency mobile multimedia applications. A novel MEC and NFV integrated network architecture is presented in [162], this can be used to enhance the mobile game experience, optimized high speed HD video streaming and local content caching for AR. The double-tier MEC-NFV architecture in [163] aligns and integrates the MEC system with the NFV Management and Orchestration (MANO) by introducing a management subsystem that enriches the MANO with application-oriented orchestration capabilities. To support the deployment of container-based network services at the edge of the network, an architecture based on the Open Baton MANO framework is proposed by combining the NFV and MEC within a single orchestration environment [164].

B. Software Defined Networking

SDN is another 5G enabling technology which will help to design dynamic, manageable, cost-effective, and adaptable networks. SDN has fuel the advancement of network softwarization by proposing to transfer the control functionality to

TABLE XI
COMPARISON OF THE REVIEWED STATE-OF-THE-ART SECURITY, PRIVACY, AND TRUST MANAGEMENT IN MEC ENABLED IOT

Ref.	Description	IoT application /domain/feature	Security	Privacy	Trust
[144]	Proposed a security framework for virtualized Small Cell Networks, with the aim of further extending MEC in the broader 5G environment	Cloud-enabled IoT	✓	✓	
[157]	Addresses the utility based matching or pairing problem within the same domain of IoT nodes by using Irving's matching algorithm under the node specified preferences to endure a stable IoT node pairing	IoT node pairing services	✓	✓	✓
[146]	Analyzes the cross-layer heterogeneous integration issues and security issues in detail and discusses the security issues of IoT as a whole and tries to find solutions to them	General IoT	✓	✓	
[22]	Presents the research challenges associated with security, privacy and trust management in Edge-centric Computing	General IoT	✓	✓	✓
[158]	Holistically analyses the security and privacy threats, challenges, and mechanisms inherent in all edge paradigms including MEC.	General IoT	✓	✓	
[34]	Holistically analyses the security and privacy threats, challenges, and mechanisms inherent in all edge paradigms including MEC.	General IoT	✓	✓	
[156]	A survey on security and privacy challenge in fog computing	General IoT	✓	✓	
[154]	Present a edge computing based distributed approach to satisfy the security and privacy requirements of IoT	General IoT	✓	✓	
[45]	Discuss the methods of improving security and privacy of IoT data by using edge computing	General IoT	✓	✓	
[159]	Introduce the preliminary design of a holistic framework for enabling trust and security by-design for cyber physical systems (CPS) based on IoT and edge cloud architectures.	IoT architecture	✓	✓	✓
[160]	Propose a trust translation model for fog nodes and a privacy-aware model for access control at fog nodes.	IoT big data streams		✓	✓

software based entities, i.e., network controllers. SDN eliminates the use of vendor specific black-box hardware, thereby promoting the use of commodity servers and switches over proprietary appliances.

Notwithstanding, the transfer of network control functionalities to software based centralized entities, demands the data plane devices to communicate frequently with the SDN controllers. Thus, SDN controllers are located closer to the data plane to reduce the latency in packet processing. MEC offers the opportunity to locate control functions closer to data plane devices. Moreover, MEC complements the SDN advancement of the transformation of the mobile-broadband network into a programmable world, ensuring highly efficient network operation and service delivery [165]. Thus, the popularity of SDN in different domains including 5G, IoT will fuel the adaption of MEC concept as well.

Many recent research works justify the added benefits of the combine use of SDN and MEC in IoT systems [166]–[173]. The role of NFV and SDN in MEC ecosystem is discussed in [166]. SDN can be also used to make MEC more flexible and cost-effective for 5G applications. The real-time heart attack mobile detection service proposed in [167], is a novel e-health IoT service that employs SDN-powered MEC in a Vehicular Ad-hoc Network (VANET) architecture for reliable performance. In [168], a novel SDN/NFV-based security framework is presented to enable integrated protection for IoT systems and in MEC applications. An SDN-based MEC framework has been proposed to provide the required data-plane flexibility, programmability and reduced latency for applications such as VR and Vehicular IoT [169].

In addition, a conceptual approach to providing security for IoT systems by using SDN and edge computing is presented in [174]. The SDN-based IoT mobile edge cloud architecture (SIMECA) proposed in [170] can deploy diverse IoT services at the mobile edge by leveraging distributed, lightweight control and data planes optimized for IoT communications. In [171], the utilization of SDN and MEC to overcome the challenges of network densification of IoTcloud integration over a smart home is presented. Likewise, the MEC-SDN framework presented in [173] guarantees the QoS requirement satisfaction and efficient use of the wireless resources in tactical network applications.

C. Information Centric Networking

To address the ever increasing traffic volume in the Internet applications such as HD mobile video, AR/VR, 3D gaming and cloud computing, a new set of network architectures and networking technologies are developed over the past few decades. These technologies employ caching, replication and content distribution in optimum ways. Among them, ICN has become one of the main approaches to addressing this demand [175], [176]. ICN is an Internet architecture that puts information at the center where it needs to be and replaces the client-server model by proposing a new publish-subscribe model. The key benefits of ICN include fast and efficient data delivery and improved reliability. Thus, ICN is considered one of the promising networking models for IoT ecosystem.

MEC and ICN are complementary concepts which can be deployed independently [67]. However, both could add value to 5G and IoT domains in a complementary fashion. Certain synergies can be exploited when these two technologies are deployed cooperatively. For example, ICN can be used for content distribution over an unreliable radio links and transparent mobility among multiple technologies [177], while MEC can be used to reduce the latency for delay critical applications such as tactile Internet [178] and AR/VR applications, or to

perform distributed data-reduction and security functions for an IoT network.

In addition, the use of MEC with ICN can further improve the performance of edge computing. It can solve some of the existing challenges in MEC ecosystem. For instance, MEC is facing a challenge of application level reconfiguration, since it requires a re-initialization of the session whenever a session is being served by a non-optimal service instance. Such application level reconfiguration will increase the delay in session migration. However, the natural support for service-centric networking in ICN can minimize the network related configuration for applications. It will reduce the reconfiguration delay and allow fast resolution for named service instances [179].

ICN can also improve the edge storage and caching features of MEC enabled networks. ICN allows location independent data replication and opportunistic caching at strategic points in the network. These features benefit both real-time and non-realtime IoT applications where a set of IoT devices or users share the same content [179].

Opportunities and challenges of MEC and ICN integration for IoT are presented in [180]. Here, the authors highlight the synergies that can be exploited when the two technologies are deployed cooperatively for IoT applications. In addition, several research works have also verified the importance of ICN and MEC cooperation [67], [181]–[184]. A novel HetNets virtualization architecture with ICN and MEC techniques is proposed for video trans-coding, caching, and multi-cast in [181]. A virtual multi-resources allocation scheme is used in the designed framework to maximize the utility of computing, caching, and communication to support the massive content delivery. The vision of combining ICN and MEC in the context of connected vehicle environments is presented in [67]. It shows how ICN in combination with MEC can address the challenges of futuristic vehicular application scenarios. A novel information-centric heterogeneous networks framework is proposed in [182] to optimize the virtual resource allocation at the edge. Authors formulate the virtual resource allocation strategy as a joint optimization problem by considering both virtualization and caching and computing at the edge. A novel framework which jointly considers networking, caching, and computing techniques to support energy-efficient information retrieval and computing services is presented in [183]. This framework integrates SDN, MEC and ICN to enable the dynamic orchestration of different resources in next generation green wireless networks. A MEC-enabled ICN-based content handling framework at the mobile network edge is presented in [184]. The proposed framework realizes context-aware content localization in order to enhance user QoE in video distribution applications.

D. Network Slicing

Network slicing proposes a way of separating the network into different network segments. Thus, it allows multiple logical network segments to be created on top of a common shared physical infrastructure [185]. Future IoT will enable a wide range of different types of connections and services. These connections and services will need performance guarantees as well as security. Network slicing can satisfy these requirements. Moreover, 5G mobile network will support both MEC and network slicing technologies [186].

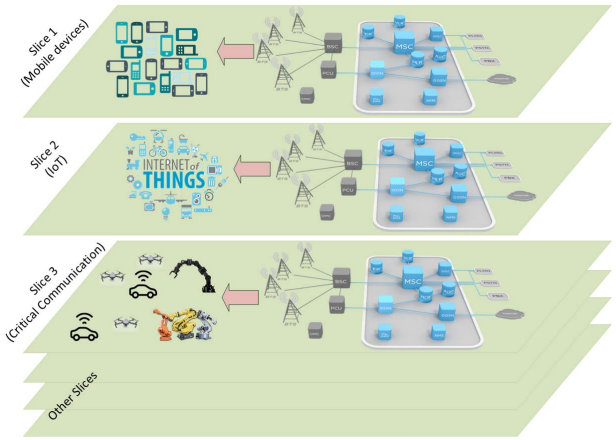

Fig. 5. Use of Network Slicing in different applications [188].

Network slicing can be used in different IoT domains. One of such application domain is massive IoT [187]. In order to support massive IoT systems, the network should be able to satisfy requirements such as massive cost reduction in communication, network scalability and edge analytics. The integration of MEC with Network slicing can be used to satisfy some of these requirements such as scalability and edge analytics. Another use case is critical communications for delay critical applications such healthcare, autonomous driving and industrial Internet. The key requirements to enable such critical communications are reduced latency and traffic prioritization. While MEC can be used to reduce latency, network slicing can support traffic prioritization.

Figure 5 illustrates the utilization of network slicing in different applications. Here, network slicing can be use to divide the MEC resources in to different slices dynamically. It will improve the efficiency of using MEC resources in different IoT applications.

Several research articles already presented the possibility of using Network slicing with MEC to provide improved services for IoT and other 5G applications.

An overview of the Third Generation Partnership Project (3GPP) standard evolution from network sharing principles, mechanisms, and architectures to future on-demand multi-tenant systems is presented in [185]. MEC is identified as one of the key attributes to realize the aforementioned network slicing extensions in 3GPP toward full multi-tenancy. A logical architecture for network-slicing-based 5G systems is presented in [189]. Here, authors show the evolution of network slicing in network architecture and the synergy with SDN, NFV and MEC technologies. The work presented in [190] discusses the design challenges of network slicing with other concepts such as cloud-RAN and MEC. A SDN/NFV packet/optical transport network and edge/core cloud platform for E2E 5G and IoT services is presented in ADRENALINTE testbed [191]. It demonstrates the use of SDN/NFV control system to provide the global orchestration

of the multi-layer (packet/optical) network resources and network slicing based distributed cloud infrastructure for multi-tenancy.

Table XII summarizes the reviewed state-of-the-art MEC-IoT integration technologies.

V. Projects

The European 5G PPP (5G Infrastructure Public Private Partnership) is one of the key layers on efforts to leverage MEC and IoT technologies to support the evolution towards 5G networks. In this section, we discuss some renowned ongoing EU research projects which are explicitly contributing to MEC and IoT technologies. These projects along with their technological aspects and the key research areas are summarized in Table XIII. Since the concept of MEC was initiated by ETSI, all of these projects are EU based. However, they have other non-EU partners as Japan, Taiwan, and China. The recent Horizon 2020 (H2020) funding scheme has fueled the MEC related research in Europe with the cooperation of other parts of the globe. Although, non-EU international level projects are hardly found on integrating MEC and IoT, the other countries have projects on different edge technologies including MCC, fog and cloudlets. We have excluded these projects from our survey since they are out of scope from the mainstream of the paper.

1) SESAME [Small Cells Coordination for Multi-Tenancy and Edge Services (June 2015 - Dec. 2017)]: SESAME [195] is one of the front-line EU H2020 projects which focuses on the development and demonstration of an innovative architecture, capable of providing Small Cell (SC) coverage to multiple virtual operators as-a-Service. This is a pioneering project that uses MEC and NFV technologies to realize the cloud-enabled small cell (CESC) concept by supporting powerful self-x (x stands for organizing, optimizing, or healing) management features and executing novel applications and services inside the access network infrastructure. SESAME is expected to deliver the small cell concept in high dense 5G scenarios. Moreover, it intends to consolidate multi-tenancy in communications infrastructures. This allows several operators or service providers to engage in new sharing models of both access capacity and edge computing capabilities.

2) ANASTACIA [Advanced Networked Agents for Security and Trust Assessment in CPS / IOT Architectures (Jan 2017 - Dec 2019)]: ANASTACIA [196], an EU H2020 funded project which promises to develop and demonstrate a holistic solution enabling trust and security by-design for heterogeneous, distributed and dynamically evolving CPS based on IoT and virtualised cloud architectures. The security framework, with self-protection, self-healing, and self-repair capabilities, will be designed in full compliance to SDN/NFV standards. This will include the security development paradigm, distributed trust and security enabler, and dynamic security and privacy seal. In particular ANASTACIA will address the security challenges in two use cases on the deployment of MEC server and smart buildings.

3) 5G-MiEdge [Millimeter-Wave Edge Cloud As an Enabler for 5G Ecosystem (July 2016 - June 2019)]: 5G-MiEdge [197] is a publicly supported research project bringing Millimeter-Wave (mmWave) technology and MEC into the mobile radio world. It was co-funded by EU H2020 and Japanese government. It combines mmW access/backhauling with MEC to enable enhanced mobile broadband (eMBB) services and mission critical low-latency applications using cost-efficient RANs. The project is composed of three key technologies; naming the protocols of mmWave access/backhaul links, ultra-lean and inter-operable control signaling mechanism (liquid RAN C-plane) over 3GPP LTE, and user or application centric orchestration algorithms for edge resource allocation. 5G-MiEdge intends to develop transmission schemes and protocols of mmWave access/backhauling which can assist the mobile edge cloud with caching/prefetching. This will be useful in realizing ultra-high speed and low latency service delivery which will be resilient to network bottlenecks such as backhaul congestion, users' density, and mission-critical service deployments. The targeted use cases are mostly stadiums, offices, and train stations.

4) 5G!Pagoda: 5G!Pagoda project [198] aims at creating a virtual mobile network that can be deployed upon request, dedicated to an application, to be used during the Tokyo Olympic Games in 2020. 5G!Pagoda intends to develop a scalable 5G slicing architecture and a highly programmable network control and data path supporting mechanism for use cases in IoT and human communication. This would be achievable through the development of a scalable network slice management and orchestration frameworks. These frameworks would serve distributed, edge dominated network infrastructures and convergent software functionality for lightweight control plane and data plane programmability.

5) Inter-IoT (Jan. 2016 - Dec. 2018): Horizon 2020 EU project INTER-IoT project [199] aims to design, implement and test an open framework that will allow interoperability among different IoT platforms. The project uses a layer-oriented approach for the interoperability framework in four application domains: smart grid, e-health, smart factories, and transport-logistics. The final goal is to integrate different IoT devices, networks, platforms, services and applications that will allow a global continuum of data, infrastructures and services which can enable different IoT use cases.

6) 5G-MoNArch [5G Mobile Network Architecture for Diverse Services, Use Cases, and Applications in 5G and Beyond (July 2017 - June 2019)]: 5G-MoNArch [200] is another project funded by EU Horizon 2020 programme and it will evolve 5G-PPP Phase 1 concepts to a fully-fledged architecture, develop prototype implementations and apply these prototypes to representative use cases. 5G-MoNArchs specific technical goal is to use network slicing, which capitalizes on the capabilities of SDN, NFV, orchestration of access network and core network functions, and analytics, to support a variety of use cases in vertical industries such as automotive, healthcare, and media. The devised 5G-MoNArch architecture will be deployed in two test beds: a sea port and a tourist city.

7) 5G-ESSENSE [Embedded Network Services for 5G Experiences (June 2017 - June 2019)]: 5G ESSENCE [201] is an EU H2020 funded project that proposes a highly flexible and scalable 5G small cell platform leveraging the

TABLE XII
COMPARISON OF THE REVIEWED STATE-OF-THE-ART MEC-IoT INTEGRATION TECHNOLOGIES

Ref.	Description	IoT application OR domain	NFV	SDN	ICN	Network Slicing
[164]	Present a NFV-enabled MEC architecture for video streaming, gaming and AR	Gaming and AR.	✓			
[163]	Present an double-tier MEC-NFV integrated architecture for 5G applications.	Gaming	✓			
[166]	Present an integrated orchestration solution by combining the NFV and MEC use cases within a single orchestration environment.	General IoT	✓			
[165]	Present a NFV-enabled MEC framework for low latency mobile applications.	General IoT	✓			
[194]	Preset an network architecture to addresses some of the central convergence challenges of NFV, 5G/MEC, IoT, and fog.	General IoT	✓			
[168]	Discuss the role of NFV and SDN in MEC and IoT ecosystem.	General IoT	✓	✓		
[169]	Present SDN-MEC based Real-time Heart Attack Mobile Detection Service (RHAMDS) by using smart watches.	ehealth, WIoT		✓		
[170]	Present SDN-NFV based security framework which can integration with existing IoT security mechanisms.	General IoT	✓	✓		
[171]	Present SDN-based MEC framework for low latency applications	VR and IoT Automotives.		✓		
[195]	Present an SDN/NFV architecture to delivery of future 5G services across multiple technological and administrative networks.	General IoT	✓	✓		
[176]	Present an conceptual approach to provide security for IoT systems by using SDN and edge computing.	General IoT		✓		
[172]	Presnet an SDN-based IoT Mobile Edge Cloud Architecture (SIMECA) for future IoT applications.	General IoT	✓	✓		
[174]	Present a four-tier architecture assisted by MEC and SDN for VANETs.	IoT Automotive		✓		
[173]	Discuss the utilization of SDN and MEC to overcome the challenges of network densification.	Smart homes		✓		
[175]	Present an MEC and SDN based framework for efficient and flexible service delivery.	Tactile Internet		✓		
[182]	A white paper on opportunities and challenges of MEC and ICN integration for IoT.	General IoT			✓	
[183]	Present an novel HetNets virtualization architecture for video transcoding, caching, and multi-cast.	VR,AR, Gaming, WIoT			✓	
[67]	Present the vision of combining ICN and MEC in the context of connected vehicle environments.	IoT Automotive			✓	
[184]	Present a novel information-centric heterogeneous networks framework for virtual resource allocation at the edge.	General IoT			✓	
[185]	Present a novel framework which jointly considers networking, caching, and computing techniques to support energy-efficient information retrieval and computing services.	General IoT		✓	✓	
[186]	Present a content handling framework which realizes context-aware content localization to enhance user QoE in video distribution applications.	VR,AR, Gaming, WIoT			✓	
[196]	Propose an 5G-ICN architecture to realize an ICN-based service delivery for future IoT applications.	General IoT	✓	✓	✓	
[189]	A discussion on use of network slicing for Massive IoT services.	General IoT				✓
[192]	Propose an novel network slicing architecture for integrated 5G communications including IoT	General IoT				✓
[193]	Propose an packet/optical transport network and edge/core cloud platform and testbed implementation for E2E 5G and IoT services.	General IoT	✓	✓		✓

paradigms of edge cloud computing and Small-Cell-as-a-Service. ESSENCE builds virtualization techniques on the distributed and network-integrated cloud inherited by 5G-PPP Phase 1 SESAME project that provides processing power at the edge of the network. The project will explicitly address two use cases including in-flight entertainment and connectivity systems and mission critical applications for public safety.

8) MATILDA (June 2017 - June 2019): The EU H2020 funded 5G-PPP Phase 2 project, MATILDA [202], aims to design and implement a holistic 5G framework for the design, development and orchestration of 5G-ready applications and 5G network services over a sliced, programmable infrastructure using VNFs. Intelligent and unified orchestration mechanisms will be applied for the automated placement of the 5G-ready applications and the creation and maintenance of the required network slices. The management of the cloud/edge computing and IoT resources is supported by a multi-site virtualized infrastructure manager.

9) 5GCITY (June 2017 - June 2019): 5GCity [203] is also an EU H2020 funded 5G-PPP Phase 2 project which demonstrates how to empower the city infrastructure and transform them into a hyper-connected, distributed 5G-enabled edge virtualization domain. The project targets three different cities (Barcelona, Bristol and Lucca), and would benefit telecommunication infrastructure providers, municipalities, and a number of different vertical sectors utilizing the city infrastructure. It will leverage the virtualization platform in order to enable the cities to create dynamic E2E slices containing both virtualized edge and network resources and lease to third-party operators.

10) MONICA [Management of Networked IoT Wearables Very Large Scale Demonstration of Cultural and Societal Applications (Jan 2017 - Dec 2019)]: MONICA [204] is an

EU H2020 funded large scale pilot project which aims to provide a very large scale demonstration of multiple existing and new IoT technologies for smarter living. It demonstrates a large scale IoT ecosystem that uses innovative wearable and portable IoT sensors and actuators with closed-loop back-end services integrated into an interoperable, cloud-based platform capable of offering a multitude of simultaneous, targeted applications. The key objectives of this project are to strengthen crowd safety and security at big, cultural, open-air events, and improve user experience. Given these goals, the final solution should be compatible with many different IoT sensors, open source, with cost effective wearables, and strengthened with data security, privacy, and trust.

11) AUTOPILOT [Automated Driving Progressed by Internet of Things (Jan 2017 - Dec 2019)]: Another large scale pilot project funded by EU H2020, AUTOPILOT [205] will deploy, test and demonstrate IoT-based automated driving use cases comprising urban driving, highway pilot, automated valet parking, and platooning. The project will integrate into vehicle IoT sensors and use cloud and MEC type IoT platforms (e.g., Brainport pilot site in Netherlands) to share sensor data and create new autonomous mobility services. The AUTOPILOT project will create and deploy new business products and services for fully automated driving vehicles used at the pilot sites. This project will feature innovations such as driving route optimization, vulnerable road user sensing and dynamically updating an IoT based HD map.

12) 5G-CORAL [A 5G Convergent Virtualised Radio Access Network Living at the Edge (Sep. 2017 - Aug. 2019)]: The newly initiated EU H2020 project, 5G-CORAL [206] leverages on the pervasiveness of edge and fog computing in RAN to create a unique opportunity for access convergence. This is envisioned by the means of virtualised networking and computing solution where virtualised functions, context-aware services, and user and third-party applications are blended together to offer enhanced connectivity and better quality of experience. The proposed solution considers two major building blocks, namely the edge and fog computing system and the orchestration and control system. 5G-CORAL project will be validated in three testbeds; a shopping mall, high-speed train, and connected cars.

VI. Lessons Learned and Future Research Directions

In this section, we present the lessons learned and the future research directions with respect to MEC-IoT integration. In particular, we focus on MEC-IoT application paradigms, technical aspects (i.e., scalability, communication, computation offloading and resource allocation, mobility management, security, privacy, and trust management), and standardization efforts.

A. Applications

1) Lessons Learned: MEC is an ideal solution that supports the increased demand for bandwidth consumption and ultra low latency requirements of IoT applications. MEC resources can be utilized for the pre-processing of massive IoT data which will reduce bandwidth consumption, provide network scalability, and ensure a fast response to user requests. However, in order to reap the maximum benefits of MEC for IoT, there needs to be more in dept research on how to efficiently distribute and manage data storage and computing resources at the network edge. Since MEC is still not well established, there can be myriad of technical challenges that need to be addressed. Moreover, due to much unprecedented user expectations, the requirements for designing MEC systems may vary upon the IoT application area.

2) Future Research Directions: The applications described in Section II are overlapping in several ways. For instance, AR and VR may explicitly support autonomous driving by exchanging information derived from multi-resolution maps created using the local sensors of the vehicles. This will extend the visibility of the vehicle. The edge servers are expected to perform pro-actively in such AR and VR systems. Tele-surgery is another domain that takes advantage of AR and VR exploitation. In the ideal situation, VR should have no distinction between real and virtual worlds. In order to achieve this goal, the concepts of MEC in VR applications might be merged with concepts like quantum computing. It is reported that ETSI and Virtual Reality/Augmented Reality Association (VRARA) intend to collaborate on interactive VR and AR technologies delivered over emerging 5G networks and hosted on MEC sites [207]. VRARA will encourage common member companies to pursue VR/AR-focused use cases and requirements for ETSI MEC Phase 2.

The adoption of machine learning techniques in 5G networks has increasingly attracted the attention of the research community. This will provide adaptive learning and decision-making approaches to meet the requirements of different verticals. The integration of Artificial Intelligence (AI) algorithms and machine learning at the edge of the networks will further assist the data-intensive requirements of the IoT applications. Particularly, AI techniques can be exploited for adaptive, optimal, and pro-active action on instantaneous networking demand in vehicular communications, in the context of self-driving vehicles. However, more efforts are needed to adopt machine learning techniques such as recursive neural networks, reservoir computing and deep learning in autonomous vehicles kind of applications due to their complex network architecture and enormous data sets. More importantly there is no unifying theories to define how such a network will behave.

B. Scalability

1) Lessons Learned: Several aspects of the present-day scalability schemes and data management paradigms will need substantial refinement in order to be able to handle the changes that are expected in future MEC-enabled IoT networks. IoT devices like sensors and RFID capturing devices are expected to keep capturing objects almost in real-time, hence generating a huge amount of readings. Timeliness is another factor in such scenarios since generated data usually have very short lifespan of about 2 seconds. Obviously, the present-day approach to information search and data management cannot handle

TABLE XIII
CONTRIBUTION OF GLOBAL LEVEL ONGOING PROJECTS ON MEC AND IOT. TODO: SHALL WE REMOVE MMWAVE HERE. WE DID NOT DISCUSS THAT A LOT

Project	SESAME [197]	ANASTACIA [198]	5G Mi-Edge [199]	5G!Pagoda [200]	Inter-IoT [201]	5G-MoNArch [202]	5G-ESSENSE [203]	MATILDA [204]	5GCITY [205]	MONICA [206]	AUTOPILOT [207]	5G-CORAL [208]
Technologies												
MEC	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓
IoT		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
SDN	✓	✓	✓	✓		✓	✓	✓	✓			
NFV	✓	✓		✓		✓	✓	✓	✓			✓
Network slicing	✓			✓		✓	✓	✓	✓			
mmWave			✓									
Research focus												
Network architecture OR framework	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	
Communication and network infrastructure	✓		✓				✓	✓				✓
Computation offloading	✓											✓
Resource management	✓					✓	✓	✓	✓			
Mobility									✓	✓	✓	
Scalability				✓					✓	✓		
Interoperability		✓			✓							
Security		✓				✓			✓	✓		
Privacy		✓							✓	✓		
Trust		✓								✓		

this expectation in a scalable manner. For this reason a more refined search and indexing algorithm will be required for both MEC-enabled IoT applications and IoT systems in general.

2) Future Research Directions: The adoption of the IPv6 is a significant move that will further advance scalability in MEC-enabled IoT applications going forward. Liu *et al.* [208] proposed the idea of CONCERT, a term coined from the combination of cloud and cellular system. The CONCERT solution exploits the principles of NFV and SDN to enhance scalability in future networks. Since scalability is a huge factor to determine where the MEC server gets deployed, and since the devices exploiting the MEC server located in the core network will inevitably experience longer latencies, then there could be a major hindrance to the use of real-time applications in such MEC settings. Regarding control signaling in MEC, the proposed CONCERT approach also adopts either a fully centralized control or a hierarchical control for better scalability and flexibility.

C. Communication

1) Lessons Learned: As MEC is still at its infancy, defining a solid communication model for the entire MEC architecture is an open research question that paves many opportunities to the academia, industry and the standardization entities. Advanced wireless communication techniques are required to design for interference cancellation and adaptive power control at the MEC servers in order to reduce the offloading energy consumption in a significant manner. The tight alliance between MEC and IoT may also create new research challenges in communication perspective.

2) Future Research Directions: As pointed out by Raza *et al.* [15], interoperability among various IoT LPWAN technologies encountered in IoT is still an open research question to address. There are still insufficient testbeds and open-source tool chains for LPWAN technologies. Massive connectivity and high data rate requirements of IoT devices (e.g., wearables) can be fulfilled by accompanying new radio access technologies such as Non-Orthogonal Multiple Access (NOMA) and massive Multiple-Input-Multiple-Output (MIMO) [76].

Moreover, many research efforts on edge caching are underway to achieve the trade-off between the transmission rate and storage at the MEC hosts [106]. The co-existence of different wireless communication technologies available for IoT may still create many challenges for edge level accessibility, since the IoT applications are diversified in versatile areas, where each has a unique set of requirements. Furthermore, they have conflicting goals such as energy efficiency, high throughput, and wide coverage. Therefore, system-level research is required to reap out the maximum benefit on exploiting such communication technologies.

Implementing MEC over FiWi access networks are investigated due to their low costs, wide deployments, and high capacity [109]. These fiber-wireless broadband access networks may provide a single communication platform for MEC and centralized cloud services over the wired and wireless networking technologies. ICN in combination with MEC is identified as another promising way of establishing a communication model for vehicular networks [67] where moving vehicles may incur frequent disconnects and re-connects to different network access points.

D. Computation Offloading and Resource Allocation

1) Lessons Learned: Decision making for data offloading at the user-end devices and the resource allocation for those offloaded data/application at the edge clouds are two

highly regarded topics discussed among the research community, especially those who engaged in MEC and IoT eras. Most of the prior works were focused on the offloading mechanisms for latency critical applications while minimizing energy consumption at the UE. In contrary, IoT permits a platform that has both delay sensitive and delay tolerant applications. Although, most of the proposed solutions are evaluated by means of theoretical analysis or simulations, there is still no proper formation of standard offloading mechanism for IoT and MEC systems.

2) Future Research Directions: Mobility is a principal feature of IoT devices which are either being transported by humans (e.g., wearable sensor) or by another carrier (e.g., vehicular networks), or being mobile by itself (e.g., robots). Mobility-aware resource management and computation offloading strategies need to be precisely investigated in the era of IoT supportive MEC systems. Scalability is the other equally important feature to consider in large scale IoT deployments where edge computing needs seamless offloading and resource allocation policies. Other accelerating tendencies towards future research efforts in the field of MEC and IoT may include server cooperation in MEC, dependency-aware offloading, and dynamic resource allocation.

The exploitation of Knowledge-Defined Networking (KDN) to make intelligent predictions about offload costs can be leveraged for efficient resource allocation at MEC servers as well as the offloading decision making at IoT devices [209]. The new paradigm of KDN is composed of Network Analytics (NA), SDN, and AI techniques. The introductory work in [210] proposes an intelligent computation offloading framework based on user dynamics and historical data.

E. Mobility Management

1) Lessons Learned: Mobility management in MEC-enabled IoT has attracted a lot of attention in both research and the industry. This comes natural, given that mobile nodes are expected to dominate the future IoT networks. An optimal offloading decision will be necessary for effective integration of MEC with IoT. Thus far, most of the works on mobility management in the context of MEC are solely focusing on optimizing the energy consumption at IoT nodes. However, designing efficient and optimal MEC-enabled IoT systems will require energy optimization at the MEC end also. This includes energy consumed on computation and energy consumed on communication.

Furthermore, most works on offloading decisions are based on static scenarios where the IoT device moves from one MEC eNB to another and remains in one steady location during the offload, which is not necessarily the situation in most cases.

2) Future Research Directions: The energy required for offloading or handover could vary substantially based on the movement factor during the offload [138]. For this reason, there will be a need for more advanced decision making algorithms. They will leverage on various prediction techniques to determine when offloading is in fact necessary, what the channel quality will be like during the offloading and what the entire offloading process will cost for each offloading condition.

For advancing the VM migration techniques, a crucial step moving forward is to optimize the migration process by minimizing the time required to complete a full migration. This will mostly dependent on the protocol design of the migration process. Hence an optimal solution is required for a collaborative effort on the side of individuals and organizations. That notwithstanding, still the VM migration scheme might not be suitable for highly delay-sensitive real-time applications. In general, to achieve an efficient and highly optimized mobility management scheme for MEC-enabled IoT applications, there will be a need for a more holistic approach. Such a solution will encompass power control, VM migration, data compression, and path selection [29].

F. Security

1) Lessons Learned: Notwithstanding the closed paradigm of MEC, it is important to realize that the whole ecosystem of MEC will not be controlled by one single owner or service provider. MEC data centers are capable of providing services without relying on centralized infrastructures. Thus, it is certain that all MEC relevant assets, such as the network infrastructure, the service infrastructure (e.g., edge data centers, core infrastructure), the virtualization infrastructure, and the user devices will not be controlled by a single entity. The scale of this effect is further confounded by the diversity that exists in IoT applications. Consequently, every element of MEC and IoT infrastructure should be targeted towards global networking environment. As discussed in [34], the "anything, anytime" principle should be the underlying building blocks and application scenarios for MEC-enabled IoT systems [152]. Conversely, the "anywhere" principle also implies that attacks can be performed from anywhere, making the edge paradigms a double-edged sword and hence the need for security measures that span the entire global networking paraphernalia.

2) Future Research Directions: The future of MEC-enabled IoT systems will revolve mostly around developing universal standard security mechanisms that can adequately protect the whole ecosystem against security threats. Such universal standards will enable both service providers and developers to understand the particularities of every edge paradigm, as they have subtle differences that will affect the implementation and deployment of the security mechanisms [34]. Currently, the absence of such global perimeters is seen as one of the banes to the security of the edge paradigms.

One notable effect of the lack of a global perimeter is the nature of the different attacker profiles that will target edge paradigms [211]. In the present day networks, adversaries are mostly external entities with no stake in control of network elements. However, with the advent of MEC-enabled IoT, there exist many adversaries that will control one or more elements of the infrastructure such as user devices, VMs, servers, sections of the network, and in the worst case, an entire edge data center [152]. Adopting deep-learning-based models at the edge level to detect malicious applications will be another

interesting research area. Applying reinforcement learning techniques to develop edge security solutions can be exploited for anomaly detection and lightweight authentication.

G. Privacy

1) Lessons Learned: The rise of new architecture, new technologies and new network services will open up new challenges to privacy protection. On the one hand, the existing privacy objectives are outdated and are not compatible with current technologies such as MEC, IoT and 5G. Therefore, these privacy directives have to be updated. Governing organizations have already started redefining the privacy objectives. For instance, the European commission adopted a General Data Protection Regulation (GDPR), in April 2016. It will be superseded by the data protection directive and is planned to be enforceable starting on 25 May 2018. On the other hand, privacy awareness is significantly increasing among the general public users [212]. Therefore, the future networks require to provide an extra level of privacy than the earlier generation of networks.

2) Future Research Directions: The future research work should be focused on addressing above privacy challenges. New privacy protection mechanisms such as Software Defined Privacy (SDP) [153], Privacy by Design (PbD) [213] and SDN based privacy-aware routing [214] can be used to provide the required level of privacy while or after the integration of MEC to IoT systems. SDP [153] allows easy orchestrations of existing tools for enforcing privacy requirements of an Infrastructure as a Service (IaaS) cloud customer. This concept can further be extended to provide privacy protection for MEC enabled IoT systems. PbD is an approach in system engineering, which promotes the integration of privacy throughout the whole design process [213]. PbD approach can be used during the MEC integration in IoT systems. If SDN is used in MEC-IoT systems, which is highly likely, user data packets containing privacy information that should not cross local spaces or even country borders could be identified. Then, the SDN controller could define flow rules so that these packets are routed only via the links and routers with high security. More sophisticated routing protocols can be designed by increasing the number of such qualifiers.

H. Trust Management

1) Lessons Learned: Trust management in MEC systems is still a barely investigated area. In order to strengthen the user ecosystem in centralized cloud environment, a flexible trust manager can be shared among the cloud infrastructure providers [215]. Likewise, the mutual trust should be incorporated among the MEC servers to enhance the secure sharing of IoT datasets.

2) Future Research Directions: Context-aware trust relationships based on social computing are yet to be investigated in the paradigm of IoT and edge computing. A comprehensive trust framework is still lacking for holistic trust management in IoT with the context of MEC which is capable of achieving all the objectives listed above and fulfills the requirements from different trust levels. Future research needs to focus on data collecting at IoT perception layer and processing at edge servers in order to improve the IoT and MEC service quality. Complex and resource consuming trust management algorithms are not affordable by the tiny IoT devices. Furthermore, device and network heterogeneity in IoT raises further challenges. There are also some open research trends for making light-weight trust management mechanisms suitable for heterogeneous IoT.

I. Standardization

The standardization of the MEC technology is relatively recent and currently ongoing. The goal is to bring together all experts and industry players in consensus to define the characteristics and rules that will govern the implementation and interconnection of the MEC technology globally. Just like other standardized technologies, the standardization of MEC will open up an infinite avenue for developers and innovators to harness the benefits of MEC in designing cutting-edge technologies and innovative solutions that will drive 5G and future networks. On the side of the customers, such standardization would by no small measure affirm their trust in MEC and other related products and services.

1) Future Research Directions: The standardization processes of MEC along with the coordination and management tasks are lead by an ETSI ISG [71]. The MEC ISG group aims at creating an open standardized and efficient platform for the seamless integration of enterprise applications from different vendors and service providers into the MEC platform. Most recently, the 3GPP has shown a growing interest in incorporating MEC into its 5G standard and has identified functionality supports for edge computing in a recent technical specification contribution.

The standardization entities are required to ensure that MEC architecture works harmoniously with the heterogeneous IoT echo systems and related technologies. Moreover, since there are numerous third-party partners such as application developers, content providers and network device vendors, the complexity of the services and the management of very large scale environment becomes challenging [216].

It is also important to do security and privacy legislation and standardization in a global context. Different jurisdictions should cooperate together to develop inter-operable security and privacy requirements to facilitate the flow of information with the required level of protection. Thus, the security and privacy regulations will play a vital role to promote the adaptations new technologies such as MEC. Regulatory entities such as governments and standardization organizations have to work together with industry to define and/or update the regulations according to the new technologies.

VII. Conclusion

The advancements of MEC and IoT technologies will be contributing immensely to the realization of the highly anticipated game-changing vision of 5G and future generations of mobile networks. The propounders of MEC; which is relatively a recent technology, have identified IoT as one of the important use cases of MEC. MEC server performs as a

gateway between the latency critical and massive IoT networks and the core network where it can provide edge-cloud computing and networking functionalities. IoT application domains are empowered with MEC technology by extending some intelligence to the edge of the network. Although MEC will provide on-site cloud computing services for IoT networks, there are still challenges in terms of device and network heterogeneity, scalability, mobility, and security. In addition to the possible future works discussed in Section VI, there are few other research topics including but not limited to MEC service level congestion control, latency aware routing, and dynamic application routing. In all essence, MEC and IoT are two complementary technologies that if well harnessed have the potential of advancing the course of the 5G networks and beyond.

REFERENCES

[1] P. Guillemin and P. Friess, "The industrial Internet of Things volume G1: Reference architecture," IoT Strategic Res. Agenda, Eur. Res. Cluster, Rep., Sep. 2009. [Online]. Available: http://www.internet-of-things-research.eu/pdf/IoT_Cluster_Strategic_Research_Agenda_2009.pdf

[2] Y.-C. Hu, M. Patel, D. Sabella, N. Sprecher, and V. Young, "Mobile edge computing a key technology towards 5G," Sophia Antipolis, France, ETSI, White Paper, pp. 1–16, 2015.

[3] P. Schulz *et al.*, "Latency critical IoT applications in 5G: Perspective on the design of radio interface and network architecture," *IEEE Commun. Mag.*, vol. 55, no. 2, pp. 70–78, Feb. 2017.

[4] T. Taleb *et al.*, "On multi-access edge computing: A survey of the emerging 5G network edge cloud architecture and orchestration," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 3, pp. 1657–1681, 3rd Quart., 2017.

[5] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Comput. Netw.*, vol. 54, no. 15, pp. 2787–2805, 2010.

[6] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Gener. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, 2013.

[7] 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.

[8] V. Gazis, "A survey of standards for machine-to-machine and the Internet of Things," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 482–511, 1st Quart., 2017.

[9] M. Weyrich and C. Ebert, "Reference architectures for the Internet of Things," *IEEE Softw.*, vol. 33, no. 1, pp. 112–116, Jan./Feb. 2016.

[10] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," *Comput. Netw.*, vol. 76, pp. 146–164, Jan. 2015.

[11] J. Granjal, E. Monteiro, and J. S. Silva, "Security for the Internet of Things: A survey of existing protocols and open research issues," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 3, pp. 1294–1312, 3rd Quart., 2015.

[12] P. Porambage *et al.*, "The quest for privacy in the Internet of Things," *IEEE Cloud Comput.*, vol. 3, no. 2, pp. 36–45, Mar./Apr. 2016.

[13] Z. Yan, P. Zhang, and A. V. Vasilakos, "A survey on trust management for Internet of Things," *J. Netw. Comput. Appl.*, vol. 42, pp. 120–134, Jun. 2014.

[14] L. Atzori, A. Iera, G. Morabito, and M. Nitti, "The social Internet of Things (SIoT)—When social networks meet the Internet of Things: Concept, architecture and network characterization," *Comput. Netw.*, vol. 56, no. 16, pp. 3594–3608, 2012.

[15] U. Raza, P. Kulkarni, and M. Sooriyabandara, "Low power wide area networks: An overview," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 2, pp. 855–873, 2nd Quart., 2017.

[16] C. Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos, "Context aware computing for the Internet of Things: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 1, pp. 414–454, 1st Quart., 2014.

[17] J. A. Stankovic, "Research directions for the Internet of Things," *IEEE Internet Things J.*, vol. 1, no. 1, pp. 3–9, Feb. 2014.

[18] J. Lin *et al.*, "A survey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1125–1142, Oct. 2017.

[19] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of Things: Vision, applications and research challenges," *Ad Hoc Netw.*, vol. 10, no. 7, pp. 1497–1516, 2012.

[20] L. Atzori, A. Iera, and G. Morabito, "Understanding the Internet of Things: Definition, potentials, and societal role of a fast evolving paradigm," *Ad Hoc Netw.*, vol. 56, pp. 122–140, Mar. 2017.

[21] D. Sabella, A. Vaillant, P. Kuure, U. Rauschenbach, and F. Giust, "Mobile-edge computing architecture: The role of MEC in the Internet of Things," *IEEE Consum. Electron. Mag.*, vol. 5, no. 4, pp. 84–91, Oct. 2016.

[22] P. G. Lopez *et al.*, "Edge-centric computing: Vision and challenges," *SIGCOMM Comput. Commun. Rev.*, vol. 45, no. 5, pp. 37–42, 2015.

[23] S. Shahzadi, M. Iqbal, T. Dagiuklas, and Z. U. Qayyum, "Multi-access edge computing: Open issues, challenges and future perspectives," *J. Cloud Comput.*, vol. 6, no. 1, p. 30, 2017.

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

[25] Y. Ai, M. Peng, and K. Zhang, "Edge cloud computing technologies for Internet of Things: A primer," *Digit. Commun. Netw.*, vol. 4, no. 2, pp. 77–86, 2018.

[26] N. Abbas, Y. Zhang, A. Taherkordi, and T. Skeie, "Mobile edge computing: A survey," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 450–465, Feb. 2018.

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

[28] M. T. Beck, M. Werner, S. Feld, and T. Schimper, "Mobile edge computing: A taxonomy," in *Proc. 6th Int. Conf. Adv. Future Internet*, 2014, pp. 48–55.

[29] P. Mach and Z. Becvar, "Mobile edge computing: A survey on architecture and computation offloading," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 3, pp. 1628–1656, 3rd Quart., 2017.

[30] A. C. Baktir, A. Ozgovde, and C. Ersoy, "How can edge computing benefit from software-defined networking: A survey, use cases, and future directions," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 4, pp. 2359–2391, 4th Quart., 2017.

[31] I. Afolabi, T. Taleb, K. Samdanis, A. Ksentini, and H. Flinck, "Network slicing & softwarization: A survey on principles, enabling technologies & solutions," *IEEE Commun. Surveys Tuts.*, to be published, doi: 10.1109/COMST.2018.2815638.

[32] Y. Mao, C. You, J. Zhang, K. Huang, and K. B. Letaief, "A survey on mobile edge computing: The communication perspective," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 4, pp. 2322–2358, 4th Quart., 2017.

[33] S. Wang *et al.*, "A survey on mobile edge networks: Convergence of computing, caching and communications," *IEEE Access*, vol. 5, pp. 6757–6779, 2017.

[34] 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.*, vol. 78, pp. 680–698, Jan. 2018.

[35] M. Perez *et al.*, "Impact of delay on telesurgical performance: Study on the robotic simulator dV-trainer," *Int. J. Comput. Assist. Radiol. Surgery*, vol. 11, no. 4, pp. 581–587, 2016.

[36] "Unlocking commercial opportunities from 4G evolution to 5G," GSMA Netw., London, U.K., Rep., Feb. 2016. Accessed: Mar. 21, 2018. [Online]. Available: https://www.gsma.com/futurenetworks/wpcontent/uploads/2016/02/704_GSMA_unlocking_comm_opp_report_v5.pdf

[37] "The business case for MEC in retail: A TCO analysis and its implications in the 5G era," Santa Clara, CA, USA, Intel Tech., White Paper, Jun. 2017. Accessed: Mar. 14, 2018. [Online]. Available: https://builders.intel.com/docs/networkbuilders/the-business-case-for-mec-in-retail-a-tco-analysis-and-its-implications-in-the-5g-era.pdf

[38] *Putting Sensors to Work in the Factory Environment: Data to Information to Wisdom*. Accessed: Apr. 29, 2018. [Online]. Available: https://itpeernetwork.intel.com/putting-sensors-to-work-in-the-factory-environment/

[39] B. L. R. Stojkoska and K. V. Trivodaliev, "A review of Internet of Things for smart home: Challenges and solutions," *J. Clean. Product.*, vol. 140, pp. 1454–1464, Jan. 2017.

[40] C. Vallati, A. Virdis, E. Mingozzi, and G. Stea, "Mobile-edge computing come home connecting things in future smart homes using LTE device-to-device communications," *IEEE Consum. Electron. Mag.*, vol. 5, no. 4, pp. 77–83, Oct. 2016.

[41] R. Morabito, R. Petrolo, V. Loscrí, and N. Mitton, "Enabling a lightweight edge gateway-as-a-service for the Internet of Things," in *Proc. IEEE 7th Int. Conf. Netw. Future (NOF)*, Armação dos Búzios, 2016, pp. 1–5.

[42] X. Sun and N. Ansari, "EdgeIoT: Mobile edge computing for the Internet of Things," *IEEE Commun. Mag.*, vol. 54, no. 12, pp. 22–29, Dec. 2016.

[43] K.-K. Nguyen and M. Cheriet, "Virtual edge-based smart community network management," *IEEE Internet Comput.*, vol. 20, no. 6, pp. 32–41, Nov./Dec. 2016.

[44] T. Taleb, S. Dutta, A. Ksentini, M. Iqbal, and H. Flinck, "Mobile edge computing potential in making cities smarter," *IEEE Commun. Mag.*, vol. 55, no. 3, pp. 38–43, Mar. 2017.

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

[46] M. S. Hossain and G. Muhammad, "Cloud-assisted industrial Internet of Things (IIoT)—Enabled framework for health monitoring," *Comput. Netw.*, vol. 101, pp. 192–202, Jun. 2016.

[47] S. M. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, and K.-S. Kwak, "The Internet of Things for health care: A comprehensive survey," *IEEE Access*, vol. 3, pp. 678–708, 2015.

[48] W. Shi and S. Dustdar, "The promise of edge computing," *Computer*, vol. 49, no. 5, pp. 78–81, May 2016.

[49] T. X. Tran, A. Hajisami, P. Pandey, and D. Pompili, "Collaborative mobile edge computing in 5G networks: New paradigms, scenarios, and challenges," *IEEE Commun. Mag.*, vol. 55, no. 4, pp. 54–61, Apr. 2017.

[50] D. Singh, G. Tripathi, A. M. Alberti, and A. Jara, "Semantic edge computing and IoT architecture for military health services in battlefield," in *Proc. IEEE 14th Annu. Consum. Commun. Netw. Conf. (CCNC)*, Las Vegas, NV, USA, 2017, pp. 185–190.

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

[52] S. K. Sharma and X. Wang, "Live data analytics with collaborative edge and cloud processing in wireless IoT networks," *IEEE Access*, vol. 5, pp. 4621–4635, 2017.

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

[54] "5G security—Making the right choice to match your needs," London, U.K., SIMalliance 5GWG Tech., White Paper, Feb. 2016. Accessed: Feb. 12, 2018. [Online]. Available: http://simalliance.org/

[55] O. Zakaria, J. Britt, and H. Forood, "Internet of Things (IoT) automotive device, system, and method," U.S. Patent 9 717 012, Jul. 25, 2017.

[56] W. Balid, H. Tafish, and H. H. Refai, "Intelligent vehicle counting and classification sensor for real-time traffic surveillance," *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 6, pp. 1784–1794, Jun. 2018.

[57] S. Amini, I. Gerostathopoulos, and C. Prehofer, "Big data analytics architecture for real-time traffic control," in *Proc. IEEE 5th Int. Conf. Models Technol. Intell. Transp. Syst. (MT-ITS)*, Naples, Italy, 2017, pp. 710–715.

[58] J. Yu *et al.*, "SenSpeed: Sensing driving conditions to estimate vehicle speed in urban environments," *IEEE Trans. Mobile Comput.*, vol. 15, no. 1, pp. 202–216, Jan. 2016.

[59] S. Nawaz, C. Efstratiou, and C. Mascolo, "Smart sensing systems for the daily drive," *IEEE Pervasive Comput.*, vol. 15, no. 1, pp. 39–43, Jan./Mar. 2016.

[60] G. Han *et al.*, "Software-defined vehicular networks: Architecture, algorithms, and applications: Part 1," *IEEE Commun. Mag.*, vol. 55, no. 7, pp. 78–79, Jul. 2017.

[61] D. He, S. Zeadally, B. Xu, and X. Huang, "An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 12, pp. 2681–2691, Dec. 2015.

[62] (2016). *Deliverable D1.1 Refined Scenarios and Requirements, Consolidated Use Cases, and Qualitative Techno-Economic Feasibility Assessment*. Accessed: Apr. 18, 2018. [Online]. Available: https://metis-ii.5g-ppp.eu/wp-content/uploads/deliverables/METIS-II_D1.1_v1.0.pdf

[63] A. Osseiran, J. F. Monserrat, and P. Marsch, *5G Mobile and Wireless Communications Technology*. Cambridge, U.K.: Cambridge Univ. Press, 2016.

[64] S. K. Datta, J. Haerri, C. Bonnet, and R. F. Da Costa, "Vehicles as connected resources: Opportunities and challenges for the future," *IEEE Veh. Technol. Mag.*, vol. 12, no. 2, pp. 26–35, Jun. 2017.

[65] V. Frascolla *et al.*, "5G-MiEdge: Design, standardization and deployment of 5G phase II technologies: MEC and mmWaves joint development for Tokyo 2020 Olympic games," in *Proc. IEEE Conf. Stand. Commun. Netw.*, Helsinki, Finland, 2017, pp. 54–59.

[66] L. Li, Y. Li, and R. Hou, "A novel mobile edge computing-based architecture for future cellular vehicular networks," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, San Francisco, CA, USA, 2017, pp. 1–6.

[67] D. Grewe, M. Wagner, M. Arumaithurai, I. Psaras, and D. Kutscher, "Information-centric mobile edge computing for connected vehicle environments: Challenges and research directions," in *Proc. Workshop Mobile Edge Commun.*, 2017, pp. 7–12.

[68] N. H. Motlagh, M. Bagaa, and T. Taleb, "UAV-based IoT platform: A crowd surveillance use case," *IEEE Commun. Mag.*, vol. 55, no. 2, pp. 128–134, Feb. 2017.

[69] M. Satyanarayanan, "The emergence of edge computing," *Computer*, vol. 50, no. 1, pp. 30–39, Jan. 2017.

[70] L. Baresi, D. F. Mendonça, and M. Garriga, "Empowering low-latency applications through a serverless edge computing architecture," in *Proc. Eur. Conf. Service Orient. Cloud Comput.*, 2017, pp. 196–210.

[71] *ETSI Executive Briefing—Mobile Edge Computing (MEC) Initiative*. Accessed: Feb. 1, 2018. [Online]. Available: https://portal.etsi.org/portals/0/tbpages/mec/docs/mec%20executive%20brief%20v1%2028-09-14.pdf

[72] M. Chen, W. Saad, and C. Yin, "Virtual reality over wireless networks: Quality-of-service model and learning-based resource management," *IEEE Trans. Commun.*, to be published, doi: 10.1109/TCOMM.2018.2850303.

[73] E. Bastug, M. Bennis, M. Médard, and M. Debbah, "Toward interconnected virtual reality: Opportunities, challenges, and enablers," *IEEE Commun. Mag.*, vol. 55, no. 6, pp. 110–117, Jun. 2017.

[74] B. Cheng *et al.*, "FogFlow: Easy programming of IoT services over cloud and edges for smart cities," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 696–707, Apr. 2018.

[75] "Cisco visual networking index: Forecast and methodology, 2016–2021," San Jose, CA, USA, Cisco, White Paper, Jun. 2017. [Online]. Available: https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/complete-white-paper-c11-481360.pdf

[76] H. Sun, Z. Zhang, R. Q. Hu, and Y. Qian, "Challenges and enabling technologies in 5G wearable communications," *arXiv preprint arXiv:1708.05410*, 2017.

[77] C. Perera, C. H. Liu, and S. Jayawardena, "The emerging Internet of Things marketplace from an industrial perspective: A survey," *IEEE Trans. Emerg. Topics Comput.*, vol. 3, no. 4, pp. 585–598, Dec. 2015.

[78] F. J. Ferrández-Pastor, J. M. García-Chamizo, M. Nieto-Hidalgo, J. Mora-Pascual, and J. Mora-Martínez, "Developing ubiquitous sensor network platform using Internet of Things: Application in precision agriculture," *Sensors*, vol. 16, no. 7, p. 1141, 2016.

[79] "Smart farming: The sustainable way to food," Beecham Res., London, U.K., Rep., May 2017. Accessed: Apr. 4, 2018. [Online]. Available: http://www.beechamresearch.com/

[80] "Building an IoT solution with PeakUp to improve management of poultry houses," Microsoft Tech. Case Studies, Redmond, WA, USA, Mar. 2017. [Online]. Available: https://microsoft.github.io/techcasestudies/iot/2017/03/30/PeakUp.html

[81] R. B. Mahale and S. S. Sonavane, "Smart poultry farm monitoring using IoT and wireless sensor networks," *Int. J. Adv. Res. Comput. Sci.*, vol. 7, no. 3, pp. 187–190, 2016.

[82] M. Boban, K. Manolakis, M. Ibrahim, S. Bazzi, and W. Xu, "Design aspects for 5G V2X physical layer," in *Proc. IEEE Conf. Stand. Commun. Netw. (CSCN)*, Berlin, Germany, 2016, pp. 1–7.

[83] P. J. Braun, S. Pandi, R.-S. Schmoll, and F. H. P. Fitzek, "On the study and deployment of mobile edge cloud for tactile Internet using a 5G gaming application," in *Proc. IEEE 14th Consum. Commun. Netw. Conf. (CCNC)*, Las Vegas, NV, USA, 2017, pp. 154–159.

[84] S. Pandi, R. S. Schmoll, P. J. Braun, and F. H. P. Fitzek, "Demonstration of mobile edge cloud for tactile Internet using a 5G gaming application," in *Proc. IEEE 14th Annu. Consum. Commun. Netw. Conf. (CCNC)*, Las Vegas, NV, USA, 2017, pp. 607–608.

[85] M. Satyanarayanan, "Keynotes: Edge computing: Vision and challenges," in *Proc. 2nd Int. Conf. Collaboration Internet Comput. (CIC)*, 2016, doi: 10.1109/CIC.2016.013.

[86] H. Kanzaki, K. Schubert, and N. Bambos, "Video streaming schemes for industrial IoT," in *Proc. 26th Int. Conf. Comput. Commun. Netw. (ICCCN)*, Vancouver, BC, Canada, 2017, pp. 1–7.

[87] K. E. Harper, T. de Gooijer, J. O. Schmitt, and D. Cox, "Microdatabases for the industrial Internet," *arXiv preprint arXiv:1601.04036*, 2016.

[88] G. Peralta *et al.*, "Fog computing based efficient IoT scheme for the industry 4.0," in *Proc. Int. Workshop Electron. Control Meas. Signals Their Appl. Mechatronics (ECMSM)*, 2017, pp. 1–6.

[89] J. Chakareski, "VR/AR immersive communication: Caching, edge computing, and transmission trade-offs," in *Proc. Workshop Virtual Reality Augmented Reality Netw.*, Los Angeles, CA, USA, 2017, pp. 36–41.

[90] A. Carvallo and J. Cooper, *The Advanced Smart Grid: Edge Power Driving Sustainability*. Boston, MA, USA: Artech House, 2015.

[91] M. H. Y. Moghaddam, A. Leon-Garcia, and M. Moghaddassian, "On the performance of distributed and cloud-based demand response in smart grid," *IEEE Trans. Smart Grid*, to be published, doi: 10.1109/TSG.2017.2688486.

[92] H. Lasi, P. Fettke, H.-G. Kemper, T. Feld, and M. Hoffmann, "Industry 4.0," *Bus. Inf. Syst. Eng.*, vol. 6, no. 4, pp. 239–242, 2014.

[93] L. Da Xu, W. He, and S. Li, "Internet of Things in industries: A survey," *IEEE Trans. Ind. Informat.*, vol. 10, no. 4, pp. 2233–2243, Nov. 2014.

[94] C. Perera, C. H. Liu, S. Jayawardena, and M. Chen, "A survey on Internet of Things from industrial market perspective," *IEEE Access*, vol. 2, pp. 1660–1679, 2014.

[95] B. Kehoe, S. Patil, P. Abbeel, and K. Goldberg, "A survey of research on cloud robotics and automation," *IEEE Trans. Autom. Sci. Eng.*, vol. 12, no. 2, pp. 398–409, Apr. 2015.

[96] J.-Q. Li *et al.*, "Industrial Internet: A survey on the enabling technologies, applications, and challenges," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 3, pp. 1504–1526, 3rd Quart., 2017.

[97] M. Albano, J. B. Silva, and L. L. Ferreira, "The industrial Internet of Things," in *Proc. 22º Seminário da Rede Temática de Comunicações Móveis*, 2017.

[98] R. Nelson, "Smart factories leverage cloud, edge computing," *Eval. Eng.*, vol. 56, no. 6, pp. 14–18, 2017.

[99] W. Steiner and S. Poledna, "Fog computing as enabler for the industrial Internet of Things," *e i Elektrotechnik und Informationstechnik*, vol. 133, no. 7, pp. 310–314, 2016.

[100] B. Liang, *Mobile Edge Computing*. New Delhi, India: Cambridge Univ. Press, 2017.

[101] D. Zhang, L. T. Yang, and H. Huang, "Searching in Internet of Things: Vision and challenges," in *Proc. 9th Int. Symp. Parallel Distrib. Process. Appl. (ISPA)*, Busan, South Korea, 2011, pp. 201–206.

[102] P. Bellavista and A. Zanni, "Towards better scalability for IoT-cloud interactions via combined exploitation of MQTT and CoAP," in *Proc. IEEE 2nd Int. Forum Res. Technol. Soc. Ind. Leveraging Better Tomorrow (RTSI)*, Bologna, Italy, 2016, pp. 1–6.

[103] J. Ren, H. Guo, C. Xu, and Y. Zhang, "Serving at the edge: A scalable IoT architecture based on transparent computing," *IEEE Netw.*, vol. 31, no. 5, pp. 96–105, Aug. 2017.

[104] R. Morabito, R. Petrolo, V. Loscri, and N. Mitton, "LEGIoT: A lightweight edge gateway for the Internet of Things," *Future Gener. Comput. Syst.*, vol. 81, pp. 1–15, Apr. 2018.

[105] A. Ceselli, M. Premoli, and S. Secci, "Mobile edge cloud network design optimization," *IEEE/ACM Trans. Netw.*, vol. 25, no. 3, pp. 1818–1831, Jun. 2017.

[106] M. Peng, S. Yan, K. Zhang, and C. Wang, "Fog-computing-based radio access networks: Issues and challenges," *IEEE Netw.*, vol. 30, no. 4, pp. 46–53, Jul./Aug. 2016.

[107] R. Tandon and O. Simeone, "Harnessing cloud and edge synergies: Toward an information theory of fog radio access networks," *IEEE Commun. Mag.*, vol. 54, no. 8, pp. 44–50, Aug. 2016.

[108] M. Peng and K. Zhang, "Recent advances in fog radio access networks: Performance analysis and radio resource allocation," *IEEE Access*, vol. 4, pp. 5003–5009, 2016.

[109] B. P. Rimal, D. P. Van, and M. Maier, "Mobile-edge computing versus centralized cloud computing over a converged FiWi access network," *IEEE Trans. Netw. Service Manag.*, vol. 14, no. 3, pp. 498–513, Sep. 2017.

[110] M. Agiwal, A. Roy, and N. Saxena, "Next generation 5G wireless networks: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 3, pp. 1617–1655, 3rd Quart., 2016.

[111] S. Barbarossa, E. Ceci, M. Merluzzi, and E. Calvanese-Strinati, "Enabling effective mobile edge computing using millimeterwave links," in *Proc. Int. Conf. Commun. Workshops (ICC Workshops)*, Paris, France, 2017, pp. 367–372.

[112] S. Barbarossa, E. Ceci, and M. Merluzzi, "Overbooking radio and computation resources in mmW-mobile edge computing to reduce vulnerability to channel intermittency," in *Proc. Eur. Conf. Netw. Commun. (EuCNC)*, Oulu, Finland, 2017, pp. 1–5.

[113] A. Dongare *et al.*, "OpenChirp: A low-power wide-area networking architecture," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops (PerCom Workshops)*, 2017, pp. 569–574.

[114] N. Ansari and X. Sun, "Mobile edge computing empowers Internet of Things," *IEICE Trans. Commun.*, vol. 101, no. 3, pp. 604–619, 2018.

[115] I. Farris *et al.*, "Federations of connected things for delay-sensitive IoT services in 5G environments," in *Proc. Int. Conf. Commun. (ICC)*, Paris, France, 2017, pp. 1–6.

[116] I. Farris, A. Orsino, L. Militano, A. Iera, and G. Araniti, "Federated IoT services leveraging 5G technologies at the edge," *Ad Hoc Netw.*, vol. 68, pp. 58–69, Jan. 2018.

[117] A. Orsino *et al.*, "Exploiting D2D communications at the network edge for mission-critical IoT applications," in *Proc. 23th Eur. Wireless Conf.*, Dresden, Germany, 2017, pp. 1–6.

[118] S.-W. Ko, K. Han, and K. Huang, "Wireless networks for mobile edge computing: Spatial modelling and latency analysis," *IEEE Trans. Wireless Commun.*, to be published, doi: 10.1109/TWC.2018.2840120.

[119] F. Samie *et al.*, "Computation offloading and resource allocation for low-power IoT edge devices," in *Proc. 3rd World Forum Internet Things (WF-IoT)*, Reston, VA, USA, 2016, pp. 7–12.

[120] 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.

[121] Y. Yu, X. Li, and C. Qian, "SDLB: A scalable and dynamic software load balancer for fog and mobile edge computing," in *Proc. Workshop Mobile Edge Commun.*, Los Angeles, CA, USA, 2017, pp. 55–60.

[122] R. Vilalta *et al.*, "TelcoFog: A unified flexible fog and cloud computing architecture for 5G networks," *IEEE Commun. Mag.*, vol. 55, no. 8, pp. 36–43, Aug. 2017.

[123] M. Bouet and V. Conan, "Geo-partitioning of MEC resources," in *Proc. Workshop Mobile Edge Commun.*, Los Angeles, CA, USA, 2017, pp. 43–48.

[124] H. Flores *et al.*, "Large-scale offloading in the Internet of Things," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops (PerCom Workshops)*, 2017, pp. 479–484.

[125] C. Wang, C. Liang, F. R. Yu, Q. Chen, and L. Tang, "Computation offloading and resource allocation in wireless cellular networks with mobile edge computing," *IEEE Trans. Wireless Commun.*, vol. 16, no. 8, pp. 4924–4938, Aug. 2017.

[126] X. Lyu *et al.*, "Optimal schedule of mobile edge computing for Internet of Things using partial information," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 11, pp. 2606–2615, Nov. 2017.

[127] H. Gupta, A. V. Dastjerdi, S. K. Ghosh, and R. Buyya, "iFogSim: A toolkit for modeling and simulation of resource management techniques in the Internet of Things, edge and fog computing environments," *Softw. Pract. Exp.*, vol. 47, no. 9, pp. 1275–1296, 2017.

[128] 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. (CLOUD)*, New York, NY, USA, 2015, pp. 9–16.

[129] M. Chen *et al.*, "Mobility-aware caching and computation offloading in 5G ultra-dense cellular networks," *Sensors*, vol. 16, no. 7, p. 974, 2016.

[130] 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.

[131] 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.

[132] C. Wang, F. R. Yu, C. Liang, Q. Chen, and L. Tang, "Joint computation offloading and interference management in wireless cellular networks with mobile edge computing," *IEEE Trans. Veh. Technol.*, vol. 66, no. 8, pp. 7432–7445, Aug. 2017.

[133] Y. Sun, S. Zhou, and J. Xu, "EMM: Energy-aware mobility management for mobile edge computing in ultra dense networks," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 11, pp. 2637–2646, Nov. 2017.

[134] J. Liu, Y. Mao, J. Zhang, and K. B. Letaief, "Delay-optimal computation task scheduling for mobile-edge computing systems," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Barcelona, Spain, 2016, pp. 1451–1455.

[135] C. You, K. Huang, H. Chae, and B.-H. Kim, "Energy-efficient resource allocation for mobile-edge computation offloading," *IEEE Trans. Wireless Commun.*, vol. 16, no. 3, pp. 1397–1411, Mar. 2017.

[136] P. Mach and Z. Becvar, "Cloud-aware power control for cloud-enabled small cells," in *Proc. IEEE Globecom Workshops*, Austin, TX, USA, 2014, pp. 1038–1043.

[137] P. Mach and Z. Becvar, "Cloud-aware power control for real-time application offloading in mobile edge computing," *Trans. Emerg. Telecommun. Technol.*, vol. 27, no. 5, pp. 648–661, 2016.

[138] T. Taleb and A. Ksentini, "An analytical model for follow me cloud," in *Proc. IEEE Glob. Commun. Conf. (GLOBECOM)*, Atlanta, GA, USA, 2013, pp. 1291–1296.

[139] D. Wu, D. I. Arkhipov, E. Asmare, Z. Qin, and J. A. McCann, "UbiFlow: Mobility management in urban-scale software defined IoT," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, 2015, pp. 208–216.

[140] W. Shang *et al.*, "Named data networking of things (invited paper)," in *Proc. IEEE 1st Int. Conf. Internet Things Design Implement. (IoTDI)*, Berlin, Germany, 2016, pp. 117–128.

[141] F. Giust, L. Cominardi, and C. J. Bernardos, "Distributed mobility management for future 5G networks: Overview and analysis of existing approaches," *IEEE Commun. Mag.*, vol. 53, no. 1, pp. 142–149, Jan. 2015.

[142] C. N. Le Tan, C. Klein, and E. Elmroth, "Location-aware load prediction in edge data centers," in *Proc. 2nd Int. Conf. Fog Mobile Edge Comput. (FMEC)*, Valencia, Spain, 2017, pp. 25–31.

[143] V. Vassilakis *et al.*, "Security analysis of mobile edge computing in virtualized small cell networks," in *Proc. IFIP Int. Conf. Artif. Intell. Appl. Innov.*, Thessaloniki, Greece, 2016, pp. 653–665.

[144] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the Internet of Things: Perspectives and challenges," *Wireless Netw.*, vol. 20, no. 8, pp. 2481–2501, 2014.

[145] I. Stojmenovic, S. Wen, X. Huang, and H. Luan, "An overview of fog computing and its security issues," *Concurrency Comput. Pract. Exp.*, vol. 28, no. 10, pp. 2991–3005, 2016.

[146] J. Wan *et al.*, "Cloud-enabled wireless body area networks for pervasive healthcare," *IEEE Netw.*, vol. 27, no. 5, pp. 56–61, Sep./Oct. 2013.

[147] J. Wan *et al.*, "VCMIA: A novel architecture for integrating vehicular cyber-physical systems and mobile cloud computing," *Mobile Netw. Appl.*, vol. 19, no. 2, pp. 153–160, 2014.

[148] N. Varga, L. Bokor, and E. Piri, "A network-assisted flow mobility architecture for optimized mobile medical multimedia transmission," *Ann. Telecommun.*, vol. 71, nos. 9–10, pp. 489–502, 2016.

[149] M. Taylor, "The EU data retention directive," *Comput. Law Security Rev.*, vol. 22, no. 4, pp. 309–312, 2006.

[150] S. Haggard and J. R. Lindsay. (2015). *North Korea and the Sony Hack: Exporting Instability Through Cyberspace*. Accessed: May 2, 2018. [Online]. Available: https://www.eastwestcenter.org/system/tdf/private/api117.pdf?file=1&type=node&id=35164

[151] P. German, "A new month, a new data breach," *Netw. Security*, vol. 2016, no. 3, pp. 18–20, 2016.

[152] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed Internet of Things," *Comput. Netw.*, vol. 57, no. 10, pp. 2266–2279, 2013.

[153] F. Kemmer, C. Reich, M. Knahl, and N. Clarke, "Software defined privacy," in *Proc. IEEE Int. Conf. Cloud Eng. Workshop (IC2EW)*, Berlin, Germany, 2016, pp. 25–29.

[154] 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.

[155] S. F. Abedin, M. G. R. Alam, N. H. Tran, and C. S. Hong, "A fog based system model for cooperative IoT node pairing using matching theory," in *Proc. IEEE 17th Asia–Pac. Netw. Oper. Manag. Symp. (APNOMS)*, Busan, South Korea, 2015, pp. 309–314.

[156] P. De Hert and V. Papakonstantinou, "The proposed data protection regulation replacing directive 95/46/EC: A sound system for the protection of individuals," *Comput. Law Security Rev.*, vol. 28, no. 2, pp. 130–142, 2012.

[157] S. Ziegler, A. Skarmeta, J. Bernal, E. E. Kim, and S. Bianchi, "ANASTACIA: Advanced networked agents for security and trust assessment in CPS IoT architectures," in *Proc. IEEE Glob. Internet Things Summit (GIoTS)*, Geneva, Switzerland, 2017, pp. 1–6.

[158] T. D. Dang and D. Hoang, "A data protection model for fog computing," in *Proc. IEEE Fog Mobile Edge Comput. (FMEC)*, Valencia, Spain, 2017, pp. 32–38.

[159] R. Mijumbi *et al.*, "Network function virtualization: State-of-the-art and research challenges," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 1, pp. 236–262, 1st Quart., 2016.

[160] L. Gupta, R. Jain, and H. A. Chan, "Mobile edge computing—An important ingredient of 5G networks," *IEEE Softw.*, to be published. [Online]. Available: http://sdn.ieee.org/newsletter/march-2016/mobile-edge-computing-an-important-ingredient-of-5g-network

[161] B. Yang, W. K. Chai, G. Pavlou, and K. V. Katsaros, "Seamless support of low latency mobile applications with NFV-enabled mobile edge-cloud," in *Proc. IEEE Int. Conf. Cloud Netw. (Cloudnet)*, Pisa, Italy, 2016, pp. 136–141.

[162] B. Li, Y. Zhang, and L. Xu, "An MEC and NFV integrated network architecture," *ZTE Commun.*, vol. 15, no. 2, p. 1, 2017.

[163] V. Sciancalepore, F. Giust, K. Samdanis, and Z. Yousaf, "A double-tier MEC-NFV architecture: Design and optimisation," in *Proc. IEEE Conf. Stand. Commun. Netw. (CSCN)*, Berlin, Germany, 2016, pp. 1–6.

[164] G. A. Carella *et al.*, "Prototyping NFV-based multi-access edge computing in 5G ready networks with open baton," in *Proc. IEEE Conf. Netw. Softwarization (NetSoft)*, Bologna, Italy, 2017, pp. 1–4.

[165] B. Blanco *et al.*, "Technology pillars in the architecture of future 5G mobile networks: NFV, MEC and SDN," *Comput. Stand. Interfaces*, vol. 54, pp. 216–228, Nov. 2017.

[166] S. Peng *et al.*, "QoE-oriented mobile edge service management leveraging SDN and NFV," *Mobile Inf. Syst.*, vol. 2017, Nov. 2017, Art. no. 3961689.

[167] S. Ali and M. Ghazal, "Real-time heart attack mobile detection service (RHAMDS): An IoT use case for software defined networks," in *Proc. IEEE 30th Can. Conf. Elect. Comput. Eng. (CCECE)*, Windsor, ON, Canada, 2017, pp. 1–6.

[168] I. Farris *et al.*, "Towards provisioning of SDN/NFV-based security enablers for integrated protection of IoT systems," in *Proc. IEEE Conf. Stand. Commun. Netw. (CSCN)*, Helsinki, Finland, 2017, pp. 169–174.

[169] A. Huang, N. Nikaein, T. Stenbock, A. Ksentini, and C. Bonnet, "Low latency MEC framework for SDN-based LTE/LTE-A networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Paris, France, 2017, pp. 1–6.

[170] B. Nguyen, N. Choi, M. Thottan, and J. Van der Merwe, "SIMECA: SDN-based IoT mobile edge cloud architecture," in *Proc. IEEE IFIP Symp. Integr. Netw. Service Manag. (IM)*, Lisbon, Portugal, 2017, pp. 503–509.

[171] M. S. Hossain *et al.*, "Impact of next-generation mobile technologies on IoT-cloud convergence," *IEEE Commun. Mag.*, vol. 55, no. 1, pp. 18–19, Jan. 2017.

[172] J. Liu *et al.*, "High-efficiency urban traffic management in context-aware computing and 5G communication," *IEEE Commun. Mag.*, vol. 55, no. 1, pp. 34–40, Jan. 2017.

[173] K. Phemius, J. Seddar, M. Bouet, H. Khalifé, and V. Conan, "Bringing SDN to the edge of tactical networks," in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, Baltimore, MD, USA, 2016, pp. 1047–1052.

[174] C. Aggarwal and K. Srivastava, "Securing IoT devices using SDN and edge computing," in *Proc. IEEE 2nd Int. Conf. Next Gener. Comput. Technol. (NGCT)*, 2016, pp. 877–882.

[175] A. V. Vasilakos, Z. Li, G. Simon, and W. You, "Information centric network: Research challenges and opportunities," *J. Netw. Comput. Appl.*, vol. 52, pp. 1–10, Jun. 2015.

[176] G. Piro, L. A. Grieco, G. Boggia, and P. Chatzimisios, "Information-centric networking and multimedia services: Present and future challenges," *Trans. Emerg. Telecommun. Technol.*, vol. 25, no. 4, pp. 392–406, 2014.

[177] E. Ahmed *et al.*, "Enabling mobile and wireless technologies for smart cities," *IEEE Commun. Mag.*, vol. 55, no. 1, pp. 74–75, Jan. 2017.

[178] M. Maier, M. Chowdhury, B. P. Rimal, and D. P. Van, "The tactile Internet: Vision, recent progress, and open challenges," *IEEE Commun. Mag.*, vol. 54, no. 5, pp. 138–145, May 2016.

[179] R. Ravindran, A. Chakraborti, S. O. Amin, A. Azgin, and G. Wang, "Realizing ICN in 3GPP's 5G NextGen core architecture," *arXiv preprint arXiv:1711.02232*, 2017.

[180] *Understanding Information-Centric Networking and Mobile Edge Computing*, 5G Americas, Bellevue, WA, USA, Dec. 2016. Accessed: Jan. 12, 2018. [Online]. Available: http://www.5gamericas.org/files/1214/8175/3330/Understanding_Information_Centric_Networking_and_Mobile_Edge_Computing.pdf

[181] Y. Zhou, F. R. Yu, J. Chen, and Y. Kuo, "Video transcoding, caching, and multicast for heterogeneous networks over wireless network virtualization," *Commun. Lett.*, vol. 22, no. 1, pp. 141–144, Jan. 2018.

[182] Y. Zhou, F. R. Yu, J. Chen, and Y. Kuo, "Resource allocation for information-centric virtualized heterogeneous networks with in-network caching and mobile edge computing," *IEEE Trans. Veh. Technol.*, vol. 66, no. 12, pp. 11339–11351, Dec. 2017.

[183] R. Huo *et al.*, "Software defined networking, caching, and computing for green wireless networks," *IEEE Commun. Mag.*, vol. 54, no. 11, pp. 185–193, Nov. 2016.

[184] C. Ge, N. Wang, S. Skillman, G. Foster, and Y. Cao, "QoE-driven DASH video caching and adaptation at 5G mobile edge," in *Proc. 3rd ACM Conf. Inf. Centric Netw.*, Kyoto, Japan, 2016, pp. 237–242.

[185] K. Samdanis, X. Costa-Perez, and V. Sciancalepore, "From network sharing to multi-tenancy: The 5G network slice broker," *IEEE Commun. Mag.*, vol. 54, no. 7, pp. 32–39, Jul. 2016.

[186] *NGMN 5G Project Requirements & Architecture—Work Stream E2E Architecture Version 1.0.8*, Sep. 2016.

[187] N. Nikaein *et al.*, "Network store: Exploring slicing in future 5G networks," in *Proc. ACM 10th Int. Workshop Mobility Evolving Internet Archit.*, 2015, pp. 8–13.

[188] (Nov. 2015). *Network Slicing for 5G Networks & Services, 5G Americas White Paper—Network Slicing for 5G and Beyond*. Accessed: Mar. 1, 2018. [Online]. Available: http://www.5gamericas.org/files/3214/7975/0104/5G_Americas_Network_Slicing_11.21_Final.pdf

[189] H. Zhang *et al.*, "Network slicing based 5G and future mobile networks: Mobility, resource management, and challenges," *IEEE Commun. Mag.*, vol. 55, no. 8, pp. 138–145, Aug. 2017.

[190] K. Katsalis, N. Nikaein, E. Schiller, A. Ksentini, and T. Braun, "Network slices toward 5G communications: Slicing the LTE network," *IEEE Commun. Mag.*, vol. 55, no. 8, pp. 146–154, Aug. 2017.

[191] R. Muñoz *et al.*, "The ADRENALINE testbed: An SDN/NFV packet/optical transport network and edge/core cloud platform for end-to-end 5G and IoT services," in *Proc. IEEE Eur. Conf. Netw. Commun. (EuCNC)*, Oulu, Finland, 2017, pp. 1–5.

[192] F. van Lingen *et al.*, "The unavoidable convergence of NFV, 5G, and fog: A model-driven approach to bridge cloud and edge," *IEEE Commun. Mag.*, vol. 55, no. 8, pp. 28–35, Aug. 2017.

[193] R. Vilalta, A. Mayoral, R. Casellas, R. Martínez, and R. Muñoz, "SDN/NFV orchestration of multi-technology and multi-domain networks in cloud/fog architectures for 5G services," in *Proc. IEEE 21st OptoElectron. Commun. Conf. (OECC) Held Jointly Int. Conf. Photon. Switching (PS)*, Niigata, Japan, 2016, pp. 1–3.
[194] R. Ravindran, A. Chakraborti, S. O. Amin, A. Azgin, and G. Wang, "5G-ICN: Delivering ICN services over 5G using network slicing," *IEEE Commun. Mag.*, vol. 55, no. 5, pp. 101–107, May 2017.
[195] *SESAME Project, H2020 EU Project*. Accessed: Mar. 25, 2018. [Online]. Available: http://www.sesame-h2020-5g-ppp.eu/Home.aspx
[196] *ANASTACIA Project, H2020 EU Project*. Accessed: Feb. 11, 2018. [Online]. Available: http://www.anastacia-h2020.eu/
[197] (2017). *5G-MiEdge Project: Millimeter-Wave Edge Cloud As an Enabler for 5G Ecosystem, H2020 EU&Japan Project*. Accessed: Feb. 15, 2018. [Online]. Available: https://5g-miedge.eu/
[198] *5G!Pagoda, EU Japan Collaboration Project*. Accessed: Feb. 19, 2018. [Online]. Available: https://5g-pagoda.aalto.fi/
[199] *Inter-IoT Project, H2020 EU Project*. Accessed: Feb. 15, 2018. [Online]. Available: http://www.inter-iot-project.eu/
[200] *5G MoNArch Project, H2020 EU Project*. Accessed: Feb. 17, 2018. [Online]. Available: https://5g-monarch.eu/
[201] *5G ESSENCE Project, H2020 EU Project*. Accessed: Apr. 15, 2018. [Online]. Available: https://5g-ppp.eu/5g-essence/
[202] *MATILDA Project, H2020 EU Project*. Accessed: Apr. 15, 2018. [Online]. Available: https://5g-ppp.eu/matilda/
[203] *5GCity Project, H2020 EU Project*. Accessed: Feb. 22, 2018. [Online]. Available: http://www.5gcity.eu/
[204] *MONICA Project, H2020 EU Project*. Accessed: Mar. 11, 2018. [Online]. Available: http://www.monica-project.eu/
[205] *AUTOPILOT Project, H2020 EU Project*. Accessed: Feb. 15, 2018. [Online]. Available: http://autopilot-project.eu/
[206] *5G-CORAL Project, H2020 EU Project*. Accessed: Mar. 15, 2018. [Online]. Available: http://5g-coral.eu/
[207] *ETSI and VRARA Cooperate on Virtual and Augmented Reality, ETSI News Event*. Accessed: May 4, 2018. [Online]. Available: http://www.etsi.org/news-events/
[208] J. Liu, T. Zhao, S. Zhou, Y. Cheng, and Z. Niu, "CONCERT: A cloud-based architecture for next-generation cellular systems," *IEEE Wireless Commun.*, vol. 21, no. 6, pp. 14–22, Dec. 2014.
[209] A. Mestres *et al.*, "Knowledge-defined networking," *SIGCOMM Comput. Commun. Rev.*, vol. 47, no. 3, pp. 2–10, 2017.
[210] A. Crutcher *et al.*, "Hyperprofile-based computation offloading for mobile edge networks," in *Proc. IEEE 14th Int. Conf. Mobile Ad Hoc Sensor Syst. (MASS)*, Orlando, FL, USA, 2017, pp. 525–529.
[211] E. Ahmed *et al.*, "Bringing computation closer toward the user network: Is edge computing the solution?" *IEEE Commun. Mag.*, vol. 55, no. 11, pp. 138–144, Nov. 2017.
[212] L. T. Sorensen, S. Khajuria, and K. E. Skouby, "5G visions of user privacy," in *Proc. IEEE 81st Veh. Technol. Conf. (VTC Spring)*, Glasgow, U.K., 2015, pp. 1–4.
[213] A. Cavoukian and M. Chibba, "A regulartor's perspective: Leading the way with privacy by design," *Cyber Security in Future Internet, Security and Privacy by Design. OUTLOOK, Visions and Research for the Wireless World*, White Paper, Wireless world Res. Forum, Zürich, Switzerland, 2014.
[214] D. Pitt, "Trust in the cloud: The role of SDN," *Netw. Security*, vol. 2013, no. 3, pp. 5–6, 2013.
[215] J. Aikat *et al.*, "Rethinking security in the era of cloud computing," *IEEE Security Privacy*, vol. 15, no. 3, pp. 60–69, Jun. 2017.
[216] H. Li, G. Shou, Y. Hu, and Z. Guo, "Mobile edge computing: Progress and challenges," in *Proc. IEEE Int. Conf. Mobile Cloud Comput Services Eng. (MobileCloud)*, Oxford, U.K., 2016, pp. 83–84.

Pawani Porambage received the bachelor's degree in electronics and telecommunication engineering from the University of Moratuwa, Sri Lanka, in 2010 and the master's degree in ubiquitous networking and computer networking from the University of Nice Sophia Antipolis, France, in 2012. She is currently pursuing the Doctoral degree with the Centre for Wireless Communications, University of Oulu, Finland. In 2014, she was a Visiting Researcher with CSG, University of Zurich, and Vrije Universiteit Brussel. She has co-authored over 25 peer-reviewed scientific articles. Her main research interests include lightweight security protocols, security and privacy in IoT, MEC, network slicing, and wireless sensor networks.

Jude Okwuibe received the B.Sc. degree in telecommunications and wireless technologies from the American University of Nigeria, Yola, in 2011 and the master's degree in wireless communications engineering from the University of Oulu, Finland, in 2015. He is currently pursuing the Doctoral degree in communications engineering with the University of Oulu Graduate School, Finland. His research interests are 5G and future networks, IoT, SDN, network security, and biometric verifications.

Madhusanka Liyanage received the B.Sc. degree (First Class Hons.) in electronics and telecommunication engineering from the University of Moratuwa, Moratuwa, Sri Lanka, in 2009, the M.Eng. degree from the Asian Institute of Technology, Bangkok, Thailand, in 2011, the M.Sc. degree from the University of Nice Sophia Antipolis, Nice, France, in 2011, and the Ph.D. degree in communication engineering from the University of Oulu, Oulu, Finland, in 2016. From 2011 to 2012, he was a Research Scientist with the I3S Laboratory and Inria, Shopia Antipolis, France. He is currently a Post-Doctoral Researcher and a Project Manager with the Center for Wireless Communications, University of Oulu. He has been a Visiting Research Fellow with the Department of Computer Science, University of Oxford, Data61, CSIRO, Sydney, Australia, the Infolabs21, Lancaster University, U.K., Computer Science and Engineering, University of New South Wales, Australia, and the Laboratory of Computer Science of Paris 6, Sorbonne Universit, France, from 2015 to 2019.

He has co-authored over 40 publications including two edited books with Wiley and one patent. He served as a Technical program Committee Members at EAI M3Apps 2016, 5GU 2017, EUCNC 2017, EUCNC 2018, MASS 2018, 5G-WF 2018, and MCWN 2018 conferences and the Technical program Co-Chair in SecureEdge Workshop at IEEE CIT 2017, MEC-IoT Workshop at 5GWF 2018, and Blockchain in IoT workshop at Globecom 2018 conferences. He has also served as the Session Chair in a number of other conferences, including IEEE WCNC 2013, CROWNCOM 2014, 5GU 2014, IEEE CIT 2017, IEEE PIMRC 2017, and IEEE 5GWF 2018. He was a recipient of two best Paper Awards in the areas of SDMN security (at NGMAST 2015) and 5G Security (at IEEE CSCN 2017). He has been awarded two research grants (IRC Post-Doctoral Grant and Marie-Curie Fellowship) and 21 other prestigious awards/scholarships during his research career.

Dr. Liyanage was a recipient of the Best Researcher Award at the Centre for Wireless Communications, University of Oulu for his excellent contribution in project management and dissemination activities in 2015, 2016, and 2017, the CELTIC Excellence Award for his research projects (MEVICO and SIGMONA Projects) in 2013 and 2017, respectively, and the Celtic Innovation Award for his SIGMONA Project in 2018. He has worked for over 12 EU, international, and national projects in ICT domain. He held responsibilities as a Leader of work packages in several national and EU projects. He is currently the Finnish National Coordinator for EU COST Action CA15127 on resilient communication services. He is/was serving as a Management Committee Member for four other EU COST action projects, namely EU COST Action IC1301, IC1303, CA15104, CA15127, and CA16226. He has over three years experience in research project management, research group leadership, research project proposal preparation, project progress documentation, and graduate student co-supervision/mentoring skills.

His research interests are SDN, IoT, Blockchain, MEC, and mobile and virtual network security.

Mika Ylianttila (M'99–SM'08) received the Doctoral degree in communications engineering from the University of Oulu, Finland, in 2005, where he is a Full-Time Professor with the Centre for Wireless Communications, Faculty of Information Technology and Electrical Engineering. He has co-authored over 150 international peer-reviewed articles. His research interests include 5G applications and services, software-defined networking, network softwarization and virtualization, network security, and edge computing. He is an Editor of *Wireless Networks* journal.

Tarik Taleb (M'05–SM'10) received the B.E. degree (with Distinction) in information engineering and the M.Sc. and Ph.D. degrees in information sciences from Tohoku University, Japan, in 2001, 2003, and 2005, respectively. He is currently a Professor with the School of Electrical Engineering, Aalto University, Finland. He was a Senior Researcher and a 3GPP Standards Expert with NEC Europe Ltd., Heidelberg, Germany. He was then leading the NEC Europe Labs Team working on research and development projects on carrier cloud platforms, an important vision of 5G systems. He was an Assistant Professor with the Graduate School of Information Sciences, Tohoku University, until 2009, in a laboratory fully funded by KDDI. From 2005 to 2006, he was a Research Fellow with the Intelligent Cosmos Research Institute, Sendai, Japan. He is an IEEE Communications Society (ComSoc) Distinguished Lecturer.

His research interests lie in the field of architectural enhancements to mobile core networks (particularly 3GPPs), mobile cloud networking, network function virtualization, software defined networking, mobile multimedia streaming, intervehicular communications, and social media networking. He has been also directly engaged in the development and standardization of the Evolved Packet System as a member of 3GPPs System Architecture working group. He is a member of the IEEE Communications Society Standardization Program Development Board. He founded the IEEE Workshop on Telecommunications Standards: from Research to Standards a successful event that got awarded best workshop award by ComSoC. He has also founded and has been the Steering Committee Chair of the IEEE Conference on Standards for Communications and Networking.

Prof. Taleb is the General Chair of the 2019 edition of the IEEE Wireless Communications and Networking Conference (WCNC19) to be held in Marrakech, Morocco. He is/was on the editorial board of the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, the *IEEE Wireless Communications Magazine*, the IEEE JOURNAL ON INTERNET OF THINGS, the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, the IEEE COMMUNICATIONS SURVEYS & TUTORIALS, and a number of Wiley journals. Till 2016, he served as the Chair of the Wireless Communications Technical Committee, the largest in IEEE ComSoC. He also served as the Vice Chair of the Satellite and Space Communications Technical Committee of IEEE ComSoc from 2006 to 2010. He has been on the technical program committee of different IEEE conferences, including Globecom, ICC, and WCNC, and chaired some of their symposia.

He was a (co-)recipient of the 2017 IEEE Communications Society Fred W. Ellersick Prize in 2017, the 2009 IEEE ComSoc Asia–Pacific Best Young Researcher Award in 2009, the 2008 TELECOM System Technology Award from the Telecommunications Advancement Foundation in 2008, the 2007 Funai Foundation Science Promotion Award in 2007, the 2006 IEEE Computer Society Japan Chapter Young Author Award in 2006, the Niwa Yasujirou Memorial Award in 2005, and the Young Researcher's Encouragement Award from the Japan Chapter of the IEEE Vehicular Technology Society in 2003. He was also a recipient of best paper awards at prestigious conferences for some of his research work.