Survey on Multi-Access Edge Computing Security and Privacy

Pasika Ranaweera*, *Member, IEEE,* Anca Delia Jurcut, *Member, IEEE,*
Madhusanka Liyanage, *Senior Member, IEEE*

***Abstract*—The European Telecommunications Standards Institute (ETSI) has introduced the paradigm of Multi-Access Edge Computing (MEC) to enable efficient and fast data processing in mobile networks. Among other technological requirements, security and privacy are significant factors in the realization of MEC deployments. In this paper, we analyse the security and privacy of the MEC system. We introduce a thorough investigation of the identification and the analysis of threat vectors in the ETSI standardized MEC architecture. Furthermore, we analyse the vulnerabilities leading to the identified threat vectors and propose potential security solutions to overcome these vulnerabilities. The privacy issues of MEC are also highlighted, and clear objectives for preserving privacy are defined. Finally, we present future directives to enhance the security and privacy of MEC services.**

***Index Terms*—Multi-Access Edge Computing (MEC), Security, Privacy, Internet of Things (IoT), 5G, Cloud Computing, Future Networks**

I. Introduction

Multi-Access Edge Computing (MEC) is a nascent paradigm proposed by the European Telecommunications Standards Institute (ETSI) to overcome the issues exerted from intricacies in highly evolving mobile and wireless communication networks. The underlying principle of MEC is to extend the cloud computing (CC) capabilities to the edge of the mobile network to curtail the attributed constraints on existing cloud infrastructure [1]. More anecdotally, MEC complements the corporate data and processing centres, providing compute, storage, networking, and data analytic resources at locations in the proximity of the data source [2]. The impending fifth generation (5G) mobile technology is one of the rationales for the emergence of MEC. The guaranteed performance metrics of 5G are: data rates up to 10 GB/s, service level latency below 1 ms, ultra-high reliability of 99.99999%, reduced energy consumption of 90%, and support for 300,000 devices within a single cell [1], [3]. In order to meet these requirements, migrating the service infrastructure to a proximate location is a critical approach. Thus, the MEC paradigm is formed and designed with the above considerations.

A typical intelligent, autonomous application or service executed on a smart device requires connectivity to the centralized cloud services for circulating control information and authentication credentials in case of an authorization mechanism. This connectivity is generally linked through the Internet for facilitating a communication channel with strong cryptic credentials. This ubiquitous and bandwidth-consuming connectivity to out-of-proximity entities is restricting the responsiveness of the applications, hindering the real-time services guaranteed by forthcoming mobile technologies. The resource availability in the in-proximity edge servers of MEC deployments are elevating the feasibility of launching real-time applications with improved autonomy. Thus, connectivity to the centralized cloud infrastructure is not required for multitudes of functions in applications hosted on current smart devices. However, more hardware should be installed in the Base Station (BS) by Mobile Network Operators (MNOs) for realizing this technology. In spite of the initial investment made by the MNO, the long-term revenue of the MNO could be increased because of the MEC-enabled applications [4].

In the existing CC service architecture depicted in Fig. 1, all the emanated service requests in the Radio Access Network (RAN) are traversed to the cloud servers, which are located at different global locations due to the non-existent storage and processing platform at the BS. The subscribers are unaware of the exact locations of the servers due to the outsourcing process. This fact is raising security and privacy concerns, as the personal data of the subscribers are handled by third parties without any concrete assurances. The channel conveying the elevated service requests and data to the cloud servers is bound to form a bottleneck in the network traffic in addition to the RAN access interface [4]. Therefore, CC-based services are expected to endure latency issues, jitter, and unresponsiveness in addition to the security ramifications from service interruption–based attacks perpetrated by adversaries. These factors prove the improbability of successfully deploying impending applications with 5G technology such as Ultra High Definition (UHD) video streaming, Augmented Reality (AR), Virtual Reality (VR), Mixed Reality (MR), Tactile internet, Machine Type Communication (MTC), Machine-to-Machine (M2M), Unmanned Aerial Vehicle (UAV), and Vehicle-to-Everything (V2E). The storage and processing infrastructure facilitated by MEC deployments, however, are ensuring the benefits of ultra-low latency, locational awareness, proximate data outsourcing, and improved capacity in the edge devices. These features enable higher bandwidth and real-time responsiveness to the subscriber applications. Moreover, MEC-based services within the RAN enhance computational processing power to avoid bottlenecks with directed mobile traffic [5].

Pasika Ranaweera is with School of Computer Science, University College Dublin (UCD), Ireland. e-mail:pasika.ranaweera@ucdconnect.ie

Anca D. Jurcut is with University College Dublin (UCD), Ireland. e-mail:anca.jurcut@ucd.ie

Madhusanka Liyanage is with the School of Computer Science, University College Dublin (UCD), Ireland and the Centre for Wireless Communications, University of Oulu, Finland. e-mail:madhusanka@ucd.ie, madhusanka.liyanage@oulu.fi

*Corresponding author

TABLE I: Summary of important acronyms.

Acronym	Definition
3GPP	Third Generation Partnership Project
4G	Fourth Generation Telecommunication Networks
5G	Fifth Generation Telecommunication Networks
AI	Artificial Intelligence
AR	Augmented Reality
BLE	Bluetooth Low Energy
BS	Base Station
CC	Cloud Computing
CDN	Content Delivery Network
CFS	Customer Facing Service
CIA	Confidentiality, Integrity, and Availability
CPS	Cyber Physical System
D2D	Device-to-Device
DDoS	Distributed Denial of Service
DoS	Denial of Service
E2E	End-to-end
eMBB	enhance Mobile Broadband
eNodeB	Evolved Node B
ETSI	European Telecommunications Standards Institute
GDPR	General Data Protection Regulation
GSM	Global System for Mobile Communication
GT	Game Theory
ICN	Information Centric Networking
IDS	Intrusion Detection Scheme
IIoT	Industrial Internet of Things
IoT	Internet of Things
ISG	Industry Specification Group
ITS	Intelligent Transport System
LAN	Local Area Network
LADN	Local Area Data Network
LPWAN	Low-power Wide Area Network
LTE	Long Term Evolution
M2M	Machine-to-Machine
MANET	Mobile Ad-hoc Network
MANO	Management and Network Orchestration
MCC	Mobile Cloud Computing
ME	Mobile Edge
MEC	Multi-Access Edge Computing
MEH	Mobile Edge Host
MEO	Mobile Edge Orchestrator
MEN	Mobile Edge Network
MEPM	Mobile Edge Platform Manager
MES	Mobile Edge Service
MitM	Man-in-the-Middle
mmWave	millimeter-Wave
MNO	Mobile Network Operator
MR	Mixed Reality
MTC	Machine Type Communication
NB-IoT	Narrow-band IoT
NFC	Near Field Communication
NFV	Network Function Virtualization
NS	Network Slicing
OSS	Operation Support System
PbD	Privacy by Design
QoE	Quality of Experience
RAN	Radio Access Networks
RFID	Radio-Frequency Identification
SDN	Software-Defined Networking
SDP	Software-Defined Privacy
TV	Threat Vector
UALCMP	User Application Life-Cycle Management Proxy
UAV	Unmanned Aerial Vehicles
UE	User Equipment
UHD	Ultra High Definition
URLLC	Ultra-reliable Low-latency Communication
V2E	Vehicle to Everything
V2I	Vehicle to Infrastructure
VIM	Virtualization Infrastructure Manager
VM	Virtual Machine
VNF	Virtual Network Function
VR	Virtual Reality
WAN	Wide Area Networking
WLAN	Wireless Local Area Network

These factors are making MEC the preeminent technology behind 5G deployment.

A. General Background on Security and Privacy

Security is a broader concept that extends to the notions of information security, cyber-security, forensic security, and network security. Information security was defined as the preservation of confidentiality, integrity, and availability (also referred as the CIA triad) of information under the standard ISO/IEC 27002 in 2005 [6]. The information under this definition is applicable to physical or electronic/digital forms of data that are subject to be documented, stored, in transit, or conversed. Forensic security covers acts committed against the laws and statutes in the governing domain. In the IT domain however, digital forensic methods are used for ensuring security. A more nascent definition for cyber-security is presented in [7] as the approaches and actions associated with security management processes followed by organizations and states for protecting CIA of data and assets in cyber-space—though latest requirements of cyber-security are going beyond CIA aspects. Factors such as traceability, authentication, authorization, anonymization, granularity, localization, and trust are novel requirements for systems where cyber-security is applicable.

Initially, network security was defined as the means to secure the communication networks from possible intrusions and vulnerabilities. Those attacks and threats were limited to the intervening and masquerading attacks such as Man-in-the-Middle (MitM), Relay, and spoofing. With adequate levels of encryption and cryptography primitives, probable attacks were plausibly mitigated. However, novel communication services are prioritizing the data rate of the network to serve more subscribers. Thus, cumbersome cryptographic primitives are imprudent. Moreover, softwarized approaches of Software Defined Networking (SDN), Network Function Virtualization (NFV), and Network Slicing demand more requirements for security assurance as presented in [8]. Most of the emerging systems are Cyber-Physical Systems (CPS) that integrate computation, networking, and physical processes to create an environment extending to cyber and physical spaces. Thus, security for a CPS represents an extensive domain for cyber, information, forensic, and network security contexts.

Privacy is an individual's right to act or behave independent of any records or surveillance activity conducted without their consent. In the digital context, personal data cannot be mishandled by service providers without their consent, and measures should be taken to keep safe a user's identity, while the user actions should be untraceable. Irresponsible entities possessing personal data of their consumers, might opt to outsource them to an external institution for deriving personal intents, behaviours, or interests to expand their commercial market. Furthermore, adversaries are capable of extracting personal credentials from weakly protected system to violate their privacy. These acts are recognized as unlawful practices, and novel legislations are focused on mitigating these occurrences. Advancement of sensory devices appended to both human and non-human entities are increasing the possibility of privacy leakages [9].

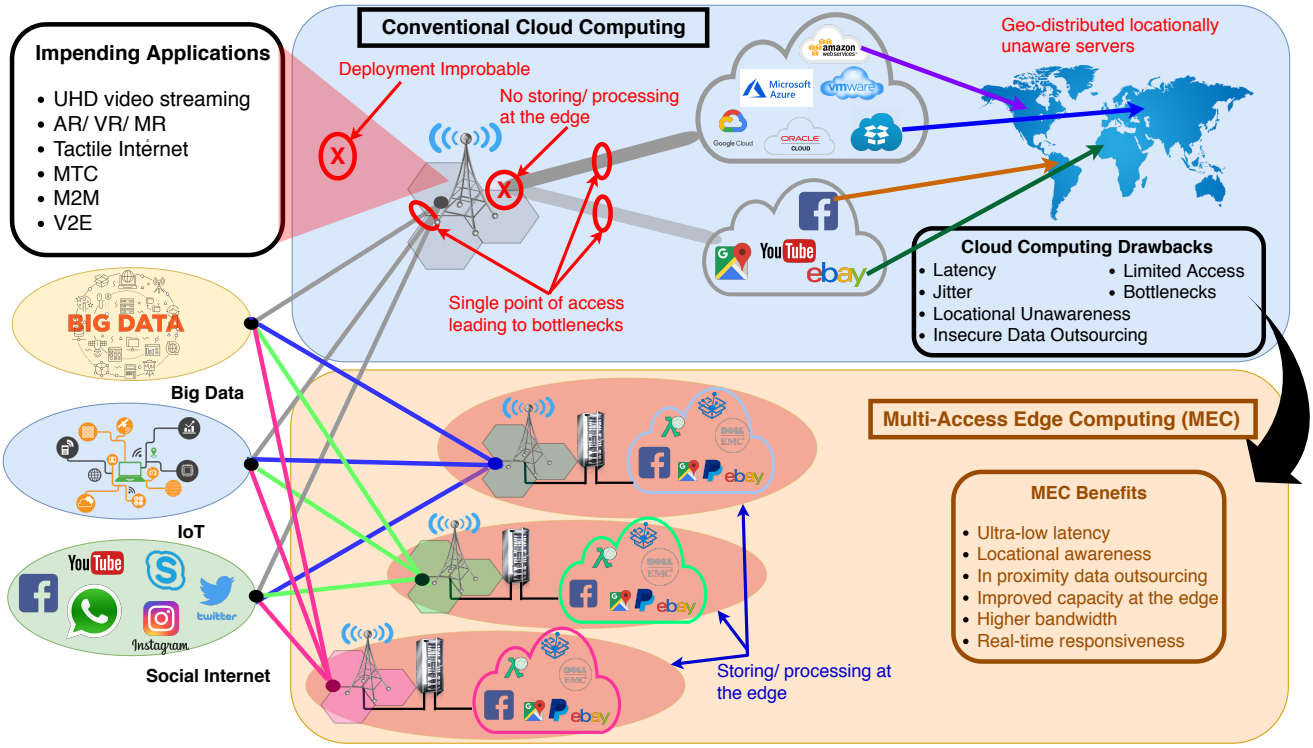

Fig. 1: MEC Paradigm and its requirement.

B. Importance of MEC Security and Privacy

The edge of the mobile network is the access point to all the services emanated in the RAN. This critical juncture is one of the weakest points in the entire network in terms of security. The majority of Internet of Things (IoT) devices in the market are produced with economically manufactured circuitry that employs weak encryption/encoding schemes and other security measures for maintaining an affordable price range in order to compete. Most such devices are vulnerable to cloning and physical tampering, imperilling the entire mobile network for countless attacks. Verifying the credibility of these devices at the edge is a major concern. In addition, the distributed nature of the MEC paradigm is broadening the avenues for adversaries, due to the migration of storage and processing service infrastructure to a proximate radio access range. Even a service impeding attempt intimidates the purpose of MEC, for attaining ultra-low latency to provision real-time 5G based services.

Impending applications and services are demanding the handling of personal credentials/information at the edge of the network for realizing the service requisites. Privacy, integrity, and trust management assurances are prime requirements with MEC deployments, despite the attributed locational and contextual awareness facilitated for the users. It is evident that virtualization technologies are vital for realizing the MEC paradigm and for creating a serviceable platform with dynamic resource allocation capability. Security of the virtualized platforms are still a gray area, due to lesser deployments. The vulnerabilities and attacks plausible on Virtual Machines (VMs) are unique and cause significant consequences to the MEC system.

Similar to CC, outsourcing MEC subscriber data to a remote storage and processing environment creates a predicament in terms of privacy rights. Establishing boundaries regarding the extent of authorized conduct on service providers capabilities is imperative for guaranteeing the trust of MEC consumers. Considering all these facts, security and privacy are important for realizing a pragmatic MEC paradigm deployment.

C. Classification of MEC Security

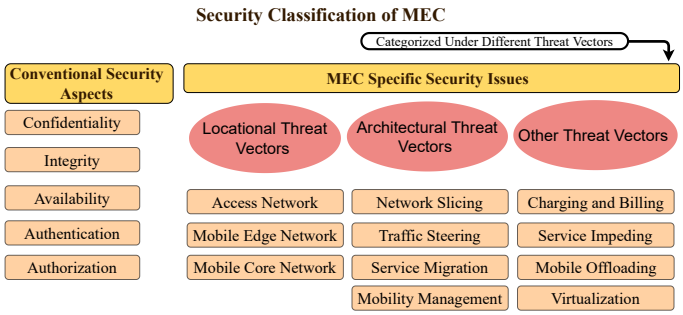

Fig. 2: Classification of MEC security.

Since security is a vast concept, a proper classification is required to simplify the various aspects that apply to the MEC context. In this paper, security is mainly classified under conventional security aspects and MEC specific security issues as depicted in the Fig. 2. Under conventional or classical security aspects (in Section III), the Confidentiality, Integrity, Availability, Authentication, and Authorization aspects are considered. The MEC specific security issues specified in Section IV, are derived based on their threat applicability. Threat

Vectors (TVs) are formed to identify the vulnerabilities/flows associated with MEC deployments. These TVs are further categorized into locational, architectural, and other aspects for better clarity.

D. Paper Motivation

MEC is a paradigm that depends entirely on mobile network deployment. Due to this dependency, integrating upcoming 5G technology to MEC should be approached with caution. Thus, materials available for the MEC paradigm are limited and more generic in terms of certain aspects. Security is one such aspect that has not been addressed by existing research, specifically in relation to standardization, due to the heterogeneous deployment scenarios applicable in the radio access network. Therefore, the prime motivation of this paper is to identify the threat vectors of the MEC system in accordance to the ETSI standards and to investigate the integration technologies for proposing solutions for the security issues.

In Table II, a summary of the existing surveys on MEC are presented, emphasizing their contribution and significance to security. The content is categorized as interdisciplinary, offloading, service migration, communication, MEC based IoT and security aspects. Moreover, the content indicates the time frame of the referred literature to understand the novelty of the presented facts. In [3], different orchestrator deployments are investigated for successful MEC integration. Further, the table shows the key enabling technologies and use cases for MEC. The MEC service orchestration directives presented with container and VM aspects are vital for realizing a functioning edge platform. Different aspects of MEC are addressed in the surveys in [5], [11], [13] and [14] that cover emerging MEC based applications, research directions, research challenges, latency requirements and game theory adaptable MEC use cases. Security and privacy issues on MEC levels are addressed in [5], that proposes already existing security mechanisms for those issues.

The comprehensive investigation in [10] is related to fog

TABLE II: Summary of important surveys on MEC

Aspect	Ref.	Referred Time Frame	Main contribution	Relevance to MEC Security
Interdisciplinary	[3]	1996-2017	A survey on MEC orchestration deployments that address MEC fundamental enablers and standardization	Minor and generic consideration on security and privacy
	[5]	2001-2017	Presents a comprehensive overview of MEC with emerging applications and novel research directions	Security and privacy issues on network, core network, MEC server, virtualization, and end devices are discussed
	[10]	1994-2018	Conducted a comprehensive survey on fog computing and its relation to other paradigms	No emphasis on MEC security despite the fog security considerations presented
	[11]	2013-2016	Discuss the applications, technological opportunities, and research challenges of MEC	A mere discussion on the effect of security on transmission delay is presented
	[12]	2009-2017	Facts about MEC, fog, and cloudlets are concisely presented comparatively	MEC security is not significantly addressed
	[13]	1976-2018	Latency requirements on 5G technologies focusing on RAN, core network, and caching	MEC security is not addressed
	[14]	1986-2018	Discusses the game theory deployments on MEC use cases	Security in Game Theory adaptations are emphasized. No clear context related to MEC
	[15]	2001-2017	An overview of MEC architecture, standards, and applications	Security is not addressed
Offloading	[16]	1997-2017	A comprehensive study on computation offloading use cases of MEC is conducted	MEC security in not addressed
	[17]	1999-2018	A survey on MEC service adoption and provisioning is presented with different offloading schemes	No relation to the MEC deployments
	[9]	2003-2019	A survey on orchestration of cloud and end connectivity through edge comparing MEC, TC, fog, and cloudlets	Security and Privacy factors on system-level and service-level are discussed. Not specific to MEC
Service Migration	[18]	1994-2018	A comprehensive survey on service migration approaches in MEC is conducted	Blockchain is proposed as a solution for security in the service migration processes
	[19]	1987-2017	A survey on VM migration approaches is conducted identifying migration optimization techniques for MEC	Minor consideration on security for VM migration
Communication	[20]	1974-2017	A comprehensive survey on radio and computational resource management in MEC	A section on security and privacy issues in MEC focused on trust, authentication, and network security
	[21]	2013-2018	mobile VR application based MEC deployments are studied	MEC security is not addressed
	[22]	1994-2017	A detailed survey of issues on computing, caching and communication techniques in MEC	Addressed security issues in edge computing. Not specific to MEC security
IoT Integration	[1]	2009-2018	A survey on realizing the potential of MEC for IoT deployments with various use case considerations	Security in potential MEC enabled IoT systems are discussed. No relation to MEC architecture
	[23]	2015-2016	MEC based IoT use cases of V2I, data analytics, computational offloading and surveillance are discussed	MEC security is not addressed
	[24]	1992-2018	A survey on the performance affects of IoT based edge computing deployments. MEC considered as a use case	Security and privacy issues edge computing and IoT are discussed. No relation to MEC Security
Security	[25]	2006-2016	A comparison of edge paradigms are presented forming threat models for proposing security solutions	Security is discussed generic to all edge paradigms focused on UE, network and service infrastructure. Not specific to MEC

computing though it has contrasted its own insights in relation to MEC, Mobile Cloud Computing (MCC), Cloudlets, and Mist computing. Moreover, a three layer IoT-fog-cloud architecture is proposed. [12] followed a similar approach but compared MEC, fog, and cloudlets from the RAN perspective. As mentioned above, latency is a critical parameter for 5G technologies. Thus, [13] studies latency requirements for diverse 5G use cases, including factory automation, Intelligent Transport Systems (ITSs), smart grids, VR, health care, robotics, and education. In addition, MEC is identified as a manifested core network deployment for 5G. Game Theory (GT) plays a key role in recognizing subscriber goals and intentions that conflict with each other. These intentions are vital for designing and optimizing networking and communication scenarios in emerging systems. Thus, [14] applies GT adaptations of classical and evolutionary gaming strategies for MEC use cases. [15] presents an overview of MEC with a concise standardization and application scenarios that include intelligent video acceleration, video stream analysis, AR, connected vehicles, and IoT. In addition, architectures, resource management, application partitioning and performance aspects of MEC were studied to finalize the survey.

The computational offloading capabilities of MEC adaptations are studied in [16], [17], and [9] in terms of orchestration, service, and resource provisioning. Allocation of computational resources, architectural considerations, and mobility management during offloading processes are discussed in [16]. [17] contrasted the prevailing offloading schemes in terms of computation, data, and single and multi-mobile users. Additionally, an Intrusion Detection System (IDS) that employs machine learning methods for detecting anomalies was proposed. [9] studies on end-edge-cloud orchestration mechanisms on transparent computing, MEC, fog, and cloudlets. In addition, computation offloading, caching, security and privacy, and future research directions are presented. Service migration approaches applicable to MEC are investigated in [18] and [19]. Mainly, live migration of data centres and handover mechanism in cellular networks are discussed in [18], while VMs, containers, and agents are summarized as hosting technologies to enable service migration. [19] classifies existing VM migration schemes into manner, distance, and granularity perspectives. Further, live migration approaches are investigated focusing on memory data migration, storage data migration, and network connection continuity objectives.

The communication aspects of MEC are researched in [20], [21], and [22]. Systems with cache enabled MEC, green MEC, and MEC mobility management are discussed in [20]. Moreover, trust and authentication management, networking security, and secure private computations are emphasized for revealing vulnerabilities in MEC systems. A MEC based mobile VR deployments are studied in [21] for proposing a optimized resource consumption method that constrains communication functions. [22] explores the issues on caching and computing aspects of MEC communication techniques, while presenting use cases and enabling technologies. Some papers [1], [23], and [24] discuss the potential for employing MEC for IoT deployments and present various MEC-enabled IoT use cases and their performance effects.

Roman et al. in [25] conducted a comprehensive survey on security aspects of edge computing paradigms, identifying their threat models. The papers [10], [11], [12], [13], [14], [16], [17], [21], [22], and [23] did not address security as a key aspect of MEC. Certain surveys, such as [1], [25], [20], [9], and [5] focus heavily on security and privacy although the context is not concurring to the ETSI standardized MEC architecture and its components. Additionally, prevailing literature does not consider the privacy aspect of MEC based deployments that extend to identifying related issues nor goals to preserve the subscriber trust. To the best of our knowledge, there is not a single study that investigates the security and privacy aspects of MEC in accordance to the ETSI standards.

E. Paper Contribution

The main contributing factors of this paper are listed below:

- Identify classical and specific security aspects of MEC;
- Define TVs in the ETSI standardized MEC architecture;
- Conduct a comprehensive survey on the identified TVs in a MEC deployment scenario;
- Reveal vulnerabilities, summarize attack vectors, and propose state-of-the-art solutions for the identified TVs;
- Discuss the privacy aspect of MEC deployments and the adaptability of MEC for enhancing privacy in 5G networks;
- Discuss the assimilated facts gathered during the research process and emphasize future research directions.

Moreover, the authors' previous survey paper [1] focused on MEC-IoT integration. It contains a brief security and privacy analysis section, focusing only on MEC-IoT integration. This current paper covers a broader scope than the previous paper; however, the sole focus is directed to security and privacy aspects of MEC.

F. Paper Organization

The rest of the paper is categorized into six sections. Section II presents the background knowledge on MEC for realizing the concept in the ETSI standardized context, while comparing its features with other edge computing paradigms. The core contribution of this survey is presented as a taxonomy for MEC security in Section III and Section IV. In Section III, the conventional security aspects of MEC are presented. Section IV introduces the TVs specific to MEC systems based on a deployment scenario illustrated in Fig. 4. These threat vectors enable us to identify probable attack vectors. The privacy aspects of MEC deployments are analyzed in Section V. This analysis reveals MEC privacy issues in establishing objectives to preserve privacy. Moreover, state-of-the-art privacy preserving solutions are summarized in relation to these privacy objectives. The insights gained from the overall survey are further discussed in Section VI; while research problems, preliminary solutions, and future research directives are presented for the MEC research community. Finally, we draw conclusions in Section VII. Relevant acronyms presented in the survey are tabulated in Table I.

TABLE III: Comparison of edge computing paradigms.

Factor / Technology	Multi-Access Edge Computing (MEC)	Mobile Cloud Computing (MCC)	Fog Computing	Cloudlets
Introduced by	ETSI (2014) [26]	Aepona (2010) [1]	Cisco (2012) [27]	Satyanarayanan et al. (2009) [28]
Standardized by	ETSI, 3GPP, ITU-T [10]	NIST [10]	OpenFog Consortium, IEEE [10]	OpenEdge [10]
Purpose	Extending cloud computing capabilities to the edge network [1]			
Infrastructure Ownership	Telecom MNOs [1]	Private Institutions and Individuals [1]		Private Institutions [25]
Node Deployment	At the Radio Network Controller (RNC) or BS [1]	Network edge [25]	Strategic location between cloud stratum and device stratum [1]	Network core [25]
Software architecture	MEO based [1]	Service Oriented [1]	Fog abstraction layer based [1]	Cloudlet agent based [1]
Virtualization	VMs or other virtualization techniques [27]	Only VMs [29]	Other virtualization technologies [27]	Only VMs [27]
Operation Mode	Standalone or Cloud Connected [27]	Cannot work Standalone [29]	Cannot work Standalone [27]	Only Standalone [27]
UE Access	Closest RNC or Access Point [1]	Internet [1]	Closest RNC or Access Point [1]	Closest Access Point [1]
Latency and Jitter	Very Low [1] [10]	Relatively High [3] [10]	Very Low [27] [10]	Very Low [25] [10]
IoT Compatibility/ Adaptability	High [2]	Low [3]	High [27]	High [1]
Storage Capacity at the edge	High [2]	High [1]	Depends on the deployment [30]	
Computation power at the edge	High [2]	High [1]	Depends on the deployment [30]	
Power Consumption	High [10]	Low [10]	Low [10]	Moderate [10]
Availability	High [25]			
Scalability	High [25]			Low [25]
Mobility	High [25]	High [25]	High [25]	Low [25]
Context Awareness	High [1]	High [1]	Medium [1]	Low [1]
Local Awareness	High [25]			
Security	High	Medium	High	Medium
Integrating Technologies				
NFV	✓ [31]	✓ [32] [33]	✓ [34]	✓ [35]
SDN	✓ [31]	✓ [32]	✓ [36]	✓ [37]
Network Slicing	✓ [31]		✓ [38]	
ICN	✓ [31], [39]	✓ [33]	✓ [40]	✓ [41]

II. Multi-Access Edge Computing (MEC)

This section presents detailed knowledge on edge computing paradigms and compares them with the features of MEC. Further, it discusses the evolution of MEC, MEC standardization, and MEC reference architecture. These facts are essential to understanding the conventional security aspects in Section III and threat vectors defined under Section IV.

A. Edge Computing Paradigms

The formation of edge computing paradigms began in the 1990s when Akamai technologies launched a Content Delivery Network (CDN) as an approach to disperse the data centre functionalities infracting against the centralized system [42]. Mobile Cloud Computing (MCC), fog computing, and cloudlets are other edge paradigms recognized in the scientific research community apart from MEC [1]. The motivation behind edge computing technologies is to extend the constricted CC functionalities and reinforce the service access infrastructure. Thus, some attributes of these paradigms resemble each other, apart from subtle differences. Divergence in the architecture, however, limits the deployment options for certain applications and technologies.

The main concept of MCC is to augment the computing capabilities of mobile devices for extending battery life and storage capacity, while offering adaptability, scalability, mobility, availability, and self-awareness in mobile computing environments [29]. Later, the intention was revised to execute mobile devices at the edge as an alternative to the centralized architecture [25]. The approach offloads the mobile process as a clone or a partial migration of the mobile agent to be executed at the edge entity, leaving the cloud infrastructure intact. The program portioning and the thread migration scenarios of the mobile device cloning process engaging various elasticity patterns as presented by Khan et al. in [43] are the prime examples of the deployment models in MCC. In spite of facilitation on deploying m-learning, m-gaming, m-healthcare, AR, and crowd-sourcing applications, public clouds fails to fulfill the latency requirements of the centralized cloud architecture that affect the end user Quality of Experience (QoE) [3]. Thus, employing MCC for real-time applications catered by 5G technology is improbable.

Fog computing was introduced by the Cisco systems in 2012, envisioning an infrastructure formed by a collaborative cloud network that facilitates services performed by geographically dispersed edge nodes equipped with similar but limited resources comprising the main cloud. OpenFog Consortium, an association that promotes fog computing, defines fog computing as “a system-level horizontal architecture that distributes resources and services of computing, storage,

control and networking anywhere along the continuum from cloud to Things" [27]. In this concept, cloud services are deployed at the edge of the network with the Internet Protocol (IP) or Multi-protocol Label Switching (MPLS) backbones in close proximity to the IoT devices. Even though the initial understanding was to make fog computing a mere extension of cloud computing, later research has defined it to be a paradigm of its own, which would be a platform to orchestrate the deployment of heterogeneous IoT applications. Fog computing forms a three-tier architecture within the strata: cloud, fog, and end user stratums [30]. Fog nodes that are formed on the virtualized technology and operate in the fog stratum link the end devices to the cloud data centre while maintaining the fog-to-fog connections that expand the fog network. The flexibility of fog node deployment enables the application of Brain Computer Interfaces (BCI) using wireless electroencephalogram (EEG) headsets, AR, real-time video analytics, cyber-physical systems, and V2E [25]. The fog nodes, which attribute comprehensive resources and functions, form a holistic and dispersed service infrastructure that realizes 5G use cases.

The cloudlet concept was first proposed by Satyanarayanan et al. in 2009 as a small cloud infrastructure located near mobile users, which could be used at small businesses or industries [28]. They are also referred as Micro Data Centers (MDCs), proposed by Microsoft Research in 2015 as an extension of traditional data centers used in cloud computing [10]. The cloudlet architecture resembles the fog computing three-tier model, where the end devices, cloudlet-based edge cloud platform, and centralized data centre form the system structure [3]. Cloudlets are deployed as VMs that facilitate a transient environment for users in a local vicinity. Offloading and caching tasks are probable with the small scale cloudlets, where face recognition and video streaming applications are ideal deployments that emulate the scaled virtual environment [30]. In addition, approaches such as Hyrax, FemtoClouds, Superfluid clouds, Edge-Centric computing, Mist computing, Cloud of Things (CoT) and Edge Cloud (EC) are alternative edge technologies proposed for various deployments that operate at diverse scales [25] [10]. Table III summarizes the comparative factors of the discussed edge paradigms.

B. Evolution of MEC

The scope of possibilities has been expanded with the advent of Integrated Circuits (ICs) as a paradigm shift that produced the third generation of Personal Computers (PCs) in the 1980s, which revolutionized industries from mechanical processing to electronic-based processing systems. After almost four decades, 5 nm silicon chips are produced to miniaturize computers into smart devices that produce a higher processing power than that of early PCs. Hence, means of computational processing capabilities, which were once deployed by cumbersome PCs, have been drastically reduced to handheld devices at present, and possibly way diminutive in the future. Thus, management of data storage, networking resources, battery lifetime, computational power, and memory limitations in handheld devices is disconcerting to Mobile Network Operators (MNOs) [3]. The data storage and processing services have evolved from mainframes (BITNET-1981) to dedicated servers and cloud computing, while networking services advanced from Advance Research Project Agency Network (ARPANET-1961) to Internet (1969), to Ethernet, to SATNET, to IPv4 based TCP/IP, to IPv6, to 802.11 Wi-Fi, to 802.11a, to 802.11g, and to 802.11n. Moreover, mobile networks evolved from 1G, to 2G - Global System for Mobile Communication (GSM), to 3G, to 3.5G – High Speed Packet Access, to 4G and to 4G Long Term Evolution (LTE).

The emergence of the IoT paradigm envisioning the anytime, anywhere connectivity for myriad versatile and comparatively miniaturized smart devices was first mentioned by Kevin Ashton in 1999 at MIT while Chana Schoenberger and Bruce Upbin published the paper titled 'The Internet of Things' in Forbes' 2002 issue, documenting the concept for the first time. However, the drawbacks and limitations in cloud computing that are exacerbated by the 3.9 billion current internet users present a significant scarcity for capacity in the MNO perspective. Even though the capacity of the core network and cloud infrastructure is upgraded, the existing mobile network limits the accessibility of increasing the number of IoT devices and launching impending applications. Thus, the novel approach of MEC is proposed as a paradigm shift to the processing and storage solutions that are amalgamated with the 5G mobile technology. The networking infrastructure for IoT, integrated with the MEC and other edge computing paradigms, are envisioned by Tactile Internet which guarantees ultra-low latency, extreme availability, reliability, and security provisioned from 5G and beyond 5G technologies [1].

C. MEC Standardization

The IBM and Nokia Siemens network introduced MEC in 2013 as a platform that could execute applications within a mobile base station, where the aspects of application migration and interoperability were not considered [25]. Later in 2014, the European Telecommunications Standards Institute (ETSI) launched the Industry Specification Group (ISG) for standardizing Mobile Edge Computing, which describes the operation of MEC as such: "Mobile edge computing provides an IT service environment and cloud computing capabilities at the edge of the mobile network, within the RAN and in close proximity to mobile subscribers" [26].

Pioneers in mobile network solution providers, such as Nokia Networks, Intel, Vodafone, IBM, Huawei, and NTT DOCOMO, were leading the ISG representation, while European 5G Infrastructure Public Private Partnership (5G-PPP) acknowledged MEC as a prime emerging technology for 5G networks [5]. The goal of ETSI MEC ISG was to facilitate an open environment for multiple vendors, providing diverse applications and services at the edge of RAN merely to overcome the limitations of existing centralized cloud computing deployments [3]. A Proof of Concept (PoC) framework for MEC was published by ETSI ISG in 2015 to highlight the rationale, roles, responsibilities, and the activity processes of the PoC framework. In the same year, another white paper was released for evaluating the business value of MEC service

scenarios such as AR, intelligent video acceleration, connected cars, and IoT gateways to identify the market drives. The MEC framework and reference architecture was published in 2016 by ISG for formulating the entities in the MEC system and to define their intended function [44]. The potential of the MEC paradigm is reaching beyond mobile networks to Wi-Fi and fixed access technologies. ETSI ISG has renamed the concept "Multi-Access Edge Computing" which conveniently justifies the acronym MEC [1]. Additionally, a 2018 ISG release accentuates the deployment scenarios and use case exemplifications of MEC with 5G integration [45]. This white paper investigates the deployment of MEC and 5G components in actual use cases with traffic steering, mobility, offloading, charging, and regulatory requirement considerations. An extension of the same directive was presented in [46] as the 2nd specification release that expands the scope of MEC use cases for camera as a service (also known as video surveillance as a service), video delivery, future factories, multi-radio access technology (multi-RAT), Internet Protocol television (IPTV), in-vehicle systems, and 5G use cases. In the latest release from ETSI in 2019 January, a variant architecture was proposed for combining Network Function Virtualization (NFV) and MEC, while in-depth focus was directed towards components in the architecture, in contrast to the previous release in [44].

D. MEC Reference Architecture

The MEC Reference architecture illustrated in Fig. 3 is the ETSI-published MEC framework and the reference architecture depicted in [44]. MEC architecture has two main levels: Mobile Edge System Level and Mobile Edge Host Level [47].

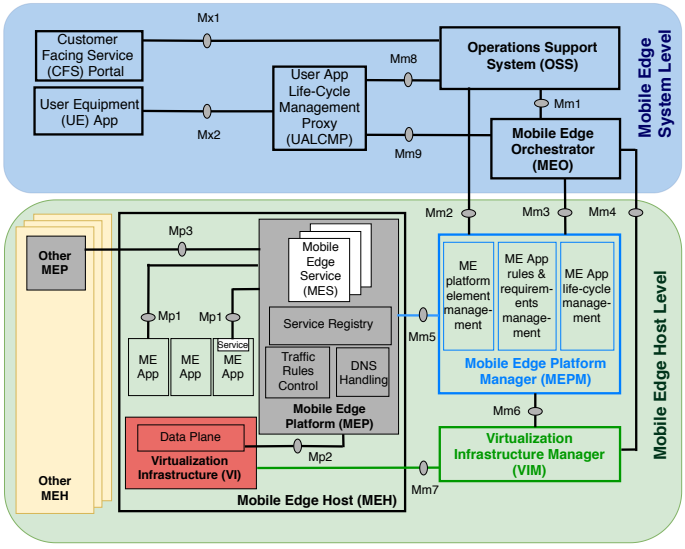

Fig. 3: MEC reference architecture.

1) Mobile Edge System Level

User Equipment (UE) is the devices that connect to the MEC edge through the access network. They could be either handheld mobile devices or automated devices that are operating without human supervision. UE Applications (UE Apps) are the programs intended to be subscribed by MEC services and executed in a single or several UE domains. The connectivity of UE Apps to the MEC host level, however, is commandeered by the User Application Life-Cycle Management Proxy (UALCMP). UALCMP handles the initial UE App requests for subscriptions. Though UALCMP is located at the mobile edge system level, subscription requests conveyed through the access network are forwarded to it from the edge network. A similar function is performed by the Customer Facing Service (CFS) Portal for third-party customers of the MEC service provider or the mobile operator for facilitating the MEC services. Operation Support System (OSS) is the entity that handles the user access authorization and subscription elapsing duration distinguishing the service types forwarded from UALCMP and CFS portal. Additionally, connections are maintained with the mobile edge platform manager and the mobile edge orchestrator for virtual resource allocation to subscribed UE Apps and provisioning service logs, respectively. The Mobile Edge Orchestrator (MEO) is the principal entity at a mobile edge system level that governs single or several mobile edge host levels. The MEO is linked to the OSS and UALCMP entities operating at the MEC system level, while connections are extended to the mobile edge platform manager and virtualization infrastructure manager in the MEC host level. The holistic management of operating MEC hosts, catered services with resource utilization and employability of the standardized topologies, are administered by the MEO.

2) Mobile Edge Host Level

Mobile Edge Platform Manager (MEPM) acts as the orchestrator for the mobile edge host level. MEPM manages the rules, requirements, and life-cycle of mobile edge applications by handling the storing, configuring, and running functions of software images in the host virtual environments. Virtualization Infrastructure Manager (VIM) governs the virtualized resources in every mobile edge host launched at the mobile edge host level. It is connected to the virtualization infrastructure of each mobile edge host, while the status of the virtual resources is updated to the MEO and MEPM. Mobile Edge Host (MEH) is the executing entity of MEC services, where all other entities are designed to mandate various monitoring and approving functions that ensure seamless operation of the holistic MEC system. A MEH contains MEC applications, a mobile edge platform, and a virtualization infrastructure. Mobile Edge Applications (ME Apps) are software-based processes that operate as Virtual Machines (VMs) on top of the virtualization infrastructure. The nature of the ME App in terms of its VM configuration (storage, processor and networking) and connectivity (to other ME Apps, to ME Apps in other MEHs or to another mobile edge host level) is reliant on the scope of the subscribing UE App and intended MEC service. ME App connectivity is established from a Local Area Data Network (LADN) that extends within a single MEH [45]. The Mobile Edge Platform (MEP) dispenses the provisions to launch the ME Apps while creating an environment to discover, advertise and consume mobile edge services. The MEPM-condoned traffic rules are notified to the LADN at the MEH by the traffic rules controller, where DNS and proxy functions are administered based on the MEPM records. Virtualization Infrastructure (VI) is the platform on which the

ME App VMs are functioning. The VI comprising the LADN is commandeered by the VIM and MEP for managing virtual resources and enforcing traffic rules, respectively. In relation to the MEC system, a Mobile Edge Service (MES) is defined as a service originated or facilitated by either the MEP or ME Apps. All the provisioned services are registered under the MEP through the Mp1 interface, where the ME App is subscribing to the relevant authorized services. More details regarding the interfaces in Fig. 3 are explicated in [44].

III. Conventional Security Aspects in MEC

This section states the classical security aspects of MEC deployments. These aspects can be conceptualized as requirements to improve the feasibility of launching MEC.

A. Confidentiality

Confidentiality is the act of preventing unauthorized entities from reading or accessing sensitive materials [48]. This aspect of security obscures information by encrypting the payload with a considerable level of cryptography. At the design stages, obscuring information that ingresses, egresses, and traverses within the MEC system is a critical requirement. This will prevent the disclosure of information by intervening and eavesdropping attacks. Mobile networks evolving from GSM to LTE employ encryption algorithms ranging from A5/2 to Evolved Packet System (EPS) Encryption Algorithm (EEA) [49]. Moreover, security specifications published under TS 23.122 and TS 33.210 guarantee the security measures available at Access Stratum (AS) and Non-Access Stratum (NAS) levels of 3GPP architecture [50]. The insights gained from the prevailing network models enhance the security of mobile protocols in regard to confidentiality.

1) Possible Confidentiality Violations in MEC:

For 5G and beyond-5G based RAN however, communication protocols should be customized in accordance to the deploying use cases and applications. The information traversing within the edge infrastructure and towards the core network should be encrypted with a considerable level of security. Unwarranted information disclosure at this level imposes more damage to MEC system than the mobile AN via exposed system states and cryptographic primitives. Non-3GPP based IoT devices face the same threat levels as mobile UEs. However, their threat domain exceeds a typical UE device due to their resource scarcity and inability to launch adequate security measures.

2) Mitigating Confidentiality Violations:

Both signalling and controlling information related to the mobile network and virtualization platform are conveyed through the link between edge and core level as described under TV E5. For such links established between edge infrastructures; tunneling, IPSec, or TLS/ SSL based encryption schemes are viable adaptations for guaranteeing End-to-End (E2E) security [5]. Slice isolation is a way of ensuring confidentiality of UEs sharing the same infrastructure, accessed through the RAN [51]. For Non-3GPP devices employed in Zigbee, Bluetooth, Wi-Fi, and LPWAN technologies, mechanisms such as light-weight security protocols, ECC, and PHY schemes are emerging methods for improving security [52].

In addition, Quantum Resistance (QR) or anti-quantum cryptographic methods are being researched to limiting the vantage of adversaries with ample resources [53]. Lattice-based, multivariate, hash-based, and elliptic curve schemes are employed for formulating QR algorithms in order to overcome exhaustive key searching or brute-force attacks commandeered by quantum computers [54]. These methods guarantee integrity in addition to confidentiality.

B. Integrity

Manipulation and destruction of data to mislead the parties engaged in communication are integrity violations. Similar to confidentiality, integrity is a widely addressed concept for mobile networks. The virtualized MEC edge platform relies on control information conveyed through feedback channels to optimize the operations of virtual entities. Therefore, integrity plays a key role in the MEC context as these services are automated, and autonomous services require accurate information to operate effectively.

1) Possible Integrity Violations:

In mobile networks, integrity is violated through intervening attacks such as MitM or Relay attempts perpetrated to manipulate or misuse the inwardly and outwardly conveyed content to and from the core network. In MEC, additional channels are being exposed to the adversary in contrast to a typical mobile network. The links established between the MEC edge level, MEC system level, and the mobile/5G core network adds more threat vectors for violating integrity. The injection of malicious codes into a legitimate information flow can cause the most devastation to the edge platform [55]. Reliance on the softwarized core and edge platform entities for autonomous operation risk compromise the entire system through such a malicious fragment. All operations conducted by an illegitimate node, or a device inserted into the network, either in the access network or within the edge platform, can be considered integrity violations.

2) Mitigating Integrity Violations:

Through EPS Integrity Algorithm (EIA), integrity protection is offered to AS and NAS stratum levels in LTE [50]. In 5G, 5G-AKA is handling the integrity assurance mechanisms for signalling channels [56]. Moreover, tenant isolation is a prospect that improves integrity protection in a multi-sliced environment [51]. In comparison to LTE, 5G is supporting integrity at the user plane [50]. This feature enables resource constrained IoT nodes for utilizing integrity verification mechanisms available under 5G RAN. For IoT devices, hash-based and session-key based encryption schemes could be employed for ensuring integrity at the PHY level [57].

Typically, edge and core levels are linked with communication channels that use existing protocols. The Encapsulation Security Payload (ESP) attribute of the IPSec is used for the integrity protection of IPSec-based tunnels which are adaptable for egressing channels of MEC edge [58]. In addition to traversing information, integrity of applications or MESs should be validated routinely. An Operation Support System (OSS) is capable of initial integrity verification, while MEO can monitor the integrity in softwarized entities deployed at the edge infrastructure [23].

C. Availability

Availability is the omnipresence of MEC resources for consumers who are willing to subscribe for services. This factor primarily relies on network performance and the effectiveness of the network interfaces. Therefore, performance of the mobile network is paramount for MEC.

1) Possible Availability Violations:

DoS-adjacent attacks that impede services are the main cause for availability disruptions in communication channels. In the existing LTE network model, the Radio Resource Control (RRC) connection status creates issues with validating the eNodeB for the UE [59]. Thus, it creates opportunities for DoS attacks, compromising the availability of eNodeBs. Since the UE requests are directed to the UALCMP initially, its capacity for serving UE should improve significantly to cater to the 5G based applications. Once the service request is granted, UE establishes a direct link with the MEC edge for instigating its service. This channel is formed via the RAN and connects to the MEH via the UPF instance in the LADN. Thus, the N3 interface of the 5G service architecture should feature adequate capacity to handle minimum UE requirements [45]. Failing to integrate these requirements to the novel networking interfaces compromises the network flow and results in inaccessibility. Further, the nature of service denial attacks has evolved drastically over the years, delivering distributed attacks with a multitude of bots. These bot-net type attacks limit the accessibility of legitimate users, compromising their availability.

2) Mitigating Availability Violations:

In the edge infrastructure, the placement policy of virtualized entities plays a key role in maintaining availability parameters. However, MEPM and VIM are static placements. Depending on the service provided by VMs as isolated hosts or VMs deployed within a singular host, each represents different availability and cost factors [60]. As the virtual environment formed by the ME Apps within a MEH can be customized according to the service type, various ME Apps should function distinctly from each other. Therefore, placement of ME Apps within the MEH directly affects the availability factor.

D. Authentication

Authentication is the process of verifying the identity of the parties engaged in communication or resource access. These mechanisms are either performed by a single party or mutually through an extended scenario. Authentication schemes employ various measures of authenticity for validating the entities. Keys are the generic tool employed for authenticating non-human entities. Depending on the domain where the authentication is instigated, the mechanisms are classified as either primary or secondary authentication. The authentication for MEC-based UEs are handled via the air interface of mobile RAN mostly as a primary approach. Thus, heterogeneous IoT devices and services incur diverse authentication requirements. Ensuring the confidentiality of keys and authentication credentials is intrinsic for UEs, core level, and edge level entities. UE protection can be acquired through the enhancement of existing EPS Authentication and Key Agreement (AKA) mechanisms employed by LTE [59]. Further, 5G based AKA and Extensible Authentication Protocol (EAP) AKA are two mandatory authentication schemes proposed under 5GPP phase 1 [50].

1) Possible Authentication Violations:

There are various ways that the authentication phase of a MEC-based service can be compromised. In primary authentication, device cloning and masquerading attacks of spoofing and impersonation are viable and common through the air interface. Further, Evil Twins (ETs) and injection attacks are plausible, in addition to the previously mentioned attacks in Device-to-Device (D2D) scenarios - where a compromised node can be authenticated as a legitimate entity to the MEC system [61]. The autonomous and virtualized edge platform is operating with virtualized entities (MEHs) that require continuous authentication with UEs, MEHs in other edge platforms, or external cloud services. Thus, adversaries can target these authentication sequences to gain access to the system. Moreover, UALCMP and CFSP, as the main authentication handling entities in the MEC system, can be subjected to DoS or DDoS type attacks perpetrated through authentication requests.

2) Mitigating Authentication Violations:

For most IoT devices, non-3GPP based technologies are employed for communication. Wi-Fi is a common technology used by most edge computing circumstances because of its range. Methods such as PUF [62], accelerometer data [63], and visible light (referred as Li-Fi) [64] are explored for improving authentication of Wi-Fi networks. Moreover, novel methods are introduced for securing LPWAN [52], NB-IoT [65], RFID [66], and BLE [67] authentication phases. These technologies are used for D2D or ad-hoc type authentication, which are common for IoT deployments. QR authentication is a directive that would benefit resource-constrained devices due to its cryptographic primitives bearing a lesser overhead [68]. Thus, such schemes are viable for IoT based technologies that interface with the MEC system.

E. Authorization

Authorization is the function of granting access to authenticated entities, classified under diverse capability levels. Depending on the service type the UE is requesting, OSS approves the capability level for the specified ME App at the edge level. In addition, MEPM is responsible for restrictions imposed by the OSS for ME Apps. Thus, MEC already possesses an authorization discipline devised within its architecture. However, a proper authorization framework should be identified from the existing deployments to be compatible with prevailing mobile services.

1) Possible Authorization Violations:

Most authorization violations are instigated as an authentication violation. OSS, as the main authorization handler for assigning virtual resources to the MESs, can be mislead by illicit UEs with granted access. These UEs can get approval to utilize massive amounts the edge platform's resources, leaving them scarce. Privilege escalation is an obvious repercussion

of an authorization violation that applies to malicious UEs and virtual entities operating at the mobile edge [69]. A compromised MEH is capable of overloading the MEC system level entities of OSS and MEO with security and service log manipulations.

2) Mitigating Authorization Violations:

Mechanisms should be implemented for handling security logs while detecting illegitimate log entries to identify malicious entities [69]. A Trusted Platform Manager (TPM) can be employed to detect illicit entities through their performance metrics. Further, 5G AKA EAP standards include preventive mechanisms for access controlling that furnish an authorization framework for the mobile network [70]. Violations into authorization acts can be mitigated through a secure authentication mechanism. The MEPM, acting as the orchestrator for the edge platform, is responsible for commandeering the access control operations securely [71]. Further, Blockchain can be employed for securing the authorization handling framework of the MEC system to minimize violations while maintaining system logs securely [72].

The table IV classifies the identified solutions in Section III for the security requirements.

TABLE IV: Classification of solutions for conventional security aspects

Aspect	Solutions	References
Confidentiality	E2E IPSec or SSL tunneling	[5]
	Slice isolation	[51]
	ECC, PHY based light-weight security protocols	[52]
	QR cryptography	[53]
Integrity	EIA integrity protection for LTE	[50]
	5G AKA for signalling integrity	[56]
	Tenant isolation in multi-slice environment	[51]
	Hash or session key based integrity assurance at PHY layer	[57]
	ESP attributed IPSec tunneling	[58]
Availability	Optimum placement of ME Apps within the MEH	[60]
Authentication	PUF	[62]
	Accelerometer data	[63]
	Li-Fi data	[64]
	LPWAN authentication	[52]
	NB-IoT authentication	[65]
	RFID authentication	[66]
	BLE authentication	[67]
	QR authentication	[68]
Authorization	Detecting fake security logs	[69]
	TPM for log validating	[69]
	5G AKA EAP for access control	[70]
	Blockchain for authorization framework	[72]

IV. MEC-Specific Security Aspects

In this section, we present the Threat Vectors (TVs) that exist in the considered MEC deployment scenario derived in compliance to the ETSI standardized architecture presented in Fig 3. Fig 4 illustrates the locational TVs applied at different levels in the MEC structure. They are categorized into three areas based on their scope of intrusion: access network, mobile edge network, and core network. In addition, TVs that are not locational, are further classified as architectural and other TVs for understanding their applicability.

A. Threat Vectors related to the Access Network

The Access Network (AN) represents the RAN defined by 3rd Generation Partnership Project (3GPP) and the access infrastructure related to non-3GPP networks, such as Wireless Local Area Network (WLAN), Worldwide Interoperability for Microwave Access (Wi-Max:IEEE 802.16), or Code Division Multiple Access (CDMA) 2000 networks [73]. In any communication system, threats mostly originate in the access network. The prime rationales for those threats are the diverse technologies deployed in the AN scope. The scalability of the proposed TVs based on AN is a great concern for applicability, due to the heterogeneous nature of the MEC-enabled services. We classified the TVs related to AN into three generic categories, described in the following subsections: A1, A2, and A3.

*1) **A1: Link between the User Equipment and a Base Station***

The connection from UE to the BS is the most typical communication link that exists and the most vulnerable to threats in a mobile communication system. Since A1 applies to the most exposed part of the mobile communication network, an adversary could either intervene or introduce a malicious device to compromise the BS. Mobile delegation is concerned with offloading computationally intensive tasks to the edge servers due to resource constraints of the UEs. The bulk storage and information traversing intended for processing in an offloading scenario are elevating the network traffic carried through the air interface [25]. Additionally, novel technologies such as massive Multiple-Input-Multiple-Output (MIMO), interference-aware receivers, advanced coding/modulations, millimeter Wave (mmWave), carrier aggregation, Wi-Fi offloading, LTE and License Shared Access (LSA) have been introduced in order to improve the spectral efficiency in the access network [74]. The connectivity of the UE through these heterogeneous technologies raises concerns over compatibility and interoperability factors that could be exploitable by adversaries.

Vulnerabilities: The wireless, broadcast nature of the air interface that links the UE to the BS is prone to attacks, such as:

- *Eavesdropping and hijacking:* Instigated as MitM, Relay, Advanced Persistent Threat (APT), Sybil, and Spoofing attempts [75], wireless communication channels are being hijacked to retrieve information transmitted in this way. The MitM attacks are plausible between the 3G network and the non-3GPP WLAN networks that compromise the internal virtualization infrastructure entities of the edge level [1]. The lesser level of encryption and integrity in low-resource IoT devices poses higher risks of compromising these channels that connect to the MEC edge system [76]. These attacks would gain the access to the ME Apps operating in MEHs and manipulate the virtualization infrastructure of the MEH to exhaust its resources while infecting other MEHs connected to the infiltrated one. Thus, a privileged escalation attempt could be launched via these attacks.

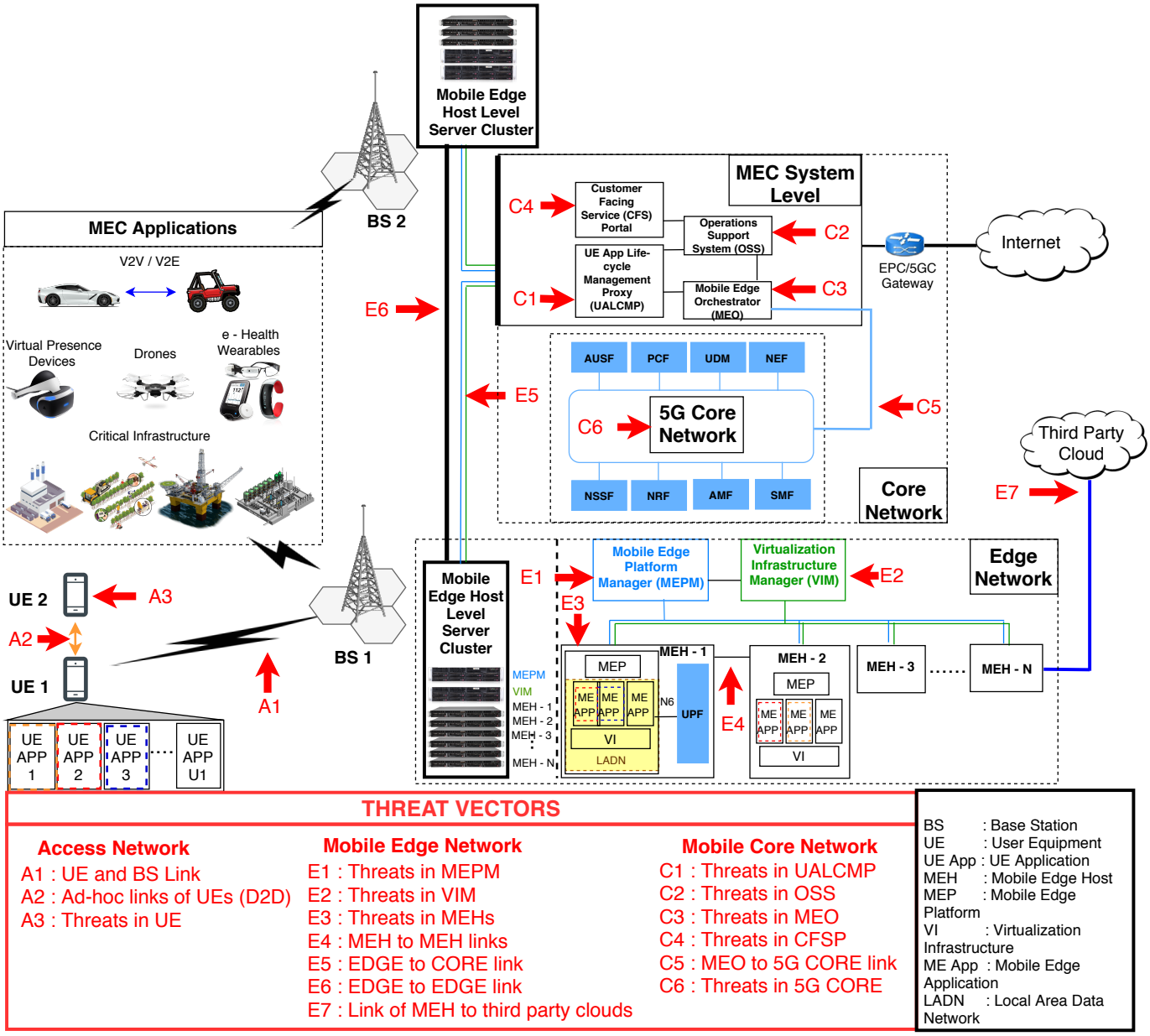

Fig. 4: Locational threat vectors of a typical MEC deployment.

- *Jamming and Denial of Service (DoS):* The purpose of jamming the wireless channels and disrupting a service via DoS attacks is to violate the availability aspect of the RAN connected to the MEC edge system. These attacks pose a higher destructiveness towards novel systems due to the delay they cause for latency-tolerant applications. Thus, with a compromised MEH, services to the consumers can be blocked or the MEC system-level entities can be disrupted through unnecessary queries to impede the service of the entire infrastructure. Novel botnet-type DDoS attacks are capable of challenging the access capacity of UALCMP and CFSP entities in the MEC system level.
- *Malicious node injection:* The diversity of the UEs connecting to the BSs would present an issue of managing the compatibility among mobile devices produced by different vendors and the communication protocols of varied UEs or UE Apps. In such circumstances, malicious nodes could be injected to the system, exploiting the vulnerabilities in the UE devices: these include susceptibility to device cloning, less secure wireless protocols (WPA/WPA2), proneness for hardware Trojans, predictable access control credentials (PIN/ pattern), or alleviated resiliency against malicious software agents disguised as partial entities of UE Apps such as spyware, adware, Trojans and malware. Such vulnerabilities could feed malicious content or counterfeited information to the ME Apps through the BSs, which would manipulate the services offered by the MEH, as mentioned in TV E3. However, these attacks could be mitigated by employing

an effective authentication mechanism embedded with a trust verification scheme for the UE and BS connectivity.

Existing Solutions: The security of the air interface ensuring CIA factors can be categorized in the following ways: the use of cryptographic primitives and their effectiveness, access network solutions, and the solutions available in the physical layer level.

- *Improving cryptographic primitives:* To overcome the traffic oriented security breaches in the AN, Rahman et al. proposed a mechanism for encrypting the payload communicated between the UE and the BS with Advanced Encryption Standard (AES) 256-bit. The signaling protocol was secured using a strategy inspired by Open Whisper System (OWS), while the AES keys were regenerated for each session to secure future secrecy [77].
- *Physical layer solutions:* Wang et al. proposed a Physical Layer Security (PLS) model for multi-tier Heterogeneous Cellular Networks (HCNs), where the entities are randomly located [78]. In the proposed model, a secrecy mobile association policy was formed based on the truncated Average Received Signal Power (ARSP). Signal-to-Interference-plus-Noise-Ratio (SINR) measurement was used to determine the connection probability of UEs.
- *5G based access network solutions:* In a study by Fang et al. [70], a 5G wireless security architecture was proposed to cover the following domains: network access, network, user, and application. The network access domain is related to A1, where the physical layer technologies, such as massive MIMO, HetNet and D2D, are identified as challenges to overcome in terms of security. Xiao et al. [79] introduced a Ray Tracing based channel model for 5G mmWave small cell communication security. Ray phenomenon, such as direct, reflected, refracted, and scattered, were considered. The correlation matrix concept was used to identify the relevance between the eavesdroppers and legitimate UEs.

Summary: The usage of conventional security primitives, though they are enhanced, aggregate unwanted burden on the application layer payload space of the traffic delivery. Despite the improved BW and multiple channel support furnished by 5G and MEC, these cumbersome approaches are limiting the extent of novel applications, such as autonomous vehicles, to broaden their features. Thus, light-weight primitives as indicated in the study by Chen [80] or QR crypto approaches [68] can be engaged to heighten the complexity of the security schemes. Another way to reduce the load of the application layer is to embed the security mechanisms into the PHY layer as in PLS approaches specified above. However, these approaches are diverse and reliant on the communication device (i.e. vendor architecture), medium (i.e. wireless/ wired, FO), and the technology (i.e. BLE, Wi-Fi, Zigbee, or LoRaWAN). Therefore, a compliance on the PLS primitives to be employed should be established to prevent interoperability and compatibility issues with PHY layer protocols. 5G-based RF networks are still at an experimental stage. Both channel models and network architectures should be specified and standardized for each 5G-based use case to avoid discrepancies after deployment. Security and privacy should also be considered primary requirements when forming such standardization.

*2) **A2: Ad-hoc connectivity between User Equipment***

The threats on A2 are associated with the links that are established between UEs in an ad-hoc manner. These links employ short range communication channels that are used for data transferring purpose under the influence of specific UE Apps. The connectivity type is Device-to-Device (D2D) that establishes a direct communication link between two devices, without requiring any BS for connectivity [81]. Short range communication technologies such as Bluetooth, Bluetooth Low Energy (BLE), Near Field Communication (NFC), ZigBee, Wi-Fi direct, narrowband IoT (NB-IoT), SIGFOX or any technology which could form a Mobile Ad hoc Network (MANET) are capable of deploying connections between UEs [1], [25], [55]. Moreover, FlashLinQ and Proximity Services (ProSe) are also capable of forming D2D communication platforms. FlashLinQ, developed by Qualcomm facilitates content sharing, gaming, and social networking features to proximity devices. ProSe is a standardization published by the 3GPP for enabling proximity discovery and direct communication for future AN based deployments [81].

Vulnerabilities: The vulnerabilities of this TV are limited to the communication channels established between the UEs. The threats originating in a UE do not directly influence the intrusions into MEC systems in this TV. A UE infiltrated by a D2D-based attack could use its connectivity with the BS to infect the MEC servers for various manipulations of the MEH explicated in E3.

- *Attacks on short-range communication technologies:* Attacks such as eavesdropping, impersonation, forging, free-riding, DoS, and privacy violation are probable [81]. Most of such attacks are feasible due to the nature of the communication protocols embedded within short range communication technologies. These technologies prioritize leveraging the bandwidth for D2D execution rather than employing security measures.
- *D2D traffic offloading:* The method of offloading cellular traffic to the UEs by the MNO is an example of a D2D instance [81]. In this approach, MNO only transmits content to specific UEs considered as cluster heads, and those UEs are multi-casting the content to respective UEs in the scope of the cluster. Moreover, use cases, such as extending the coverage through D2D connectivity for rural areas and establishment of critical communication channels for disaster or terrorist situations (where the cellular network is disabled), envision future potential for D2D-based services. In these use cases, connectivity between a UE cluster head and the MEC servers is maintained for content sharing under the supervision of the MNO. Thus, this scenario opens up new possibilities for adversaries to exploit the cluster head UEs for manipulating the service offered from them.

Existing Solutions: Ensuring D2D security mainly involves authentication, while the intervening attacks can be mitigated through a layered security model.

- *Authentication mechanisms:* In order to overcome the possible vulnerabilities of the ad-hoc link, an autonomous

authentication mechanism is an intrinsic necessity, prior to establishing the D2D link. Rahman et al. proposed a two-way mobile number based authentication scheme to secure the possible D2D engagements in their application [77].

- *Physical unclonable functions:* Physical unclonable functions (PUFs) are novel approaches used to authenticate non-human entities adapting biometric-resembled imprints generated from the unique features inherited during the fabrication process of devices or circuitry based on Challenge Response Pairs (CRPs). Hao et al. introduced a Physical Layer (PHY) End-to-End (E2E) authentication scheme that generates an IBE PHY-ID based on RF Carrier Frequency Offset (CFO) and In-phase/Quadrature-phase Imbalance (IQI) features extracted from the D2D transmissions of IoT devices [82]. CFO and IQI are acting as PUF features in this proposed system. Gao et al. reviewed the emerging nanotechnology-based PUFs on electronic circuitry while identifying the strong and weak PUFs based on their performance metrics [83]. Moreover, Marchand et al. conducted a study on Transient Effect Ring Oscillator (TERO) for PUF implementations in Field Programmable Gate Array (FPGA) families Xilinx Spartan 6 and Altera Cyclone V [84]. The results of this study proved that TERO-PUF is reliable while insensitive to voltage and temperature changes. The use of FPGA-based IoT devices is low compared to available technologies although TERO-PUF deployments for varied IoT processes were validated in this study. Zhang et al. [85] proposed a two-factor authentication mechanism for mobile phones; employing a PUF derived by comparing the audio similarity of the environments, the mobile device and the accessing PC was located. The audio similarity value is taken as a PUF parameter rather than a traditional CRP system even though the PUFs vary due to the heterogeneity of the IoT devices. These approaches suggest potential towards ensuring security in D2D-based communication channels.
- *Layered Security:* A layered security model was proposed by Hamoud et al. that employs different security mechanisms in each layer as follows: 1) Application layer: Identity Based Encryption (IBE), Elliptic Curve Cryptography (ECC), group key management, probabilistic key management, and Cipher-Policy Attribute Based Encryption (CP-ABE); 2) Network layer: secure multi-hop D2D communication, secure network coding based data splitting and shuffling, modeling of attacker intentions using game theory, routing control, and PKI based group key management; 3) MAC layer: multi-priority access controlling framework for location and identity privacy; 4) Physical layer: Channel State Information (CSI)-based key extraction, radio resource allocation scheme, and secrecy-based joint power access controlling scheme [81].

Summary: The main drawback of D2D communication in terms of security is the resource scarcity attributed by the IoT and CPS devices. Thus, lightweight approaches are essential to conserve energy, while security keys, hashes, and authentication codes should be generated in an optimal way. As these protocols are mostly autonomous, authentication credentials are computed in an algorithmic manner which can be replicated by a resourceful adversary. Thus, PUF fulfills a lacking aspect of M2M communication by employing unique and non-crypt analytic parameters to secure the D2D channels. However, in authentication stages or in a layered security circumstance, the repeated message flows included with encapsulation, coding, and modulation constructs consume energy that does not contribute to the throughput. Therefore, selective minimal security features/mechanisms should be identified for each D2D or M2M function to maximize the operating time.

*3) **A3: User Equipment (UE)***

UE can be a mobile, personal computer, CCTV camera, or wearable sensor or sensory system which can be in direct contact or connected through a gateway device to the BS. The variety of technologies attributed to a UE on the aspects of operating systems (Android, iOS, Windows, Symbian, BlackBerry, and WebOS), memory management (SD, micro-SD, and HDD), communication (RF, RFID, NFC, Bluetooth, Wi-Fi, and Ethernet), physical design and structure contribute to the improbable deployment of a generic security solution for UEs in a holistic extent. The UE contains information related to various aspects of the daily life of a person, such as private information (photos, medical reports, medical statistics, and CCTV footage), location (GPS), daily routines (shopping and transportation), enterprise information, critical infrastructure information (energy consumption, financial, banking, and emergency service status) and online account statistics—where divulging such credentials and parameters could be fatal for one's well-being [25]. Thus, threats to mobile users' privacy is of great concern [17], [5]. The resources embedded to a UE in terms of processing power, storage capacity, and battery life are the most significant factors for this threat vector [76]. Certain softwareized and virtualized attacks require a minimum level of resources to launch in an executable platform. Thus, enhanced processing and storage resources in the current UEs improve the possibility of launching such attacks that are capable of hindering detection by conventional means.

Vulnerabilities: The threats could be instantiated by a UE with or without the knowledge of the user. Even a genuine user is capable of activating a malicious software agent unintentionally. This risk of UEs being vulnerable to both physical and remote attacks makes this threat vector extremely critical. The UEs are vulnerable to physical damage, Side Channel Attacks (SCA), malicious code injection, and hardware Trojans, while all other attacks explicated in TV A1 and TV A2 are applicable to the communication interfaces.

- *Physical attacks:* Physical damages are the most common type of attacks for this TV, where they lead the attacker to re-configure the affected device such that they convey misdirecting information to ME Apps [5]. These misinforming attacks lead the MEC system to interrupt its services by feeding fake but calculated information to the edge devices. A typical scenario would be the reconfiguration of ME Apps to execute continuously (without termination and commandeering maximum resources) and exhausting its resources.

TABLE V: Summary of Countermeasures for Threat Vectors in Access Network

Ref. No.	Proposed Countermeasures	Applicable TVs in AN		
		A1	A2	A3
[77]	Encrypting payload with AES 256-bit and securing signaling with OWS	✓		
[70]	5G wireless security architecture	✓		
[78]	PLS model for multi-tier HCN	✓		
[79]	RT based channel model for 5G mmWave small cell	✓		
[77]	Two-way mobile number based D2D authentication scheme		✓	
[81]	Layered security deployment		✓	
[82]	E2E authentication scheme using IBE PHY-ID		✓	
[84]	PUF scheme for FPGA based on TERO		✓	
[85]	PUF based Two factor authentication scheme for mobile phones		✓	
[86]	Anomalous detection using machine learning			✓
[87]	SPE framework for UEs and intent based validation policy			✓

- *Side channel attacks:* The attacker's intention in launching a SCA is to extract the cryptographic parameters by cryptanalytic means. Acoustic cryptanalysis, electromagnetic analysis, timing, power-monitoring, and differential fault analysis are such SCAs applicable for UEs [88]. Security protocols engaged in communication channels are exposed with such revealed credentials. Since these attacks are arduous to detect, due to their variety, countering consumes time and resources.
- *Malware:* Malware or viruses pose a high risk factor for UEs, as their means of penetration can occur in various ways. The repercussions of a malware attack resemble a malicious code injection attack. However, the damage level it causes are reliant on the malware type—for the variants of Trojans, worms, rootkits, Spyware, Ransomware, and Adware.
- *Mobile delegation:* The offloading of services due to mobile delegation could result in UE experiencing various offloading mechanisms such as full offloading and partial offloading. These offloading mechanisms are prone to attacks [16]. An infected UE App, or a UE when offloading partial or complete executable, or when offloading passive content to the MEC server has the ability to inject a malicious agent to be activated in the corresponding ME App in the MEH. Such an attack directly contributes to the TVs E3 and E4.
- *Vulnerabilities in gateway devices:* In case of UE acting as a Machine Type Communication Gateway (MTCG) for applications like e-health or any other MTC deployments, the malicious content could be generated at one of the sensors or actuators where the UE is acting as an intermediary ingress point to the intrusion.
- *Overloading resources:* Resource allocation and scheduling of the ME App is controlled by the Mobile Edge Platform (MEP) in each MEH, where the MEP communicates with the UE App in case of a mobile delegation circumstance [44] [16]. An infected UE App could influence the MEP to allocate inessential resources at the MEH, causing a service interruption. The capability of UE to be deployed in a tamper-resistant manner, employing lightweight but effective cryptographic primitives with high resiliency, relies on the design and the manufacturer of the device.

Existing Solutions: As the attacks for this TV is targeting the UE and its ingressing/egressing channels, the solutions are focused on detecting and remedying the SCAs and malware penetrating the UE.

- *Detecting side channel attacks:* The SCADET SCA detection tool introduced by Sabbagh et al. can be used to detect prime+probe type SCAs in micro-architectural devices, which are employed in IoT devices for performing various functions [89]. Mushtaq et al. [90] propose a cache-based detection method for similar SCAs on an AES algorithm. [91] employs deep learning for SCA detection, while [92] detects motion-based SCAs via smartphone keystrokes.
- *Malware detection:* Islam et al. [86] introduced Qualcomm's Snapdragon Smart Protect as a viable solution to UEs for protecting mobiles against malware and other attacks. The Snapdragon, being a low-power, always on system, uses machine learning for detecting anomalous behavior and threats originated through the WiFi access points. Thus, infected UE App detection is plausible, while the WiFi based exploits could be mitigated to secure the UE device. Furthermore, the same paper proposes a detection mechanism which performs static analysis and run-time behavioral analysis of the UE Apps at inactive state and run-time, respectively.
- *Security framework:* Krupp et al. proposed a Security and Privacy Enhanced (SPE) framework for UE or mobile devices [87]. The main feature of SPE is that the system installation abstains from jail-breaking or rooting the existing operating system, which makes the system independent of the OS updates. An existing ontology is used for enforcing customizable security and privacy policies. Moreover, the intent of the applications regarding the user data is to validate the actions and to enforce security policies.

Summary: The higher resources and functions available for mobile devices are attracting novel, application-level threats, in addition to the typical malware, SCA, physical, or cloning attacks. In fact, adversaries can combine the method of attacking, where both malware and SCA type attacks can be perpetrated in a single threat attempt. A typical IDS is not adequate to detect all such novel attacks. Thus, application-level security features should be embedded into mobile devices in their design stages to detect and prevent them. Though there are techniques for detecting SCAs currently, novel side

channels are determined by adversaries from time to time. The processors, circuitry, and TRX interfaces should be subject to extensive security tests prior to releasing the product.

TABLE V summarizes the countermeasures and the best practices for mitigating threats from within AN-based threat vectors.

B. Threat Vectors related to the Mobile Edge Network (MEN)

The entities located in the edge network or the host level of the MEC paradigm, such as Mobile Edge Platform Manager (MEPM), Virtualization Infrastructure Manager (VIM) and the Mobile Edge Hosts (MEHs), are investigated in this section for establishing the threat boundaries. The placement of MEC servers is localized in compared to the conventional data centres. Thus, MEC edge (i.e., host) level is prone to tangible or physical security attacks [20].

*1) **E1: Mobile Edge Platform Manager (MEPM)***

The MEPM is the entity that monitors the MEH activities, using the connectivity that it maintains with the Mobile Edge Platform (MEP) contained by the MEH. This entity performs resource allocation and monitoring functions with the connections that it maintains with VIM, MEO and OSS. As MEPM is the highest level entity in the MEC host level, it is responsible for performing the following functions: managing the ME App life-cycle, traffic steering, and recording fault and performance metrics from VIM. Moreover, MEPM reports the holistic monitoring statistics of the host-level entities to the system level.

Vulnerabilities: The placement of MEN entities at the edge limits the physical tampering based attack vectors. However, the risk is higher compared to conventional CC.

- *Feeding fake configuration/ feedback data:* MEPM could be furnished with fake information regarding the resource allocation–based configuration or the feedback data. Such a threat could originate either within the AN or from an infiltrated ME App. As the MEPM is connected to the OSS, MEO and VIM, such false information is disseminated to the system-level entities, destabilizing the entire MEC system.
- *Infected through ME Apps and UE Apps:* An infected ME App could force the corresponding MEP to lead the MEPM to allocate undesired resources to induce service disruption. An already exposed UE App or a communication channel in the AN has the capability to mislead the MEPM such that it allocates more MEHs for processing, leading to resource depletion.
- *VM based attacks:* VM based attacks such as VM manipulation, Domain Name System (DNS) amplification, VM escape, Virtual Network Function (VNF) location shift, and security log troubleshooting attacks are probable for this threat vector.

*2) **E2: Virtualization Infrastructure Manager (VIM)***

VIM executes the integral task of facilitating ME Apps of virtualized infrastructure resources in every MEH within a single edge vicinity. The connections of VIM towards MEO and MEPM feed the statistics to perform the tasks of managing and monitoring Local Area Data Network (LADN) deployed in MEHs. As this is the main entity assigned for facilitating the virtual resources at the edge, the role of the VIM is similar to a hypervisor for MEHs. Thus, VIM performs the functions of allocating, managing, releasing, and performance monitoring of virtualized resources [44].

Vulnerabilities: The hypervisor functionality of the VIM attracts adversaries whose intention is to manipulate resource allocation capabilities, targeting resource depletion.

- *VM based attacks:* As VIM is responsible for allocating resources, it could be subject to attacks such as VM manipulation, VM escape, or any malicious attacks targeted for virtual deployments. These attacks would exhaust the system resources via various methods, such as allocation of inessential processing and storage facilities for a single ME App in the Virtualization Infrastructure (VI), allocating excessive amounts of ME Apps to process a single application, or blocking resources or interrupting services to a particular ME App.
- *Misleading system level entities :* The system-level entities could be confiscated for privilege escalation or service interruption threats due to their connections with VIM. If the VIM is compromised by an attack, malicious misconfiguration exploits could be launched by an attacker [69].

*3) **E3: Mobile Edge Host (MEH)***

MEH is the main host-level functional entity which performs the computational, storage, or networking operations in the MEC paradigm. An MEH consists of an MEP, Virtualization Infrastructure (VI), and a data plane or Local Area Data Network (LADN) which maintains the local connectivity among ME Apps. Additionally, the User Plane Function (UPF) is a 5G access network entity included inside the MEH for integrating the 5G core network into the LADN. As MEH is the only entity that stores the content conveyed from UE Apps, the risk of being exploited is high.

Vulnerabilities: MEHs are the main target of any attack originating from the AN towards the MEC system. As they are the main functional elements which support service processing, storage, and computation, any attempt to penetrate the MEC system through a malicious act should be directed towards the MEH from the attackers' point of view.

- *Computational offloading:* The threat of an MEH being subject to an infection of a malicious adversary is highly reliant on computational offloading processes, as discussed in the AN threat vectors. Once infiltrated, it has the capability to mislead the MEP and VI for resource allocation and service continuation.
- *VM based attacks:* The attacks applicable to any VM-based deployments are prone to ME Apps, as they are deployed in a VI. As MEHs are launched as VMs, all such attacks are directly impactful to its operation. Furthermore, service impeding attacks such as DoS or DDoS affect the autonomous operation of the MEHs.
- *Feeding false statistics to exploit internal entities:* The false statistics conveyed by the affected ME Apps could cause misconfigurations in the VI and the MEP, which could be exploitable by privilege escalation type attack.

These could lead to service disruption through resource depletion.

- *Exploiting the connection to the UPF:* The UPF component included in the MEH is maintains a link to the 5G core network. An attacker can exploit this link to attain networking credentials. Further, an infected MEH can feed false information to the core network and compromise the stability within core network entities.
- *SCAs on VMs:* Shared memory–based, cross-VM, cache-based, and energy consumption–based SCAs are possible for VM manipulation [93].

4) *E4: Connectivity between Mobile Edge Hosts*

ME Apps might require connecting with one or several MEHs for processing high end applications—in which a single MEH does not possess the resources to perform the intended function. This requires the connectivity between ME Apps operated under MEHs, which are established through MEPs. This is probable for high-end applications such as Industrial IoT (IIoT), surveillance, or critical infrastructure services. As the VI and LADN of two MEH entities are accessed, the respective VIM and UPF should be notified in addition to the subscriptions in the MEPM.

Vulnerabilities: A malicious ME App emerged from the methods explained under E3 TV is capable of infecting other connected ME Apps and MEP elements, in addition to the entities inside an MEH. However, the connections among MEHs are internal and obscured to adversaries. Thus, MitM type attacks are improbable.

- *Malicious injections:* A malicious injection occurring in the AN, after traversal into a MEH, is capable of infecting another MEH through the E4 connection.
- *Rouge ME Apps:* An infected ME App could manipulate the MEPM for resource depletion, while depleting the resources of each MEH that a malicious agent manages to propagate.

5) *E5: MEC platform connectivity between the edge and the core*

This bi-directional connection between the mobile edge system-level entities and the host-level entities is a critical link in the MEC paradigm. As these two levels are separated by the location, the connectivity could be established from long range communication links using technologies such as Microwave (MW), Fiber Optic (FO), Satellite, or RF. The registration process for a particular MES requested by a UE App is established through this link [44]. UEs connecting to an MEC system should first register at OSS through the connection extended from the BS to the UALCMP entity in the core [12]. This is the initial interfacing of UE Apps with the MEC platform. The nature of the UE App (whether it is operated by a trusted or a malicious entity), authenticity, and content transmitted from the UE App to ME App are factors to be investigated in this threat vector.

Vulnerabilities: A resourceful adversary could manage to intervene at this communication link. Even though the possibility of intervention is lower with long range communication links, the exposure of the control information could give the attacker the opportunity to exploit the MEPM, VIM, and MEH host-level entities as desired. Similarly, if the attacker managed to alter the status-updating parameters conveyed from host level to the system level, MEO and OSS could be subject to service interruption attacks.

- *Attacks on radio channels:* RF links are vulnerable to attack vectors discussed under A1.
- *Attacks on MW links:* Electromagnetic Pulse (EMP) based, Sybil, DoS, and DDoS attacks are probable with MW links [94].
- *Attacks on FO connections:* FOs are vulnerable against fiber tapping and hidden pulse attacks [95].
- *Attacks on satellite links:* Satellite Communication (SATCOM) links face the threats of kinetic, jamming, and cyber-attacks [96].

6) *E6: Connectivity between Mobile Edge Apps operated under Mobile Edge Hosts at different Base Stations*

In this situation, the UE App related to the user accesses ME Apps operated under MEHs at different mobile edge host levels residing in two BS locations controlled under a single MEO (or ME system level). A crowd-sourcing application or a smart grid application that deploys two instances of the same ME App operating at different locations is an exemplification of such a scenario. Even as ME App instances operate at geographically dispersed edge levels, they are governed by a singular trust domain contrived by an OSS and an MEO.

Vulnerabilities: The connectivity between two host levels governed by the same system level could be prone to intervening attacks as explicated in E5. These interposing attacks are capable of penetrating both the MEC host levels.

- *Intervening attacks:* Attack vectors perpetrated as MitM or Relay can be applied on various communication link types, as presented in E5.
- *Attacks on migrating services:* The service migration from one host level to the other poses the possibility of infecting two host levels through malicious content. As these applications are only probable with upscale use cases, the effects of the attacks could be incisive.

7) *E7: Connectivity with the Mobile Edge Host and the Cloud Servers*

In the case of services hosted by third party consumers, MEH maintains a connection to a centralized cloud or a server platform as a typical massive IoT based cloud implementation. In that scenario, the MEH (or MEHs) pre-processes the content in their possession before conveying them to the cloud service. Typically, the cloud service hosts the edge services as a Function as a Service (FaaS) implemented through a cloud wrapper MEC application [45]. The connection to the cloud server is instigated through the LADN of the MEH.

Vulnerabilities: The security policies and rules adopted for this type of a channel are a rarely investigated area. CSPs are susceptible to such attack vectors. Thus, interoperability issues might be plausible.

- *Intervening attacks:* Intervening attacks such as MitM, relay, or impersonation attacks are plausible for the communication channel extending from MEH to the cloud platform. Masquerading attacks launched by adversaries

to appear as a cloud service can perpetrate sinkhole or wormhole attacks.

- *Packet sniffing attacks:* The channel between the cloud service and the MEH is vulnerable to traffic sniffing attacks for perpetrating geo-location leakage or any other data exfiltration attempt [5].
- *Malicious injections:* An attack launching from this channel, due to its bi-directional connectivity and exposed nature, could result in a malicious agent in the MEH, enabling E3-based threats. Moreover, the cloud platform or centralized servers are prone to malicious attacks from an infected MEH.

Existing Solutions related to the Mobile Edge network: The mobile edge network is forming an autonomous virtualization infrastructure that interconnects all the ETSI-defined, MEC host-level entities. Thus, E1–E7 TVs pose novel challenges that require nascent solutions that operate with enhanced awareness and intelligence. The following solutions are therefore ideal.

- *Employing a trusted platform manager:* In the mobile edge host level, the VIM and the VI are the entities most probably compromised by external attacks due to the resource facilitation of ME Apps. A Trusted Platform Module (TPM) could be employed to mitigate the threats originating from the VNFs of the VI based on resource manipulation as proposed by Lal et al. [69]. A TPM is capable of measuring, analyzing, and validating status statistics of platform firmware, BIOS, boot loader, and OS kernel of the virtualized platform. A TPM acts as an attestation controller for verifying the software integrity to evaluate the trustworthiness of the virtual entities in the VI, in addition to authentication handling. Moreover, TPMs support the use cases of shared TPM, in which the TPM is shared by several VMs and a virtual TPM (vTPM) is deployed by the hosting service to be managed as a software entity [97].
- *Security zoning:* Separating the traffic through the VI for data traffic and management traffic would simplify the handling of traffic, while confiscating the infected VMs reaching the management level (i.e., VIM). This could be achieved through security zoning or forming Demilitarized Zones (DMZs) by applying differentiated access control and firewall policies on different zones [69]. Nova-network and Neutron are examples of security groups available in Openstack [98]. Moreover, forming DMZs would benefit TVs E4, E5, E6 and E7—where the connections are maintained between edge-level entities.
- *Virtual machine introspection based intrusion detection:* Virtual Machine Introspection (VMI) is a procedure of inspecting the content and the run-time behaviour of VMs deployed in a VI. Hypervisor introspection tools such as LibVMI act as a host-based IDS for monitoring activities such as memory checking and vCPU register inspection for detecting anomalous behavior in VMs [69]. Using such introspection tools enhances the performance of the hypervisor, in addition to establishing a defense mechanism for VM-based manipulation attacks probable in VIs. Garfinkel et al. [99] introduced a policy-based hypervisor introspection framework, or a VMI IDS running on a Virtual Machine Monitor (VMM). The proposed VMM virtualizes the hardware entities at operation for leveraging the properties they inherit: isolation of software running on VMs, inspection of VM states (CPU, memory and I/O), and interposing ability, while execution of programs in the VM. The main function of a VMI IDS is to maintain an OS interfacing library that develops policies and executes them to perform lie detecting, program integrity detecting, signature detecting, and row socket detecting.
- *Encrypting and signing VNF images:* Encrypting the VNF-based hard disk volumes is the best practice for mitigating the confidentiality threat of the MEC edge level. The security keys could be stored in the TPM. Moreover, VNF-based images could be cryptographically signed and verified during the launch time for mitigating the infiltration attacks attempted through VNF image uploading.
- *Remote attestation server:* Using a remote attestation server for validating the subscribed ME App and its related VM configuration would provide integrity and authenticity verification for VM processes at each executable entity at the edge level [102].
- *Security frameworks:* The holistic nature of the proposed SDN/NFV security framework by Farris et al. is insightful for adapting security measures suggested at the security enforcement plane for the edge level of MEC [100]. An approach to develop a dynamic and adaptive security mechanism employing SFC is mentioned by Hu et al. [101]. The proposed on demand security framework contains the compartments of an SFC controller, security chain controller, SDN controller, and security chain enabled domain which serves as the SDN-based packet

TABLE VI: Summary of countermeasures / best practices for Threat Vectors in Mobile Edge Networks.

Ref. No.	Proposed Countermeasures / Best Practices	Applicable TVs in MEN						
		E1	E2	E3	E4	E5	E6	E7
[69] [97]	TPM for validating resource exhaustion	✓	✓					
[69] [98]	Form DMZs to apply access control and firewall policies at VI	✓	✓	✓	✓	✓	✓	✓
[69]	Hypervisor introspection tools serving as a HIDS	✓	✓	✓				
[99]	Policy based VMI IDS framework	✓	✓	✓				
[69]	Encrypting VNF Hard disks	✓	✓	✓				
[69]	Signing VNF images	✓	✓	✓				
[69] [97]	Using a remote attestation server	✓	✓	✓				
[100]	Security framework for SDN/NFV deployments in IoT	✓	✓	✓	✓	✓	✓	
[101]	On demand dynamic SFC based security service model	✓	✓	✓	✓	✓	✓	✓

forwarding entity. An application of MEC-based Intelligent Transportation System (ITS) vehicular use case is modeled to the proposed framework. A LTE/System Architecture Evolution (SAE) network inclusive of the MEC edge level is mapped to the security chain enabled domain, while MEC-based ITS system level is mapped to the security chain controller. The proposed system, however, is only applicable to a scenario where the MEC subscribed services are operated by servers or clouds deployed external to the MEC system level entities, and the network traffic is forwarded and monitored from the SDN based MEC edge level. Thus, such an approach is applicable to E7 for securing the network traffic extended to the third party service infrastructures.

- *SCA detection on VMs and clouds:* Zhang et al. [103] introduced a SCA detection method for clouds called CloudRadar. The SCAs are detected as anomalies in the cache behaviour of VMs operating in the edge environment.

Summary: Determining the novel threats possible on an edge platform formed with virtualization technologies is a challenge that should be addressed prior to deploying MEC. TPMs offer the ability to attest the connecting UEs to determine their legitimacy. This is an important fact that leads to preventing the edge platform from malicious penetrations. Furthermore, VMIs are key tools for determining anomalous behaviour of virtual entities. These two technologies together form a protective shell to prevent malicious injections from ingressing to the MEC edge level. A VMI can be attached to the VIM that monitors the VM performance, while a TPM can be connected with the MEPM for distinguishing malicious ME Apps from the legitimate ones. In addition, security mechanisms can be embedded into the virtual infrastructure when forming virtual entities or VMs. However, light-weight virtualization or containerization technologies are attributing lesser securing mechanisms. Thus, security constructs should be implemented at the VM or hypervisor platform level. Furthermore, orchestration function of the MEPM should be designed with the security-aware features.

TABLE VI summarizes the countermeasures and best practices focused on MEN based threat vectors.

C. Threat Vectors related to the Core Network

The core network expands from the MEC system level devices such as UE App Life-cycle Management Proxy (UALCMP), Customer Facing Service Portal (CFSP), Operations Support System (OSS), and Mobile Edge Orchestrator (MEO) to the backhaul network that extends to the Internet connectivity.

*1) **C1: User Application Life-cycle Management Proxy (UALCMP)***

This entity is the initial contact point for any UE App that intends to subscribe MEC services. The main function of the UALCMP is handling multiple UE App requests while determining their life cycle. As this entity includes proxy functionality, the internal addressing function is facilitated for the MEC system to link UE Apps to their corresponding ME App or ME Apps operated at the MEN.

Vulnerabilities: The attacks perpetrated on the UALCMP are targeted at its access interfaces for overburdening them.

- *Attack vectors on the access interface:* The request handling nature of this entity has the possibility of DoS, DDoS, or masquerading attacks; these would entail for service disruption or access granting for malicious intruders.
- *Manipulating life-cycle of Apps:* As the UE App life-cycle is determined by this entity, an adversary is capable of furnishing falsified information for obtaining an increased life-cycle beyond its requirements.
- *Consequences for the OSS:* As the OSS is dependent on the requests and information of the UALCMP, the service disruption of UALCMP could directly affect the OSS operations.

*2) **C2: Operation Support System (OSS)***

The OSS grants the service requests forwarded through the UALCMP or CFS portal, while instantiating or terminating ME App functions. Additionally, OSS maintains links to MEPM and MEO for extracting control information. OSS grants the approval for subscribers to use ME Apps that are configured for a particular MEC service. Thus, this entity is critical to the attackers for gaining access to the MEC system.

Vulnerabilities: As the MEC host level is reliant on OSSs' approval for instigating the MESs, the attackers' intention is to delay its operation through the UALCMP.

- *Service denying attacks:* As the UALCMP is the entity facing the service requests from UE Apps, the OSS has to be protected from DoS or DDoS attacks.
- *Feeding false information in the registration process:* Since all the UE Apps subscribing to Apps should be registered in the OSS, the attackers could attempt to inject fake information to impersonate valid entities for pertaining MEC services. If an attacker were successful, the mobile delegation–based operations would enable the possibility to infiltrate the MEC host level.

*3) **C3: Mobile Edge Orchestrator (MEO)***

MEO represents the core functionality of the MEC concept, which assigns the role of the hypervisor for the holistic MEC system. It observes the deployed MEC hosts and resource utilization status at the edge. As the hypervisor, MEO supervises the VMs and underlying hardware configured for virtualization [69]. The main functions of MEO are service migration, mobility management, and traffic steering monitoring. The hypervisor role of MEO is still applicable to scenarios where the MEC system is integrated with other driving technologies such as NFV Infrastructure (NFVI) with NFV Orchestration (NFVO) capability [31].

Vulnerabilities: In the scenario of the MEO acting as the hypervisor being compromised, the automated network configuration exploits, orchestration exploits, malicious misconfiguration, and SDN controller exploits are probable [69]. The configuration parameters forwarded from the entities such as MEPM, OSS, UALCMP, and VI are also vital to the utilization of the MEO. Therefore, mechanisms should be employed for detecting such attacks and remedying them.

- *Resource manipulation attacks:* Though MEO is deployed at the system level where malicious intrusions are improbable, resource allocation and service manipulation attacks such as DNS amplification and VM escape would be highly probable. Due to the effects of such attacks, the configuration of the MEO system could be destabilizing such that it cannot perform at its optimal level.
- *Security-log troubleshooting attacks:* As in the case of a security log troubleshooting attack, the logs of the operations of MEO or any other entity would be altered. Thus, the control statistic could not be conveyed to the corresponding ME entities for optimal operation. Even if the log information is conveyed, the entities would malfunction due to their altered content.

*4) **C4: Customer Facing Service Portal (CFSP)***

CFSP facilitates the access of ME Apps to third-party services, where it is capable of recalling service-level information from such applications [44]. Car park monitoring, connected vehicles, and IoT big data are applications suited for MEC deployment. These deployments use sensors that gather enormous amounts of data, which are pre-processed at an MEC edge server and conveyed to a centralized corporate server for further analysis [16]. For most of these services, MEC acts as a low latency aggregation point. Thus, third-party consumers instigate the service requests from Cloud Service Providers' (CSPs) end. The role of the CFSP is to approve the deployment of MEC resources for processing of such third-party requests.

Vulnerabilities: As the role of the CFSP is handling requests, it could be prone to service based attacks such as DoS and DDoS. Moreover, proper approval mechanisms should be employed by the CFSP to enable traffic steering of third party applications to the MEC host level entities. Use cases applicable to E7 are examples of extended services approved by the CFSP for third party applications. A compromised CFSP could manipulate the service subscriptions of OSS.

*5) **C5: Connectivity of the Mobile Edge Orchestrator (MEO) and the 5G Core Network***

A secure interface has to be defined for the MEO and 5G core network [104]. The control signals will be exchanged between the 5G core network and MEO via this interface. Since this is the main interface that interacts with the 5G core network, this is one of the critical interfaces in the whole MEC architecture. It is possible to host both 5G core network elements and MEO in the same physical host. However, it is more likely to implement them in two different physical hosts [105]. In that case, the communication link should be established between MEO and 5G core network via the physical network. This network can be implemented using any network technology such as wireless, wired, or optical. Depending on the connecting medium and the deployed location, these entities will face different security challenges.

Vulnerabilities: The interface between MEO and 5G core is yet to be defined. However, several security threats can already be identified relative to this interface.

- *TCP/IP attacks on the channel linking MEO and the 5G core:* It is more common to use separate physical hosts for 5G core network and MEO [105]. In that case, the control traffic will be transferred between two entities via an open 5G backhaul network. Therefore, the interface between MEO and 5G core will be vulnerable to typical TCP/IP attacks such as eavesdropping, spoofing, DoS, replay, and reset attacks. It is mandatory to enable proper security mechanisms, such as mutual authentication, E2E encryption, or Challenge-Response Procedures (CRPs), to mitigate these issues. The impact of these attacks will be minimum if both MEO and 5G core are deployed in the same physical host.
- *Lack of a standard interface:* Another challenge is to properly define an interface between 5G Core and MEO [106]. It is challenging to define a proper and unified security mechanism without a standard interface. However, this challenge is somewhat relaxed since ETSI [107] is leading both 5G and MEC standardization tasks.

*6) **C6: 5G Core Network***

Ultimately, the 5G core network controls the entire 5G network. The 5G core network will enable the MEC capabilities for the selected services. Moreover, all the control signals will be forwarded to the MEC system via the 5G core network. Therefore, 5G core network is the vital element ensuring the proper operation of the whole MEC system.

Vulnerabilities: Since the 5G core network is the main control entity of whole 5G network, any attack on the 5G core network will have a significant impact on the 5G MEC system.

- *Nature of softwarized core:* In contrast to pre-5G networks, 5G networks have a softwarized or virtualized core [108]. Here, all the core network functions are implemented as VNFs. However, several security concerns are observable in the functionality of VNFs. The hardware based pre-5G core network had natural protection against many attacks due to its closed, complex, and vendor-specific nature [109]. However, the NFV base 5G core network is open and software controllable. It is comparably easy to manipulate a software-based system than a hardware-based system.
- *Typical VNF based attacks:* VNFs are vulnerable to attacks such as interoperability issues [110], VM escape [111], VNF Manipulation [69] and VNF location shift attacks [69].
- *Mismatching policies:* Different VNFs are developed by different VNF providers, and they attribute different levels of security polices. The mismatch between these differences can lead to vulnerabilities when they are deployed in the same system [110].
- *VNF based service denying attacks:* A variety of DoS/DDoS attacks on targeted services is possible when VNFs are hosted in the cloud, e.g attack on Bitbucket [112]. The impact of DDoS is even greater for virtualized networks, since this attack could spread to untargeted VNFs that are hosted on the same physical host [113].
- *VNF software flaws:* Since VNFs are software, they are vulnerable to software flaws which can lead to unintended behaviour. For instance, these software flaws can be used to bypass firewall restrictions or perpetrate buffer

overflow to execute arbitrary code [113].

- *Hypervisor flaws:* A malicious VM can escape from the virtualization environment and execute arbitrary code within the hypervisor to compromise it [111]. An attacker misuses the privileges of a compromised hypervisor to install kernel root kits in VNF's OS and to manipulate the VNF [69].
- *Issues in migration:* An attacker can migrate from a compromised VNF to a different location where fewer security or privacy policies are enforced to gain additional access to the system [69].

Existing Solutions related to the Core network: Since the core network or MEC system level forms a virtualized infrastructure, certain solutions applicable to MEN also apply here.

- *Updating security credentials:* As the MEO is the main hypervisor at the system level of the MEC deployment, it is critical to update the security patches timely while activating remote access services such as Secure Shell (SSH) only when required [69]. A strong password policy is also required for cloud and system level administrators.
- *Kernel hardening tools:* The use of Security Enhanced Linux (SELinux) for the ME system level would benefit from the kernel hardening tools such as secure virtualization (sVirt) or hidepd, where the separation between data files and the processes are instigated. Thus, the infrastructure of Linux kernels would enhance the possibility for counterattacking the external or internal impregnation attempts at each entity at system level.
- *Hypervisor introspection:* Hypervisor introspection [121] could be used at system level for detecting anomalous behavior.
- *Remote attestation:* Linking the remote attestation server with the edge and system levels would provide the MEO with the capability to visualize the subscribed processes transparently for verification [97].
- *NFVI trust platform:* Yan et al. [114] propose a NFVI Trust Platform (NFVI-TP) for future 5G networks where the traffic flows are steered using SDN and cloud computing adopted for instigating services. The formation of this framework is holistic and possible for deploying at MEC system level due to the expansion of virtualized security and trust functions across the NFVI system. The design focus of the proposed platform towards 5G network is ensuring the symbiosis of 5G core network and the system level entities. The proposed framework employs a Root Trust Module (RTM) for certifying the trust of entities and serves as a TPM. Moreover, the framework performs remote attestation, trust management, QoS enhancement, VNF reputation management, identity management, secure authentication, and SDN security.
- *SDN/NFV framework:* A framework is proposed by Farris et al. [100] for enforcing security in SDN/NFV deployments for MEC-IoT use cases. The framework is formed with three planes: the user plane, the security orchestration plane, and the security enforcement plane. The user plane provides means of configuring security policies applicable to the system and the network, such as authentication, authorization, filtering, channel protection and forwarding. The security orchestration plane enforces policy-based security mechanisms to employ security enablers for raising intelligent awareness. Thus, the functionalities of this plane include policy interpreting, monitoring, and providing security enablers. The security enforcement plane combines the functions of operational domains control and management (IoT/ SDN/ NFV MANO), infrastructure and virtualization (physical entities for performing compute, storage and networking functions), VNF (security and trust mechanisms in the VI), and IoT (CoAP, EAP and DTLS protocols). Thus, the proposed framework extends to the MEC edge level, as it

TABLE VII: Summary of Countermeasures/Best Practices for Threat Vectors in the Core Network

Ref. No.	Proposed Countermeasures / Best Practices	Applicable TVs in CN					
		C1	C2	C3	C4	C5	C6
[69]	Updating the security patches timely			✓			
	Limiting the operational time of remote access services only when required						✓
	Employing strong password policy			✓			
	Using SELinux kernel and its tools	✓	✓	✓	✓	✓	✓
[69] [99]	Hypervisor introspection			✓			
[97]	Linking remote attestation with host and system levels	✓	✓	✓			
[100]	Security framework for SDN/NFV deployments in IoT	✓	✓	✓			
[114]	A framework to apply adaptive trust evaluation and sustainable trusted computing technologies to ensure computing platform trust and achieve software-defined network security	✓	✓	✓			
[113]	Discuss the security issues in SDNs when virtualized as VNFs		✓	✓		✓	✓
[115]	Study the feasibility of extending the current NFV orchestrator to have the capability of managing security mechanisms					✓	✓
[71]	Propose a security orchestrator apply to security management in ETSI NFV architecture	✓		✓		✓	✓
[116]	Presents a threat analysis and corresponding security requirements in the context of NFV	✓	✓	✓		✓	✓
[117]	Analyze the challenges on Data center in the form of Network Security Function Virtualization (NSFV) over Openflow infrastructure					✓	
[118]	Present the different architectural design patterns for the integration of SDN/NFV-based security solutions into enterprise networks					✓	✓
[119]	Present the integration approaches of network and security policy management into the NFV framework			✓		✓	✓
[120]	Provides a method of identifying the first hardware unit attacked by the security attack and security mechanism for NFV-based communication networks			✓		✓	✓

merges MEC operations and domains comprehensively.
- *Security frameworks:* Security policy frameworks to secure VNFs in NFV networks were proposed [118], [119]. A security architecture for NFV-based communication networks was proposed [120].
- *Modifying NFV orchestrator:* Modifications to the current NFV orchestrator to manage the 5G security mechanisms were proposed [71], [115], [116]. Moreover, Network Security Function Virtualization (NSFV) concept was proposed [117] to provide E2E security in 5G networks.

Summary: The UALCMP and CFSP are the interfacing entities in the MEC system level. These two entities can be subjected to DoS type attacks. In order to mitigate such attacks, an attestation server can be employed for approving the requesting UE Apps. Hence, a trust domain can be established and centered around the OSS that contrives a NFVI trust framework with TPMs at different levels. The MEC system level will be developed in a virtual environment. Thus, kernal hardening tools would protect the MEC entities at the operating system level. Further, hypervisor introspection is a key requirement for the system level entities to monitor anomalous processes occurring at both edge and system levels. Such a function can be embedded as a construct into the MEO to provide a holistic overview for malicious patterns. In addition, an agent of the said security construct should be deployed at the edge, connected to the MEPM to perform securing acts. The 5G core network standardization and its integration into the MEC system level is still a grey area. Thus, interrelations of MEC system level entities to the 5G core network entities should be standardized in the near future.

Table VII summarizes the countermeasures and best practices for mitigating threats originated within the core network based threat vectors.

D. Architectural Threat Vectors

These threat vectors elaborate the vulnerability vectors that could exist in architectural improvements associated with the MEC deployments.

*1) **AR 1: Network Slicing (NS)***

Network slicing is to slice a physical network into several logical networks to enable the simultaneous use of a singular physical network at different virtual/logical levels for heterogeneous IoT applications to alleviate capital and operating expenditure [122]. Thus, it creates an agile and dynamic on-demand networking platform on top of a physical networking infrastructure [31]. According to the 5G Information Centric Networking (ICN) model, NS framework has five functional planes: service business plane, service orchestration/ management plane, IP/ICN global orchestrator plane, domain service orchestration/ management plane, and infrastructure plane [123]. Compared with other resource sharing initiatives, such as RAN sharing, Dedicated Core Networks (DCN), and enhanced DCN (eDCN), NS offers a higher range, virtualization support, function modularization support, end-to-end connectivity, and better isolation techniques [124]. This threat vector discusses the vulnerabilities associated with NS processes and techniques.

Vulnerabilities: Most of the threats directed toward the network slicing technique exist through the network's vulnerabilities; these include the non-existent mutual authentication schemes between the entities in different slices; insecure communication among Network Slice Instances (NSIs) and Network Slice Managers (NSMs); incompatibility of diverse security protocols and policies at different slices; different security levels at different slices which could permit an attacker to exhaust the resources a secure slice gaining the access from a low security slice; and attachment of UE to multiple slices which increases the tendency for blending of information flaws in case of an infected UE App [125].

- *Attacks on vulnerabilities in the slices:* The above mentioned vulnerabilities attract attack vectors of MitM, tracing, DoS, DDoS and SCA [125] [122].
- *Slice validation issues:* Invalidation of NFV-based network slices are probable due to server shutdown for maintenance, misconfiguration, and firmware errors [126].
- *Impersonation attacks:* An impersonation attack is a highly probable threat as it could target NSMs and NS entities in different scenarios in the interaction [125].
- *Complexity among slices:* The vulnerabilities and the complexity of NS affect the MEC deployment. In order to coordinate services for various applications, MEC system level and host level entities are dispersed throughout different network slices. Thus, the attacks mentioned previously could assist adversaries in gaining control over the networking interfaces of the MEC hosts for service exhaustion and injecting malicious entities to disrupt the functioning MEHs.
- *Compatibility among slices:* The incompatibility and dissimilarity between security protocols and policies as mentioned earlier would maintain different security levels among different MEHs interacting at various network slices. These risks are susceptible to TVs E3 and E4.

Existing Solutions: Several practices are proposed for mitigating security risks in network slices which are adoptable in MEC deployments [125].

- *Authentication schemes:* Adapting mutual authentication schemes among NSMs and host platform entities before launching NSIs would intercept impersonation attacks. Moreover, NSMs should authenticate themselves at each interaction.
- *Auditing and validation of NSIs:* The NSIs that execute virtual functions or VMs should be audited and validated periodically to prevent VM-based attacks.
- *Security differentiation and slice isolation:* Different security levels should be applied to network slices with adequate isolation so that the reach of the malicious agents is restricted.
- *Authentication framework:* Ni et al. [122] proposed a service-oriented authentication framework to support NS in 5G-enabled IoT services. The proposed framework focuses on fog computing architecture for describing the authentication sequences. However, the deployment of network slices in the proposed framework is adaptable to both fog and MEC paradigms considering the resem-

blance in the service structure in the access network entities, while the core network is served by the 5G technology for both cases. The framework establishes the goals of privacy, preserving slice selection, service-oriented anonymous authentication, and service-oriented key agreement.

Summary: The NS paradigm is a means of simplifying complexities among heterogeneous networks by partitioning the network slices. The standards for NS are quite novel, and its integration into prevailing networks including MEC is in a questionable state. Even then, definition of a slice is a complex dilemma that should mitigate interoperability and compatibility concerns. Authentication among the NSIs lying in the same slice or among the slices is a challenge that should be commandeered by the NSM. In the MEC context, the edge platform acts as an intermediary in a considered slice extending from a UE to a cloud platform. Diverse security policies should be applicable for different slices, while an entity should trace the actions of NSIs for auditing purposes. MEC entities can be utilized to perform security, auditing, and monitoring functions.

*2) **AR 2: Traffic Steering***

The traffic steering of the MEC platform is conveyed by the Mp2 reference point (connection between the MEP and the data plane of the VI in a MEH). The configuration of the data plane is managed by the MEC platform, where it conveys traffic steering requests to Policy Control Function (PCF). PCF sends the corresponding traffic steering rules to the Session Management Function (SMF), where SMF handles the corresponding Protocol Data Unit (PDU) sessions [45] [73]. Moreover, Service Function Chaining (SFC) is a technique which facilitates the traffic steering policing adapting SDN and NFV constructs [127]. SFC forms the middleboxes (MBoxes) or Service Functions (SF) such as firewalls, Deep Packet Inspection (DPI) entities, Access Control Lists (ACLs), Intrusion Detection / Prevention Systems (IDS/ IPS) or Network Address Translation (NAT) [128]. As SDN and NFV are forming the MEC infrastructure for interconnecting the system level, host level, and access network, SFC is viable traffic steering technique for MEC deployments. This TV is investigating the flaws in traffic steering rules at 5G core network entities of the MEC architecture and intermediary networking entities.

Vulnerabilities: The 5G core network presents novel architectural challenges due to the requirement for provisioning diverse applications. Thus, the core network caters to these services with integrated entities into the MEC edge level. Mandating the policies related to steering the mobile traffic at the edge level is a prime requirement as such. Therefore, vulnerabilities related to these TVs are focused on 5G network entities, SFC, and the traffic headers.

- *Flows in application functions:* Application Functions (AFs) could influence the traffic routing through selection procedure of the UPF or the service request function for configuring the traffic steering rules [45]. The ability of AFs to influence the traffic rules could prompt a flaw in this process. If an attacker exploits an AF, traffic-based attacks, such as sinkhole, wormhole or Reduction of Quality (RoQ) attacks, are applicable to the LADN located at the MEH. Thus, more effective attacks such as service manipulation could be launched with resource allocation failures in the core network.
- *Service function chaining:* In terms of SFC deployments in the MEC architecture, confidentiality and integrity risks exist due to the possibility of interception, modification, or manipulation of steered traffic with incompatible security and traffic forwarding policies [127]. Moreover, SFs could disrupt services due to overloading, misconfigurations, resource scarcity, or security attacks.
- *Inconsistent packet headers in integrating security and traffic parameters:* The opaqueness attributed to MBoxes through modification of packet headers leads to inconsistencies in steering with altered addressing parameters. Therefore, attaining compatibility among security and traffic steering policies is a vital requirement for this TV.

Existing Solutions: As SFC is becoming a popular and mandatory implementation for achieving efficient traffic steering in virtualized or softwarized networks, most prevailing solutions are related to it.

- *SFC based solutions:* Hantouti et al. [127] analyzed existing SFC-based techniques and their effectiveness in terms of efficiency. In addition to classifying the existing SFC-based traffic steering methods, such as header based, tag based, and programmable switch based methods, qualitative assessment was presented for SDN-based SFC approaches while highlighting the security aspects. Li et al. [129] proposed a service chaining MEC architecture for implementing security functions which embeds the elements of access service, security classifier, virtualized security functions, and the gateway.
- *Fuzzy-based decision making in applied security:* A Fuzzy Inference System (FIS) based algorithm is used to determine the order of security functions to improve the decision-making process while packet routing is implemented from network service header encapsulation. The proposed FIS-based mechanism is evaluated and proved effective than the Simple Additive Weighting (SAW) method in this research.
- *Security framework for SFC:* Fysarakis et al. [128] implemented a reactive security framework for an industrial-grade wind farm using SDN and Supervisory Control And Data Acquisition (SCADA) elements. Various SFs such as IDS, SCADA IDS, Honeynet, firewalls, and DPI are deployed in the framework while OpenDaylight (ODL) and SFC-ODL are used for developing the SDN controller. Classification of a traffic and function chaining process is observed through a Graphical User Interface (GUI).

Summary: Standardizing traffic steering policies for the MEC system via the 5G-based PCF AF is a key requirement for realizing the MEC paradigm. Further, SFC based deployments are imminent with the CPS and IoT autonomous applications. Thus, security mechanisms should be embedded into SFC sequences, in addition to performing selective security constructs based on FIS (or any other decision supporting)

algorithms. In order to perform selective security, a framework is a realistic approach where a decision making entity can be formulated and integrated with PCF, MEO, and the MEPM entities for mandating the steering policies with security awareness.

*3) **AR 3: Service Migration***

Service migration is the process of transferring executable content configured to offer a specific MES, either between edge levels or between cloud and the edge [18]. This process could expose unprecedented vulnerabilities and flaws in an MEC environment. In a CC-based service migration, services originally hosted at cloud environments are migrated to the edge servers located proximate to the mobile devices. This reduces latency and improves the capacity of the access network. Thus, as the services are executable programs, tools or software running on a virtualized platform, the code of that particular software should be migrated to the edge in such circumstances. There are four approaches being considered for code migration by Rodrigo et al. [25]: 1) migrating only part of the code; 2) migrating an exact replica or a clone of the entire execution environment with the memory and CPU images; 3) migrating mobile agents created by mobile devices to the edge; and 4) amalgamating process cloning and mobile agents at the edge. The MEC services are typically launched as VMs in the VI of MEHs. VM migration is conducted as either live or non-live approaches [19]. In a non-live migration, the entire VM with its running states are encapsulated and transferred to the migrating vicinity, while the local operation suspends completely. In live migration, VMs are orchestrating simultaneously at different edge platforms without suspension, while multiple VM migrations are plausible via Local Area Network (LAN) or Wide Area Network (WAN) coverage. Other than services, migrating computational processes are viable applications for MEC deployments where the network controller acts as the resource selector for utilizing the computation power. The computational migration models could be formulated using the Markov Decision Process (MDP) problem based on a random-walk mobility model or a threshold-based model such as the Lyapunov optimization technique [17], [20].

Vulnerabilities: The migration of services means migrating an entire serviceable platform or a part of it to the mobile edge hosts operating at the edge. Still, the security of the migration process is a grey area due to the diversity of utilized resources and the scope of the services. The migration process begins with a service operated within a single MEH or multiple MEHs. The unauthentic nature of the Internet-based connectivity among MEC edge entities poses security issues extending to VIM, UEs, and the migration data traversing channels [19].

- *Malicious code injection:* Malicious code injection attacks targeting the migration channels are imminent at the edge network. Detecting the malicious code would be improbable once the migration process is completed. This leads to the exploitation of communication links between the edge service infrastructure and the cloud server or core network entities.
- *Attacks on mobile agents when migrating:* In the case of employing mobile agents for service migration at the edge, the probability for an intrusion is higher as the code or the service platform migrated from the access network are subjected to threats under A1. Thus, it is imperative to secure the migration processes with proper security mechanisms for mitigating massive service manipulations at the edge of the MEC deployment regardless of the diversity of the services.

Existing Solutions: Understating the dynamics involved in service migration is critical to developing security measures for the MEC architecture.

- *Secure migration framework:* Machen et al. [130] introduced a layered framework for migrating active services using VMs and containers implemented through KVM and LXC technologies, respectively. The proposed layers in the framework base, application, and instance support the MEC system for migrating a service from single MEC system level to another. The framework was tested using applications such as games, RAM simulations, video streaming, and face detection. The container-based model demonstrated peak performance. The authors, however, identified that the security risks are higher with container-based implementations compared to VMs where the connectivity is solid while migrating.
- *Blockchain for securing migration:* Wang et al. [18] suggest to employ Blockchain for resolving trust issues among entities on different domains while migrating.

Summary: Migrating the services from one MEC-based eNB to another is a unique and required function in the

TABLE VIII: Summary of Countermeasures/ Best Practices for Architectural Threat Vectors

Ref. No.	Proposed Countermeasures / Best Practices/ Method	Applicable Architectural TVs			
		AR1	AR2	AR3	AR4
[125]	Adapting mutual authentication among network slice and host network entities	✓			
	Authenticating NSMs	✓			
	Auditing and validating VM based slice instances	✓			
	Isolation and application of diversified security for different slices	✓			
[122]	Secure service oriented authentication framework	✓			
[129]	SFC based MEC architecture for SFs		✓		
[128]	Reactive security framework for wind farms		✓		
[130]	Layered Framework for VM and container migration			✓	
[18]	Employing Blockchain for establishing trust in migration			✓	
[131]	Dynamic tunneling method for PMIPv6				✓
[132]	PMIPv6 based security protocol for SH-IoT				✓
[133]	Study on PLS random models for mobility				✓

MEC context. This phase can be identified as one of the weakest occurrences of edge computing in terms of security. Employing security is questionable for the migration channel due to the latency concerns in live migrations scenarios. As the channel itself conveys executable content, exposure could lead to impregnation of malicious agents into the edge infrastructure. Therefore, a security framework is a requirement to exploit the latency and security trade-off for maximizing efficiency. Further, Blockchain solutions can be employed for securing the states and credentials in the migration process.

*4) **AR4: Mobility Management***

The term 'mobility' can be described as maintaining the connectivity of a UE when roaming from a certain coverage area of a serving BS to another via a handover mechanism to maintain service continuity [16]. The coverage of a BS could vary from multiple macro BS, Small Cell BS (SCBS), Wi-Fi Access Points (APs) to standard RAN BSs. Thus, concerns are raised over security with different capacity BSs offering various coverage and handover models. In a mobile delegation circumstance, where a UE has offloaded its processing to the edge data centers in the previously serving BS, there are two scenarios in which the continuity is established: 1) VM migration where the current VM in the serving BS MEH would be migrated to the roamed BS MEH; 2) selection of a new communication path to the UE App and the serving MEH VM. Under this TV, those issues would be investigated to identify the best strategies to counter prevailing vulnerabilities under mobility scenarios.

Vulnerabilities: The heterogeneous nature of configurations, user-server association policies, and trust domains among different coverage areas or cells are issues associated with mobility that results in severe interference and pilot contamination. Additionally, these issues degrade transmission performance and improve the latency of the service provisioning [20].

- *Availability threats:* The above mentioned mobility issues impose availability threats on UE Apps that are exploitable by an attacker with significant awareness by hijacking the frequency of the roaming channel of UE prior to or while the handshake process is underway. Such an attack is plausible with a higher latency attributed to an inefficient mobility process.
- *Complexity on UE mobility:* UE mobility in the prospect of 5G core network integration is a complicated process. Core network entity Network Exposure Function (NEF) and AN entity User Plane Function (UPF) subscribe mobility services for MEO and MEHs in MEC deployments [45].
- *VM based attacks:* In the case of VM migration, VM or the UE App could be prone to VNF location shift attack, where the UE App would be configured to instill parameters beyond the legal bounds of the service. Additionally, the key management protocols are burdened to renew the credentials in this scenario as the VM is migrated into a different trust domain.
- *Impersonation attacks:* The request for establishing the connectivity to the serving VM or ME App should be conveyed through the UALCMP to be registered in the OSS operated under the same or a different MEC system level. An attacker pretending to be a valid UE App under mobility could launch an impersonation attack which causes OSS to allocate MEH resources at the edge through MEO intervention. An adverse situation is the launching of simultaneous mobility requests as DoS or DDoS attacks for disrupting the edge services.
- *5G BSs with low security level:* Mobility and roaming events can happen frequently in the 5G network because of the popularity of local 5G networks or micro 5G operators [134]. Such localized 5G networks have limited coverage. In such a scenario, the possibility of encountering a malicious local 5G network is quite high [135]. Most of these local 5G operators do not have a high level of security similar to the main MNOs [136]. Therefore, it is comparably easy to attack local 5G networks.

Existing Solutions: The available mobility solutions are either proposed for establishing tunnels, security protocols, or models based on PHY layer parameters. All these solutions are formed with an awareness of dynamic mobility.

- *Distributed mobility management via dynamic tunneling:* Lee [131] introduced a dynamic tunneling method for the IP mobility management scheme Proxy Mobile IPv6 (PMIPv6). The proposed deployment is a Distributed Mobility Management (DMM) scheme which employs Distributed Mobility Anchors (DMAs) dispersed to cater to the UEs in the mobile network, where each DMM is served by a single Local Mobility Anchor (LMA). A mutual authentication scheme based on ECC with key agreement is employed between the DMA and the mobile entities. Moreover, tunnels in the DMM are dynamically configured considering session arrival and handover amounts. Such a system could be deployed into a MEC system, where specified MEHs acting as DMAs would establish secure mobility management among different mobile edge host levels.
- *Mobility aware security protocol:* Shin et al. proposed a security protocol for a Smart Home IoT (SH-IoT) scenario based on the PMIPv6 mobility model which facilitates route optimization, handover management, mutual authentication, key exchanging, Perfect Forward Secrecy (PFS), and privacy [132]. In the proposed protocol, a cloud-based trust management entity maintains the secure shared credentials among the LMA and the Home Gateway (HGW), in addition to the master session key shared between the Mobile Access Gateway (MAG) and HGW in the SH-IoT network. The protocol is formally verified using BAN-logic and Automated Validation of Internet Security Protocols and Applications (AVISPA) tools.
- *Secrecy in PLS mobility models:* Tang et al. [133] studied the effect of random mobility on PLS under Rayleigh fading channel for a typical BS and mobile receiver communication, where an eavesdropper is located in a circular region. The secrecy performance/probability was studied for random mobility models such as Random Waypoint (RWP), Random Direction (RD), and Border

Move (BM). The analysis on secrecy characteristics was conducted for different mobility models based on Secrecy Outage Probability (SOP) and Ergodic Secrecy Capacity (ESC) metrics. According to the results, the RWP model presented the highest secrecy performance, while secrecy improvement strategies were proposed by the authors.

Summary: Integrating mobile mobility models into the MEC system and managing the mobile and data networks collectively are challenges under this TV. At these instances, adversaries are given an opening to impregnate the MEC edge. Securing the mobility signalling channels via cryptic tunnels in a dynamic manner would challenge attempted attacks. Further, security mechanisms can be embedded into mobility protocols as specified above. PLS-based mobility models reduce the overhead on the application layer with enhanced handover convergence times, though managing the mobility aspect of both the MEC and the mobile network with embedded security is a conundrum.

Table VIII summarizes the possible countermeasures that could be adoptable for mitigating the threats of the architectural threat vectors.

E. Other Threat Vectors (OTVs)

*1) **OTV1: Charging and billing for MEC subscriptions***

The responsibility to launch MEC service infrastructure belongs to the telecommunication operators or MNOs, merely due to their authority over the prevailing mobile network with dispersed BSs. As MNOs expect profits for their existence, multitude of MESs would be subscription-based deployments with pay-per-use billing models that resemble cloud computing services. In these circumstances, current billing models applied in conventional cellular networks by tracking the routed traffic traversing through the core network are not applicable. Thus, investigating the flaws in current billing models and contemplating the probable implications on the edge computing based charging schemes is imperative for feasible deployment from MNOs' perspective.

Vulnerabilities: An adversary capable of misleading an autonomous charging process is capable of conferring financial losses to the MNO. Therefore, mitigating the inconsistencies in the charging process is a critical security requirement for the MNO.

- *Limited traceability:* There is a high probability that UE Apps launched at the edge network as ME Apps do not conveying their subscription-based consuming status to the core network entities. Displaced operations in the edge infrastructure isolated from the core entities constrict the traceability of the UE Apps subscribed through the OSS.
- *Issues with scalability and variety of MESs:* The proposed approach to charging is perpetrated by the Policy Control Function (PCF) Network Function (NF) in 5G core network employing both online and offline charging schemes [45]. Functioning with myriad potential UE Apps and accounting their corresponding ME Apps and diverse service types (priority/ best effort) for consumption appears to be an arduous task. Thus, the potential for exploitation with possible deliberated billing frauds and roaming frauds reveal a critical security failure in the MEC charging system.

Existing Solutions: ETSI specifies the requirements for off-line and on-line charging schemes for MEC based services [137]. Billing records are aggregated by the MEC system and forwarded into the Packet Data Network Gateway (PGW) on the EPC standard. This aggregation should be conducted with tracking capability to trace the billing records for detecting cyber-billing fraud.

Summary: Tracing the service consumption details in both the mobile network and the MEC platform is a requirement for establishing charging schemes for MESs. Certain MES might utilize a single edge platform or more than one edge platform. Thus, tracing the subscriber IDs over a widened geographic area is challenging. Further, securing the charging transaction framework is a critical requirement in mitigating cyber-billing frauds.

*2) **OTV2: Service impeding/delaying threats***

The MES subscription functionality performed by the OSS receives the requests through UALCMP and CFS Portal. Once the UE Apps from the regular subscribers and third party subscribers are approved for launching ME Apps, all the MESs are executed in a common virtualized infrastructure without any distinction. Such an environment is subject to resource exhaustion by insignificant processes and would lead to service disruption of priority services.

Vulnerabilities: The access capacity of current access control systems is limited, and distinguishing legitimate requests from malicious ones is challenging. These factors delay services at different phases of the service sequence that ultimately results in complete service disruption.

- *Weaknesses in the access control system:* An adversary is capable of infiltrating the MEH infrastructure, leveraging the access controlling methods' weaknesses. Approved malicious ME Apps are capable of consuming excessive resources in the MEH environment, resulting service disruption. This type of infiltration could be a result of a delinquent access control mechanism that does not feature a scheme for classifying the MES service type or its nature. Hence, a method to separate and distinctly recognizing ME Apps based on their emanating service type is intrinsic to MES deployment.
- *Delays caused by novel Quality of Experience (QoE) directives:* The directive of "application aware performance optimization" in MEC allows applications to influence the configuration of RAN resources according to the customer experience [26]. These are common with QoE directives, where unintended delays might result due to complex flexible resource bending based on feedback.
- *DoS and DDoS attacks:* A DoS- or DDoS-based threats are probable for RAN access interfaces from a malicious agent influencing the MEC cell configuration for coverage adjustments.
- *Jamming attacks:* The jamming attempts perpetrated on radio or wireless channels result in service delay, as well.

Existing Solutions: To mitigate service-delaying threats, detection is the primary approach. Thus, ample techniques

are followed to investigate an optimal detection technique to prevent them with time to spare.

- *Utilizing edge infrastructure for DDoS mitigation:* Bhardwaj et al. [141] proposed a novel approach to mitigating IoT-based DDoS attacks, leveraging the edge computing infrastructure. ShadowNet has been employed for preventing application-level IoT based DDoS attacks, which proves better early detection (10 times faster) and enables 82% of traffic to ingress during an active DDoS operation.
- *Novel DDoS detection methods:* Various studies have been conducted on mitigating DoS and DDoS attacks that might lead to service disruption through impeding. Methods such as entropy based mitigation, blockchain, fuzzy logic, genetic algorithms, and adaptive artificial immune networks were researched [138]–[140].

Summary: Weaknesses in the access control systems and validating authentication schemes invite DoS-type threats that lead to service delay. In addition, the complexity of the novel communication protocols to cater to enhanced user experience creates unintended delays in the transmissions. For security, detection and prevention of DoS and DDoS attacks are the challenges to mitigating this TV. AI- or ML-based detection schemes may lead to more accurate detection and rapid countering of DoS threats.

*3) **OTV3: Mobile Offloading***

Mobile offloading, or computational offloading, is the process of outsourcing heavy computing tasks, which are unfeasible to perform in the UE or the mobile device, to the edge environment [17]. A typical offloading task is different from a data offloading scenario. The raw data to be processed is conveyed to the MEC edge, while the ultimate decision, value, or classification is notified to the UE after the computation. The main benefits of mobile offloading are extension of the battery life of UEs, ability of users to employ sophisticated services that demands beyond their UE specifications, and improved capacity for storage within the edge infrastructure [16]. The intended outcomes of minimizing the energy consumption and offloading time (addition of transmission, execution, and receiving times) form a formidable problem model for offloading tasks in which the security is considered as a secondary goal.

Vulnerabilities: As security is a secondary goal of offloading, an extensive investigation into offloading schemes has not been conducted. There are issues with caching, authenticating the UE, and conveying credentials when offloading and retrieving the processed results. Offloading during a handover situation creates a complex scenario.

- *Issues with caching / cache poisoning:* The mobile offloading processes intended by the MEC edge deployments require caching functionality in the virtualization infrastructure. The multitude of UE Apps delegated to the edge demand extended caching spaces that would overrun the VM processor caching, resulting in service interruption and major latency. An adversary could target this vulnerability of the caching mechanism to launch cache poisoning attacks. Managing and monitoring the caches are intrinsic to the dynamic memory of the VI and ceasing any feasible attacks.
- *Authentication credentials:* Ensuring the security of sensitive credentials used in authentication schemes established between the edge and mobile devices is imperative for eliminating exposure of the entire system. Compromised credentials grant the perpetrator the ability to launch spoofing, eavesdropping, and data manipulation attacks on the edge system.
- *Credential transmission:* The credentials traversing from the edge to the core network are susceptible to intervening attacks due to the dispersed nature of the two networks. Thus, employing adequate levels of cryptic engagements in the communication channels, along with employing trust management schemes among entities operating on edge and the core, is critical to protecting the confidentiality and integrity of the secure credentials.

Existing Solutions: The offloading problems are not only related to security, but also deal with energy, computational, and networking costs that improve the efficiency of the process. Thus, security solutions should be concerned with the efficiency of the offloading task.

- *Genetic algorithms:* Huang et al. formulated the computation offloading problem considering security, energy consumption, and workflow execution time for a MEC environment [142]. Genetic algorithms are employed for devising coding strategies for Security and Energy Effi-

TABLE IX: Summary of Countermeasures / Best Practices for Other Threat Vectors

Ref. No.	Proposed Countermeasures / Best Practices/ Method	Applicable Other TVs			
		OTV1	OTV2	OTV3	OTV4
[137]	ETSI charging and billing specifications	✓			
[138]	Blockchain		✓		
[139]	Fuzzy logic		✓		
[140]	Adaptive artificial immune networks		✓		
[141]	Leveraging edge computing to mitigate IoT-DDoS attacks		✓		
[139], [142]	Genetic Algorithms (GAs)		✓	✓	
[143]	PLS model for multi-user multi-carrier MEC channels			✓	
[144]	Secure computational offloading method for D2D			✓	
[145]	Secure UAV edge computing offloading scheme			✓	
[146]	MEC offloading with secure data and resource allocation			✓	
[147]	Security service orchestration center for SDN control plane				✓
[148]	SPLM for secure live migration of services				✓
[149]	Access control policies and deployment guidelines for Docker				✓
[150]	Docker escape attack defence				✓

cient Computation Offloading (SEECO). This approach is quite significant because of its SEECO consideration for MEC-based applications with resource-constrained UEs.

- *Physical layer security:* Xu at al. [143] proposed a physical layer security model for a multi-user MEC system with a multi-carrier channel that is subjected to eavesdropping attacks. An algorithm was formed for joint optimization of secure offloading via solving the latency-constrained weighted-sum energy minimization problem.

Further work on security enhancement of mobile offloading has been conducted in papers, including [144]–[146], [151].

Summary: Mobile or task offloading is one of the reasons for the existence of edge computing paradigms. Thus, there are a considerable number of offloading models proposed and perfected to balance energy and other costs while offloading the content towards the edge platform. For optimizing the energy while applying security, genetic algorithms can be employed. In addition, PLS models can be utilized for securing the offloading channels. However, development of the offloading function from the MEC edge platform perspective becomes complicated due to the engagement of the MEHs and its autonomous nature.

4) ***OTV4: Virtualization and Orchestration at the edge***

It is evident that edge computing paradigms are reliant on virtualization technologies for deployment. Virtualization offers a dynamic service provisioning functionality that could launch flexible and configurable softwarized executable instances at the edge platform. Prevailing virtualization approaches are combining hypervisor-based and light-weight virtualization technologies to form edge computing platforms [152]. Containers are deployed within a VM to attribute more dynamic governing capabilities. Even though hypervisor-based and container based methods provide an adequate level of isolation, a hybrid system might generate unintended problems that may affect security and performance. Moreover, there are a variety of orchestrating deployment options available, such as OpenNFV, CloudNFV, OpenBaton, Open MANO, Cloudify, and T-NOVA [3]. Interoperability and compatibility among these technologies are vital for creating a virtual ecosystem.

Vulnerabilities: The attack vectors probable under AR3 and OTV3 are applicable for gaining access to the virtual platforms.

- *Migration and offloading:* A typical virtualized environment is isolated and operates within its boundaries in cloud computing. In MEC or any other edge computing scenarios however, service migration and offloading scenarios are imminent. In these approaches, an adversary could intercept the migration or offloading channel for eavesdropping, relaying, or impeding purposes.
- *VM based attacks:* VM based attacks such as VNF location shift, VM manipulation, privileged escalation, VM sprawl, and VM escape are probable for intercepting the VMs [69].
- *Less tolerant containerization:* Lightweight virtualization approaches or containers are becoming popular for launching virtual platforms due to their flexibility and dynamic nature. However, they have a greater risk of intrusions than VMs due to their direct link with the kernel. Containers face issues internally for the isolation of processes, file system, network, device, and inter-process communication [153].
- *Attacks on software and orchestrators:* Softwarized attacks, along with SDN based attacks, can compromise the networking topology of the edge system. A compromised MEO, or a MEPM responsible for orchestration, could imperil the entire service infrastructure.

Existing Solutions: The security mechanisms for this TV focus on solving the issues related to virtualization technologies. Security architectures and defense mechanisms for container technology are presented below.

- *Security architectures / models:* Wang et al. [147] proposed a novel security service architecture for SDN, contriving a security service orchestration center in the control plane. This security service maintains a rule engine that ensures threat mitigation in terms network-based attacks towards the edge platforms. Sun et al. [148] proposed a security model called Security Protection of Live Migration (SPLM) for securing migration through security policy transfer and encryption. The proposed model consists of a Centralized Management Platform (CMP), virtual security gateway, security agent (SA), and hypervisor access engine entities, where the CMP and SA are performing the security functions.
- *Protection for container technology:* Yasrab et al. [149] specified the mitigation policies for Docker (i.e. container technology) for attack vectors such as kernel exploits, DoS, container breakouts, poisoned images, MitM, and ARP spoofing. Further, access control policies and secure deployment guidelines are mentioned for enhancing docker execution. Jian et al. [150] proposed a defense mechanism for a Docker escape attack based on detected anomalous behaviour through namespaces.

Summary: The lower risk tolerance of containerization technology, combined with the possibility of VM based attacks, extends the threat domains of the MEC edge platform. Further, vendor-based hypervisor specifications create compatibility issues among edge platforms that can be exploited by an adversary. These flaws can be exploited to impact the orchestrator entity at both edge and system levels. Therefore, securing container technologies is critical for virtual deployments. Moreover, security architectures that function at all layers of a virtual platform can be used to apply security with efficient orchestration.

Table X summarizes the potential threats to the MEC system with their correspondence to the threat vectors specified in this section. Further, a color scheme is used to indicate the likelihood of the respective threat succeeding.

TABLE X: Potential Threats and their Correspondence to Threat Vectors

Ref.	Threat/ Attack	Description/ Consequences	Threat Vectors																		
			Access			Mobile Edge							Core						Architectural			
			A1	A2	A3	E1	E2	E3	E4	E5	E6	E7	C1	C2	C3	C4	C5	C6	AR1	AR2	AR3	AR4
General Threats																						
[154]	Viruses/ worms	Disruption of all the processes in an infected entity/ system. An infected UE will attempt to propagate the malicious agent to the MEH.	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓				✓	✓		✓	✓	✓	✓
[5] [155]	Denial of Service (DoS)	Disrupting or stopping a service by overloading a service providing entity through conveying multiple service requests simultaneously. These attacks are either delaying or disrupting the MESs via various MEC interfaces.	✓	✓			✓	✓				✓	✓	✓		✓			✓	✓		
[125]	Smurf / Distributed DoS (DDoS)	A DoS attack originated from different locations rather than from a single location. Traceability is difficult than DoS. Higher impact for MESs.	✓	✓			✓	✓				✓	✓	✓		✓			✓	✓		
[5] [155]	Man in the Middle (MitM)	Intervene a communication link by intercepting the channel. Once accessed the attacker could alter or mislead the communicating parties. All the communication and internal links within and egressing the edge platform are prone to such attacks.	✓	✓					✓	✓	✓	✓							✓		✓	✓
[55]	Relay Attack	Combination of a MitM and a replay attack (re-sending extracted authentication credentials at a later instance to be identified as a valid user). Communication links towards the MEC system is subjected for these threats.	✓	✓						✓	✓	✓							✓			✓
[54], [55]	Advanced Persistent Threats(APTs)	A cyber-attack in which a series of hacking attempts are forwarded to a targeted entity. UEs and MEC interfaces are subjected to APTs via the air interface.	✓	✓	✓			✓	✓	✓	✓	✓	✓			✓			✓		✓	✓
[55]	Sybil attack	Attack launched by forging large number of pseudonym identities. These attacks could be targeting UALCMP and CFSP in an IoT context.	✓	✓									✓	✓		✓			✓			
[125] [154]	Spoofing/ Impersonation Attack	An attack where the adversary masquerades itself as an authorized entity. In MEC, a masqueraded UE is manipulating the edge and core entities.	✓	✓						✓	✓	✓	✓	✓		✓			✓	✓	✓	✓
Non Crypt-analytic Threats																						
[154] [125]	Side Channel Attacks (SCAs)	A crypt-analysis attack formed to determine the secure credentials of a protocol without exploiting the vulnerabilities of the crypto algorithm, such as acoustic crypt-analysis. UEs and MEHs in an exposed edge environment are subjected to SCAs.			✓			✓														

[25] [5]	Physical Damage	The adversary manipulating the entity or device physically to gain access or sabotage. UEs are imminent for physical tampering.			✓																	
[154]	Hardware Trojan (HT)	Malicious modification of the circuitry in a device for leaking information through radio emission and manipulate or destroy the hardware platform of the device. With 5G radio TRXs, HTs can impact the service continuity.			✓																	
Networking/ Routing Threats																						
[55] [155]	Malicious Node Injection	The adversary employs a node as a UE between the communication nodes or within the network to seek access and perform false information feeding or eavesdropping acts.	✓	✓															✓			✓
[55]	Sinkhole Attack	A compromised node attempt to attract traffic by advertising fake routing information. A sinkhole UE or a MEH in the edge platform could disrupt the services by diverting the traffic flow. A 5G based infected eNB is capable of resembling the action.	✓	✓					✓	✓	✓								✓	✓		
[55]	Wormhole Attack	The attacker would intercept a transmission and forwards to an intended location of the adversaries choosing. Applicable for UEs, MEHs, and rouge eNBs.	✓	✓					✓	✓	✓								✓	✓		
[55]	Reduction of Quality (RoQ) Attack	Enabling a manipulated service to attain more resources such as bandwidth in communication link than it requires. E.g.: A UE opting for excessive BW from the MEC eNB.	✓	✓	✓		✓	✓	✓		✓	✓							✓	✓		✓
[55]	Denial of Sleep Attack	Denying devices to activate their stand-by mode or sleep mode for power utilization in IoT or CPS networks. A MES engaged with an affected UE leads to interruption.		✓	✓														✓			
Virtualization/ VM based Threats																						
[25]	Service Manipulation	A service offered by any service providing entity is taken over forcefully to launch selective DoS or information tampering attacks. Applicable for MEHs and connected MEC system and edge level entities.				✓	✓	✓						✓	✓			✓	✓			
[25] [5]	Privilege Escalation	Launched by an internal or external adversaries exploiting the infrastructure vulnerabilities such as ill-maintenance or mis-configurations using privileged control or inside information				✓	✓	✓						✓	✓				✓		✓	

[25]	VM Manipulation Attack	An infected VM manipulates the operations under its control and possibly infects the other VMs in contact with it. MEHs operating as VMs are capable of manipulating the entire edge platform.				✓	✓	✓	✓												✓	
[69]	DNS Amplification Attack	An attacker forwards numerous malicious DNS queries through spoofed IP entities towards NFVI hosted virtual DNS (vDNS). Orchestrator / Hypervisor hosts more vDNS to accommodate the requests that cause service disruption	✓		✓	✓	✓	✓							✓							
[69]	VM Escape Attack	Occurs due to the isolation failure of the hypervisor and the VNFs where the attack propagates from single VNF to the hypervisor management APIs and finally to the hypervisor. Attacker gains access to infrastructure resources while sabotaging virtual firewall functionality				✓	✓	✓							✓							
[69]	VNF Location Shift Attack	Using the migration capability of NFVI from one legal boundary to another, an attacker shifts the corresponding resources to an illegal location that bans the service, exert financial penalties while violating privacy						✓					✓					✓			✓	✓
[69]	Security log troubleshooting failure	Compromised VNFs generate massive amount of logs on the hypervisor and deleting the initial log entries, which makes analysis of logs an arduous task while privacy leakage risks exists				✓	✓	✓					✓	✓								
Softwarized Threats																						
[113]	Software Vulnerabilities	Executing arbitrary code that exploit the flaws such as buffer overflow and weak firewall policies			✓	✓	✓	✓					✓	✓			✓				✓	
[69]	Data exfiltration / destruction	Data of an infected entity or a system would be transferred or destroyed without approval			✓			✓														
[156]	Malicious Code Injection	Code fragment of a malicious agent is injected to an active agent or a transferring executable content. Such attacks are imminent with service migration scenarios in MEC.			✓			✓													✓	

Lower Likelihood Threats Medium Likelihood Threats High Likelihood Threats

V. Privacy of MEC

In this section we address the privacy aspects of the MEC paradigm. The issues associated with MEC deployments that would compromise the privacy are identified, while the objectives for privacy preservation are declared. Finally, the related literature on privacy-preserving directives is summarized.

A. Privacy issues in MEC

In spite of the privacy enabling factors inherited by the MEC paradigm due to its proximate locality (improved location privacy; edge acting as the trusted, monitoring, privacy provisioning agent), certain aspects of MEC should be investigated to apply sufficient privacy mechanisms for users.

1) Data Privacy:

The confidentiality of user data that is either stored, processed, or traversing is considered data privacy. Any mishandling of such private data is known as a privacy leakage. Enabling Big Data applications, facilitated with high bandwidth and ultra-low latency enhancements of MEC, will generate massive amounts of personal data in the future. Applications such as healthcare, banking, and crowd-sourcing are brimful of such sensitive data [157]. Moreover, a certain dataset of a user is disseminated to server placements administered among various telecom operators due to the open service platform of MEC. This poses a confidentiality issue. In the current era, Artificial Intelligence (AI) based pattern recognition techniques are applied on user data by certain companies to identify trends and interests. As these activities outsource data without user consent, privacy is violated conspicuously. Thus, the preservation of subscriber privacy is a vital concern for launching the MEC paradigm.

2) Location Privacy:

Though Location Based Services (LBSs) enable various applications for MEC subscribers, exposure of the geo-location endangers the financial, entertainment, professional, and secrecy aspects of human life: hijacking, blackmailing, or ransoming situations are possible [158]. The user location could be revealed to the subscribed service legitimately either intentionally or unintentionally as a pop-up service request for location sharing, that the subscriber is consenting without proper assimilation, without the awareness of the consequences. Moreover, secondary mobile channels broadcasting the wireless transmission, apart from the direct channel, are bound for monitoring by eavesdroppers for tracking location [159]. These factors contribute to the violation of location privacy.

3) Identity Privacy:

Impending tactile Internet and IoT concepts are expanding the scope of the cyber-space. A method is needed to identify the billions of entities and people comprising it via interfacing UEs [157]. Any knowledge-based (username), possession-based (Random Number Generator [RNG]), inherence-based (bio-metric) cyber-address—or Physical Unclonable Function (PUF) in case of UEs—is adoptable for proving one's identity. Identity is the key to safeguarding private information in the cyber-space. An adversary capable of replicating a user identity could access the entire data cluster mapped to that identity. Attacks such as UE tampering, UE cloning, and masquerading, which commit identity theft, are examples of privacy violations in the access network. In the core network, a cyber-invader capable of exposing identity credentials of the users or entities is presented with the opportunity to exploit the MEC system. Thus, preserving the identity of the users with expedient mechanisms is a principal requisite for MEC deployments.

4) Authorized and Curious Adversaries:

An authorized entity that captures disowned data with an honest and curious intent could exist. The extracted data could then be used for usage profiling, location tracking, and disclosing credentials [25]. Thus, user privacy is violated regardless of the motive of the intruder. Such an initiative can be taken by the infrastructure or a third-party service provider that subscribes to an MES. Due to the openness of the edge ecosystem, constricting these legitimate practices is a conundrum. Every entity engaging with the ecosystem should be aware of their responsibility. Moreover, a mechanism should exist to detect any misbehaviour perpetrated by an entity or a user.

5) Computational Offloading:

Computational offloading is an exploitable feature of MEC system that could be monitored by the adversaries to determine the location information [160]. Tracking such intervening attacks are questionable due to the complexity of the offloading process and non-accountability of the attack origination. Moreover, MEC servers inherit the features to track the usage patterns of the subscribers from the contextual information and channel status parameters. This creates a distinct concern with subscribers with respect to their private information [159]. Thus, computational offloading is a feature that risks the privacy of the MEC system.

6) Service Migration:

Migrating services from one MEH to another at the same edge level or at another edge level is possibly dependent on the scope of the subscribed service and the mobility of the UE. Certain services such as AR or autonomous vehicles demand service migration in order to satisfy service requirements. Thus, a cyber-eavesdropper capable of reviewing the service statistics of the MEH entities is in a position to track the user from the migrating service patterns [158], leading to a violation of location and usage pattern privacy aspects. This vulnerability exists with compromised MEC entities that could monitor service statistics of the VI platform.

B. Objectives for privacy preservation in MEC

Based on the privacy issues and the scope for improving the privacy-related mechanisms in MEC, the following objectives are proposed as regulatory privacy policies.

1) O1 — Global compliance for privacy policies

Privacy policies should be adopted as legislation in a global context for maintained various standards beyond national or continental borders. Moreover, standardized levels of privacy policies should account for the interests and service domain of various stakeholders for pragmatic assignment of privacy regulations.

2) O2 — Responsibility of MEC service providers and consumers

MEC service providers should be responsible for any committed privacy violation within their domains, while the consumers are obligated to report any privacy violation they or other parties experience. Satisfying the responsibilities enables a privacy preserved ecosystem where privacy violations are not left unaccounted for.

3) O3 — Privacy compliance on integrating technologies

MEC integrates technologies such as NFV, SDN, ICN, Network Slicing, IoT, and 5G [39]. These technologies are operated and standardized by diverse institutions and corporations. Thus, it is vital to establish a common code of conduct among such organizations regarding privacy mechanisms and policies for mitigating conflicts of interests.

4) O4 — Data portability

This objective requires disseminating private information among MEC service providers without employing mandated standards [157]. It ensures the interoperability of the holistic cross-domain MEC system.

5) O5 — Accountability and transparency of Data Handling

As diverse stakeholders act in an MEC system, each party should declare their intention on data storing, processing, and transferring activities to other parties, including the users, for maintaining transparent service obligations.

6) O6 — Declaring minimum specification requisites of UE for subscribing MESs

Heterogeneous IoT devices subscribing to MEC services inherit varying resources. Depending on the specifications of the device, the provided level of privacy guarantees also varies (i.e., a high-end device gets better assurance than a low-end device). Thus, it is vital for MESs to publish the minimum specification requirements for ensuring the guaranteed privacy level.

7) O7 — Optimal utilization of UE resources with embedded privacy-enhancing mechanisms

Operating over the life-time of a UE is a critical factor for MESs to encourage subscriptions. An MES that performs with lower resource consumption would be preferable to the consumers. It is evident that each MES should employ privacy-preserving mechanisms embedded in their service protocols. Thus, achieving optimal resource utilization of the UE with applied privacy-preserving mechanisms is a clear objective for MEC service providers.

C. Privacy Preserving Solutions

1) Task Offloading based solutions:

As offloading becomes a common occurrence with MEC, the privacy of the data being conveyed towards the edge infrastructure is a concern addressed above. In 2017, He et al. studied the location privacy and usage pattern privacy of the MEC task-offloading feature [159]. The paper investigated the balance to restore privacy protection while maintaining maximized operational delay and energy consumption performance. A Constrained Markov Decision Process (CMDP) based scheduling algorithm was proposed as an approach to the task offloading process. CMDPs offer a better outcome compared to Markov Decision Processes (MDPs) due to their capability of applying multiple actions via cost parameters, thereby leading to better specification of the model. As most IoT-based privacy discussions are focused on conventional cloud computing deployments, He et al. [160] (2018) identify novel vulnerabilities in MEC-enabled IoT deployments from the wireless offloading feature. An adversary model is formed considering an untrusted/compromised service provider that monitors the UE and MEC server engagements for revealing the location of the UE employing estimation techniques. This offloading problem is formed using MDP. The privacy-aware solution is introduced as a deep Post-Decision State (PDS) learning process formulated by integrating PDS and Deep Q-Network (DQN) techniques that utilize energy-harvesting statistics. The deep PDS approach suggests an offloading strategy to the IoT device faster than the DQN method. Though the offloading scheme follows MDP in contrast to CMDP in the previous solution, the deep PDS strategy is proving viable due to its extended experience–storing feature that converges to a faster outcome to overcome the lapses in the scheduling algorithm.

2) Privacy partitioning:

In this approach, data or devices that include information are partitioned into various layers where different privacy preserving techniques can be applied effectively. Chi et al. [161] introduced a novel technique called privacy partitioning which composed a trusted local partition and untrusted remote partition. The proposed method targets privacy preservation of deep learning classification tasks employed in mobile offloading processes. The bipartite topology based on threat modelling and interactive adversarial deep networks is adopted for modelling the threat domain. The intention of the proposed framework is to attenuate the access capacity of the attackers exploiting the internal states of the deep network.

3) Mitigating privacy leakages in big data:

Big data is the representation of an extremely large amount of data that cannot be processed by conventional processing techniques. The extent of the resources required to extract, store, process, and retrieve such a volume creates doubts over the adaptability of privacy preserving mechanisms. Du et al. [162] proposed a privacy preserving method that aims to maximize the query accuracy and minimize the privacy leakage probability for big data and heterogeneous IoT applications. A machine learning–based differential privacy method is adopted by aggregating Laplacian random noise in an output perturbation process. Another method called objective perturbation is employed for forming an objective function to aggregate noise. The amount of noise is dependent on the sensitivity of data. The experimental results suggest that the privacy preserving is feasible with accurate data retrieval.

4) Chaff service based privacy preserving:

Chaff services are launched to confuse the adversary by distracting its focus towards the chaff process, while legitimate services are running simultaneously, obfuscated from the attacker. He et al. [158] proposed a chaff service based approach to preserve the user privacy. In their work, the chaff service is launched by the user or the MEC platform for confusing the eavesdropper. The eavesdropper is modelled as a maximum

likelihood detector, while several chaff control strategies are considered for formulating the model. Robustness analysis is conducted for each strategy for determining the defence strategy. Employing chaff services are expensive for the service platform. Thus, the authors conclude that deploying the proposed method should be a second line of defence.

5) Privacy models and protocols:

Security and authentication protocols that ensure the anonymity of the users engaged in communication are imperative for ensuring the privacy of the MEC subscribers. An Anonymous Authentication Key Agreement (AAKA) protocol was proposed by Jia et al. [163] for preserving the user identity and diminishing the traceability. Elliptic Curve Cryptography (ECC), bilinear pairings, and complexity assumptions are employed for forming the mutual authentication scheme for MEC subscribers. A security analysis and computational cost evaluation are conducted by the authors for proving its applicability. Ensuring user identity and anonymity leads to preservation of privacy.

A model for preserving privacy in IoT enabled MEC deployments was proposed by Li et al. [164]. The solution includes three entities, namely: Terminal Device (TD), Edge Server (ES), and Public Cloud Centre (PCC), where encrypted data forwarded from the TDs are aggregated at the ES for conveying them to the PCC. Data retrieval is only possible at the PCC by possessing the private key. This three-entity system model employs a Bilinear map of composite order groups, and Boneh-Goh-Nissim cryptosystem that inherits homomorphic properties. Five main phases, initialization, registration, encryption, aggregation, and decryption, ensure the privacy of user data traversed from TDs to the PCC.

6) Network privacy for mobility circumstances:

The allowance for higher mobility in future 5G networks creates challenges to ensure the privacy of users due to dynamic network configurations. Zhang et al. [165] investigated the adaptability of MEC for improving Mobility System Support (MSS) function proposed for overcoming the network privacy issues in Virtual Private Network (VPN) based mobile deployments. A model is formulated incorporating two BSs within a RAN. Privacy is quantified as a factor cohesive of mobile entity actual location and observed location from peer nodes. The security of the proposed model is examined in terms of anonymity, unlinkability, untraceability, repudiation, and confidentiality. Simulations result in a higher value for the location privacy metric, while performance is visualized as the highest value with least operational cost for MEC and MSS amalgamation.

7) Blockchain-Based Solutions:

Blockchain contrives a cryptographically linked or chained data blocks that are infeasible to reveal without proper credentials. This concept presents an opportunity to design a privacy protection schemes for novel MEC based protocols. Gai et al. [166] presented a permissioned blockchain model for Smart Grid Networks (SGN). The proposed high-level architecture composed of three layers intends to preserve the privacy of users enrolled in SGN operating as the nodes in the blockchain system. The identification function is based on pseudo identifiers for ensuring privacy. An entity called Super Node (SN) manages the identities of the other nodes in the SGN. The system does not record the identity details of the operating nodes in order to guarantee privacy.

8) GDPR legislation:

The European General Data Protection Regulation (GDPR) is a reform package which was enforced on the 25th of May 2018; it is an initiative taken for strengthening citizens' fundamental rights in the digital age for securing private data and preserving the privacy of individuals using any IoT application [167]. Under these novel regulations, any web or hosting service intended to acquire data from any individual should draw their consent before initialization. Unauthorized

TABLE XI: Summary of privacy solutions on the MEC.

MEC Feature / Application	Ref. No.	Privacy Solution	Applicable Privacy Objectives						
			O1	O2	O3	O4	O5	O6	O7
Mobile Offloading	[159]	CMDP based scheduling algorithm is proposed for task offloading process that ensures location and usage pattern privacy with optimum power consumption				✓			✓
	[160]	A deep Post-Decision State (PDS) learning method for suggesting an optimal offloading strategy to the IoT device that preserve the location privacy of the UE from cyber-eavesdropping				✓			✓
	[161]	Privacy partitioning method for deep learning classifications employing bipartite topology							✓
H-IoT and Big Data	[162]	Employed OPP and OJP methods for aggregating Laplacian random noise to the data for mis-informing the adversary. Privacy leakage probability is minimized				✓			✓
Service Migration	[158]	Chaff service based approach for confusing the eavesdropper that preserves privacy of subscribers				✓			
Authentication	[163]	AAKA protocol for preserving user privacy from identity protection		✓		✓	✓	✓	
IoT data aggregation	[164]	Three layer privacy preserving model for IoT enabled MEC deployments that employ a crypto system with homomorphic properties				✓			
Mobility	[165]	MEC incorporated MSS model for preserving location privacy that demonstrate operational cost efficiency							✓
Smart Grid	[166]	Blockchain based edge computing model for Smart Grid Networks that guarantee user identity privacy				✓			
GDPR	[167]	GDPR initiative	✓	✓		✓	✓		✓

handling and capturing of data is considered an offence. GDPR promotes anonymization, pseudonymization, and encryption to protect personal data, while ensuring trust by making user identities untraceable. The declaration of GDPR legislation is a critical juncture of privacy preservation in disseminating the awareness on lawful domains in the IT industry. Table XI summarizes the privacy preserving mechanisms in relation to their coverage on privacy objectives.

VI. Lessons Learned and Future Work

This section provides a concise explanation of insights gained from the survey in terms of security and privacy of MEC systems, as depicted in Fig. 5. The research problems from each previous section/subsection have been identified, and a summary of preliminary solutions is given. The presented insights align with the future directives proposed by emerging research for recognizing the potential for deploying MEC.

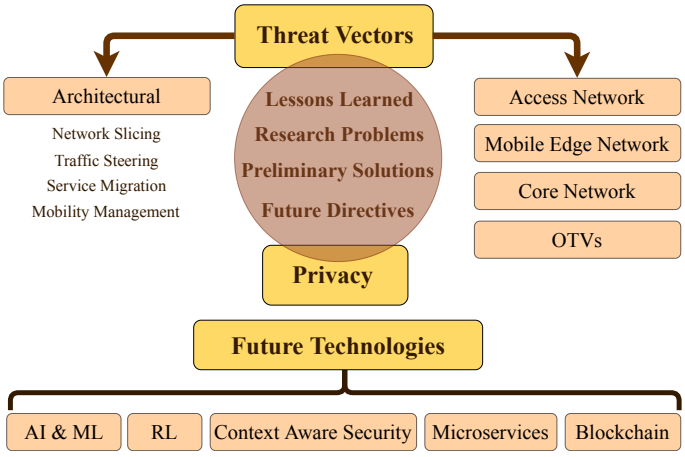

Fig. 5: Presented insights of the survey.

A. Threat Vectors

1) Access Network

Lessons Learned:

Technological heterogeneity is the salient inherence of an access network that raises concerns over the deployment scenarios of MEC in terms of scalability and security. Numerous wireless mobile communication technologies, ad-hoc technologies, and technologies engaged with UEs indicated in Section III are manifesting the interoperability and compatibility conundrums of the access network. The extent of RAN coverage and other non-3GPP technologies is confined in MEC due to the migration of storage and processing infrastructure to the edge network compared with prevailing CC deployments. However, this partition of the MEC deployment is the most vulnerable to intrusion or intervening-based security attacks. Thus, meeting confidentiality, integrity, and availability requirements is paramount to forming security protocols in the access technologies. Achieving a holistic and generic security solution, however, is inconceivable due to diverse access technologies in this domain.

Security is a prominent investigative topic among research efforts in the access network domain. Thus, various security solutions are proposed—either generic or specific to certain applicable scenarios, though security solutions focused on MEC access network deployments are inconspicuous. In terms of the users or subscribers, measures for securing privacy should be initially launched in the hardware, firmware, and software of the UE to maximize threat mitigation. This enables a first line of defense for sensitive credentials stored in the UE. From the insights we gained from this survey, we gathered that lesser work was focused on solving security issues in UEs. Moreover, employed security mechanisms should be aware of the resource consumption of the UEs to utilize battery life. Thus, efficiency and security are factors to be optimized in the UE operating in the access network.

Research Problems:

The research problems on this set of TVs are formed considering the IoT-based problems applicable on the air interface for heterogeneous device access.

- *How to manage scalability and interoperability due to heterogeneity of UEs?*
- *How to Embed security and privacy defensive features at the design stages in UEs?*
- *How to exploit the trade-off between employing security and energy consumption of UEs?*

Preliminary Solutions:

The 5G-based access network solutions proposed by Fang et al. [70] are capable of addressing the interoperability and scalability issues, in addition to security concerns presented with future access networks. PLS and Privacy by design offer unique opportunities for embedding security mechanisms at the UE design stages that would aid the communication payloads, lightening its load. The energy consumption cost required to apply security measures should be studied and modelled to understand the balance of the mentioned trade-off. Apart from work by Alharby et al. [168], there has not been significant work carried out in this area. However, the findings in this paper can be extended to build a model that presupposes the applicable level of security (security overhead) for a given energy estimate.

Future Directives:

The future of securing MEC-enabled services at the access network is swinging between optimism and pessimism. Though there are numerous security solutions proposed, derived via multitudes of research-based investigations, amalgamating all such solutions is raising concerns, as demonstrated in this survey. Several proposed techniques, however, demonstrate the potential for utilization in the context of mobile networks and mobile device or UE compatibility. PLS is one such approach that employs security mechanisms in the physical layer of the communication protocols to obscure the cryptic credentials to the softwarized entities or cyber-eavesdroppers. Thus, it offers a unique and versatile deployment option for MEC-enabled services to ensure security while mitigating the datagram overheads compared to network or application layer–based security implementations.

PUF is another promising technique related to the physical layer that guarantees future use. Various physical features

or electronic circuitry–based parameters were utilized for generating a biometric resembled imprint to derive the user identity. Thus, determining the optimal PUF for guaranteeing the highest security and privacy is the central research question for directives on this approach. Moreover, PUFs should be selected in a way that they satisfy the requirements of universal applicability, distinguishing certainty, permanent nature, and convenience of the extraction mechanism. ECC, IBE, and CP-ABE mechanisms demonstrate potential in the application-layer deployments.

Security of the UEs, gateways, or networking devices engaged in a local networking domain that connect to a MEC edge level is not addressed significantly, according to the current research findings. This is a vital research direction to be considered in the future for developing malicious entity detection, anomalous pattern detection, measures for predicting threat vectors through autonomous threat assessment, and self-healing mechanisms. MEC-enabled mobile delegation approaches for computational task offloading confirm the requirement of a solid security scheme embedded in UE. These offloading mechanisms enable the adversaries to intercept the offloading channels for either retrieving information or injecting malicious content to exploit the edge level entities. Thus, investigating the applicability of mechanisms such as homomorphism and blockchain for securing the offloading protocols—and the development of integrity assurance scenarios for detecting probable violations, while satisfying the transmission efficiency of the communication channel—is an impending directive towards realizing MEC. The diversity among the Operating Systems (OSs) of UEs is forcing the MEC enablers for establishing a generic construct when engaging them. OS and firmware updating strategies are vulnerable to exploitation due to their various inherent security levels. Thus, a minimum level of security policies should be standardized by the ETSI for subscribing MEC services. Finally, as for the GDPR compliance of privacy preservation mechanisms and objectives specified in Section V for MEC enabled UE device—their firmware and software is an achievement for the future.

2) Mobile Edge Network

Lessons Learned:

The mobile edge network is the most integral environment of the entire MEC system because of its uniqueness compared to other edge computing paradigms. In contrast, featured technological and device heterogeneity is lesser than the access network. Thus, threats are limited to the comprised MEC architectural components (E1, E2, and E3) and the connections between them (E4, E5, E6, and E7), as illustrated in Fig. 4. However, proximity to the access network elevates the risks of the principal storage and processing platforms of MEC, which adversaries are capable of exploiting. Assuming the physical accessibility to edge level entities is prevented by enforcing intrinsic restrictions, the threats to the mobile edge network could be categorized into three approaches: virtualization protocols targeted attacks (E1, E2, and E3), malicious infiltrations (E1, E2, E3, and E4), and intervening attacks (E5, E6, and E7). In terms of the entities, MEH is the most vulnerable container that stores the traversed data from the access network. ME Apps facilitate an executable platform for malicious agents obscured in the MEH databases. Moreover, seamless operation of the edge network is entirely reliant on the MEH resource utilization and service provisioning.

Virtualization and VM-based service deployments are the key enablers of the holistic MEC system. The edge level of the MEC architecture is more reliant on virtual storage and processing infrastructures. Implementing such a virtual environment could be attained via VMs or containers. The containers operate through the utilization of the underlying OS kernel virtualization, while VMs are implemented by hardware virtualization that forms an isolated execution platform with a distinguished OS in each VM [19]. Both approaches are possible for deployment.

Due to the intricate virtualization platform to be launched in the edge—expected to feature a highly evolved service infrastructure with subscription-based heterogeneous support—adversaries are incentivised to exploit the vulnerabilities. Thus, VM-based attacks such as VM manipulation, DNS amplifications, VM escape, VNF locations shift, and security log troubleshooting attacks are imminent [69]. These attacks, however, are typically orchestrated by a malicious entity. Malicious entities are integrated onto the edge network via external connections it maintains from the access network, direct connections to third party cloud services, and MEC communication links (E5 and E6). Once the system is penetrated by malicious entities, misconfiguring the virtualization platform leads to compromising the entire MEC system, including the system level. Thus, detection, quarantine, and disinfection of malicious agents are principal requirements for the edge network. Moreover, intervening attacks perpetrated on the external connections are subject to confidentiality, integrity, and privacy violations of MEC subscribers.

Research Problems:

The placement of the MEC entities at the edge present an isolated advantage in contrast to the access network devices. Thus, problems to be addressed are reliant on the malicious penetrations, flaws in virtualization, and network interceptions.

- *What is the best-suited virtualization technique to deploy the MEC autonomous edge infrastructure?*
- *How do we overcome the VM-based attacks launched in the MEC edge platform?*
- *How do we prevent infiltration of malicious agents inside the MEH?*
- *How do we secure the internal network of the MEC edge platform?*

Preliminary Solutions:

Proper monitoring of the MEC entities and the autonomously instigated virtual instances is critical to protecting the edge network. To that end, TPMs [169] offer the capability of tracing the performance metrics in both virtual and cyber-physical domains, in addition to the attestation facility that can be formulated for connecting UEs. VMI [170] is an approach to detect VM-based and malicious penetrations within the edge network. In addition, security zoning and VNF image hardening are preventive practices for enhancing the protection of the MEN [69].

Future Directives:

In retrospect on virtualization technologies, a proper mechanism should be investigated for launching the virtualization platform of MEHs. As explained above, the choice of technology deviates between containers and VMs. The selection criteria should consider efficiency and support for migration, mobility, scalability, and security. VM technologies should employ security measures in their protocols for preventing the addressed attacks. A DMZ approach is a viable scheme for distinguishing security levels in accordance with the priority of the service. In order to negate the effect of malicious activities in the edge, a Virtual Machine Introspection (VMI) method could be employed for analyzing the VM hard disk offline for detecting malicious agents [171]. The direct detection of malicious agents from scanning the virtual hard drive is only applicable to the cases of known signatures. Thus, monitoring the usage statistics of memory, storage, network, and hardware is an indirect approach to inspect uncharacteristic behavior of ME Apps. The monitoring agent could be deployed as a part of the hypervisor or as an external entity that operates within or externally to the VM [172]. A direct communicating link, however, should exist between the hypervisor and the monitoring agent in case of external monitoring. Utilizing machine learning techniques provides a unique opportunity for VMI processes to enhance their detection accuracy and reliability as presented in [173].

The external connections from and towards the edge network—more specifically the link between edge and system levels—is a vector that MEC service providers should manage circumspectly. As all the control signaling, including the service instigation / approval notifying, are conveyed via this channel, probable intrusions are imminent. An amalgamation of SDN and Virtual Private LAN Service (VPLS) technologies called Software Defined VPLS (Soft VPLS) extended to a Metropolitan Area Network (MAN) with a MPLS backbone (Soft VPMS) demonstrate potential for securing the connectivity among geo-distributed MEC edge and system levels [174]. The tunnel management feature of the Soft VPMS technology facilitates distinguishing MEC service types for meeting variant latency requirements [175]. The fast transmission adaptability of VPLS architecture makes a case for its deployment for MEC as a use case of Data Centre Interconnect (DCI) [176].

3) Core Network

Lessons Learned:

The separation of the core network or the system level from the edge network guarantees a significant security assurance for the orchestration entities in the MEC system from malicious content as they navigate the edge network for storage and processing. However, the connectivity between the system level and the edge level entities is critical for the initiation and termination of MESs and ME Apps. Once the MES is approved by the OSS, continuation of the process does not require ubiquitous connectivity to the system level until its termination. The MEO, however, maintains an overall perception of the edge level virtual resource allocation through the VIM. This bi-directional channel is critical to the security perspective due to its capability to detect resource depletion attacks, which are the most probable type of attacks at the MEC system level. Additionally, VM-based exploits are probable on MEO. The service log registry and the troubleshooting mechanism of the MEO are salient for the hypervisor operation.

UALCMP is a critical entity in MEC structure for two reasons: one is the ingress portal to the entire MEC system, while the other is for maintaining the internal addressing scheme for MESs and ME Apps launched at several edge levels under its control. Thus, perpetual functioning of the UALCMP is paramount to the seamless operation of the MEC service platforms, as it acts as a single point of failure. The access capacity of UALCMP, however, could be upgraded as it is located in the core network. Though the addressing (proxy) and the service request handling functions should be isolated to cater parallel processing systems, which persist in executing, even if one system (request handling system) is disrupted. Similarly, the factors applicable to UALCMP are recurrent for CFSP, which performs request handling for third-party services provisioned by the MEC infrastructure owner. The approval process, however, should be stern compared with UALCMP, as they are high-level services demanding elevated aggregate of resources and accessibility. The current research does not address guided methodologies to establish invulnerable SLAs or proxy functionality applicable to both UALCMP and CFSP entities. The legitimacy of the UE Apps or services requesting the MEC subscriptions are a vital concern due to malicious intents of the adversaries. Either UALCMP, CFSP, or the OSS entities do not inherit the functionality to evaluate the authenticity of the services requesting access to the system. Thus, an authority should exist to attest the services for prevention of inserting malicious content and masquerading attempts towards the MEC system. The standardization of the interfacing 5G core network and the MEC system level entities is imperative for realizing the MEC as a pragmatic solution that has been developed as an extended mobile solution. In spite of the existing work on the security concerns of this vector, the solutions are entirely reliant on a solid standardization.

Research Problems:

The core network and MEC system-level entities are considered to be secure and to reside inaccessible to the attackers. However, manipulations are possible via E5 and C5 connections that intend to mislead the entities. Furthermore, MES request handling entities of UALCMP and CFSP are prone to masquerading type attacks.

- *How to secure the connection between the MEC edge and system levels?*
- *How to detect and prevent resource exhaustion and misleading attacks?*
- *How to detect illegitimate UEs requesting access and to prevent DoSs?*
- *How to integrate security functions in the MEO?*

Preliminary Solutions:

The connection between the MEC edge and the system levels is envisioned to be established with SDN and NFV technologies. Thus, frameworks proposed elsewhere [100], [118], [119] give insights on ways to implement such SDN/NFV channels effectively. Further, the kernel hardening and hypervisor introspection tools are valuable for this virtual infrastruc-

ture. Illegitimate entities intended to access the MEC system can be detected via remote attestation [97] and TPM [114] functions. The current cloud-based orchestration architectures should be revolutionized according to the novel 5G requirements, and to perform security functions internally [115], [116], [177].

Future Directives:

As VM based intrusions are imminent on the MEO, a proper hypervisor introspection method is a requisite to secure the system level, similar to the edge level. The introspection mechanisms should feature higher scalability and responsiveness in contrast to the edge level VMI systems. These introspection mechanisms are to be independent of the regular orchestration processes conducted by the MEO. Thus, a separate processing platform should be integrated into it. A TPM is a novel method for validating VNFs employing hardware utilization statistics [69]. The Direct Anonymous Attestation with Attributes (DAA-A) and the TPM 2.0 are two such approaches [25]. Recently published patent on TPM, referred in [178], is suggesting various integration options to MEC system for validating the integrity of virtual processes. Remote attestation is another technique proposed by researches for validating the trust status of a NFV based process remotely. If an MEC system level is incapable of hosting a TPM-based service within its processing domain, the service could be outsourced to a verified attestation service provider. Even the assurance level of a security module is verifiable via remote attestation, according to the patented technique in [179].

Apart from the attestation techniques applicable to VNFs operated in a virtual environment, the concept could be extended to UE Apps and MESs. An authority, acting as a Trusted Third Party (TTP) that validates the service requests forwarded to the UALCMP or CFSP of the MEC system level, would unburden the system with legitimacy concerns. Such authorities are capable of acting remotely as the Certificate Authorities (CAs) in a Public Key Infrastructure (PKI). Thus, this approach is a viable concept for mitigating malicious penetrations, while outsourcing the trust issues to a verified authority.

4) Architectural

a) Network Slicing

Lessons Learned:

The NS concept is still in its inception stages, in terms of standardization for supporting heterogeneous services, though integration of NS concept to MEC deployments is imminent. Thus, identifying the MEC components capable of performing the functions perpetrated by NS functional entities is a goal for the future. 5G core network components, however, are already mapped with a published 5G network-slicing architecture [124]. Incompatibility of different slices to communicate to each other is a major concern for NSIs. If NSIs are represented by MEHs in the MEC system, incompatibility could be mitigated with the generic virtual protocol adaptation. Integrating the NS MANO formation into the MEC system level is probable with the MEC-NFV MANO integration achieved elsewhere [31]. In terms of security, impersonation attacks are plausible, due to the inadequacy of mutual-authentication schemes within inter-slice entities. Once a MEH acting as a NSI is compromised, the security of the adjoining NSI is at risk, regardless of the slice in which it represents. Moreover, UEs pose a severe threat due to their ability to switch between the functional slices depending on their subscribed services.

Research Problems:

The standardization of NS is critical for pragmatic deployment of the concept. As this is a paradigm defined to simplify the complexity of the future networks, interoperability and compatibility are major factors in realizing the concept.

- *How to achieve compatibility and interoperability among NSIs residing at different network slices?*
- *How to integrate network slicing concept into MEC?*
- *How to establish communication between network slices securely?*

Preliminary Solutions:

Authentication is a key mechanism that appears in multiple instances of NS applications due to its diverse technology dispersed into many slices. Thus, an authentication framework [122] is a necessity to conduct access control for a holistic NS-based network. Furthermore, proper slice isolation [180] is leading to counter many security attacks perpetrated at NSIs. NSIs should be audited and validated continuously to mitigate impersonation-like attacks.

Future Directives:

Mapping the NS architectural layers: business (slice management), NS service instance (out of eMBB, eMTC, and URCC services), NS instance (VNF slices), and resource (NFVI based radio, network, storage, and computing) layers to the MEC architecture is critical for realizing the integration of these two concepts [124]. The protocols should be standardized to enable inter-slice communication among NSIs with embedded security mechanisms. The interfaces should be varied for diverse slice interaction in UEs for restricting the shifting ability from one slice to another. This will require the users to authenticate themselves with varied credentials to improve the security in inter-slice communication. Implementing a security function in each slice with adequate level of isolation leads to safeguarding privacy in addition to security [181]. An approach, as proposed elsewhere [126], to enhance the robustness of NS from an algorithm for slice recovery and reconfiguration is a novel initiative to counter invalidating flaws in inter-slice communication. A viable network slice selection mechanism, as patented in [182], is a major requirement for deploying NS in an MEC-enabled environment.

b) Traffic Steering

Lessons Learned:

The MEC paradigm is formed combining the edge computing concept with mobile technologies, where traffic is steered utilizing mobile network-based components. MEC-generated traffic steered from UE to the edge and core networks are orchestrated by 5G core network entities such as PCF and SMF NFs. The LADN of the MEH is directly communicating with the UPF NF to enforce steering policies. As the majority of MEC-based traffic is traversed via the mobile network, engagement of the 5G entities is imminent. Thus, the security of traffic steering processes is dependent on these core network entities and their protocols. A merger between SDN and NFV technologies is envisioned to form the networking

infrastructure of MEC. Thus, SFC is a method that elaborates the potential for adapting in MEC traffic steering constructs, as it is based on SDN and NFV. However, traffic steering security is not considered significantly.

Research Problems:

Though the ETSI is defining the traffic steering policies for MEC, security is a factor that should be considered circumspectly.

- *How do we integrate 5G core network traffic steering entities or AFs into the MEC system?*
- *How do we develop SFC based reliable traffic steering policies for MEC?*
- *How do we modify traffic steering protocols and headers to embed security mechanisms?*

Preliminary Solutions:

SFC-based solutions [129] are required to enhance the traffic steering of the MEC systems. The method and the order of applicable various security measures should be determined in an analytical manner. FIS can be employed to determine the optimized methodology for applying steered traffic security. Furthermore, well formed security frameworks [128] would allow the MEC system to adapt security measures at different stages with more efficiency.

Future Directives:

SFC is a technique to be further investigated for its adaptability to MEC systems. However, standardizing the 5G core network entities interfacing specifications with the MEC components is critical for proposing pragmatic security solutions. The patent [183] explicates a traffic steering scenario in wireless communication that conveys assisting information from the eNodeB via a dedicated signaling channel. This method is optimal for MEC-enabled UEs to steer the traffic through a less occupied channel, optimizing the holistic traffic profile of the serving BS. Traffic steering methods such as load aware and heterogeneous mechanisms are proposed as viable options for MEC deployment [184]. In terms of security, Soft-VPMS–based adaptation to the networking infrastructure of the MEC system represents great potential for traffic steering management.

c) Service Migration

Lessons Learned:

Versatility to migrate a service from one functioning infrastructure to another is a feature that improves the realization of MEC in the current heterogeneous IoT market, which solves the demand for a ubiquitous connectivity to service access in a geographically dispersed context. Maintaining the service continuity subject to mobility-based 5G guarantees, however, challenges the deployment of migrating schemes for operating seamlessly [18]. A particular migration process might range from traversal of a single executable file to a cloning of an entire serviceable platform. Thus, a proper scheduling mechanism that confiscates a recording scheme for state logs is a major requirement. In addition, suspensions during the migration process are inevitable due to connectivity failures, bandwidth restrictions, or intended service disruption attacks perpetrated by adversaries. The resumption of service and retrieval of stateful logs are entirely reliant on the scheduling mechanism. Moreover, scheduling mechanisms that embed migration protocols are critical for ensuring security and restoring the service in an unintended intermittent circumstance.

The migration process is dependent on the virtualization technology (i.e., either containers or VMs [19]). Containers are lightweight in comparison to VMs that are best suited for resource scarce environments. The reason for convenience is also the pitfall of containers on self-reliance in the perspective of migration, due to the requirement of OS libraries to operate on a migrated environment. VMs are capable of executing on any host due to the migration of the entire executable constructs onto the foreign vicinity. Thus, establishing security protocols on container based deployments are restricted from the resource availability and compatibility of the local and migrating service platforms.

Research Problems:

A service migration that is rapid and secure is a requirement raised by the edge computing paradigms for maintaining service continuation in mobility circumstances. Since this is a novel area, there are doubts in the research context.

- *How do we migrate the services reliably from one MEC edge to another?*
- *How do we secure the service migration channel?*
- *How do we exploit the trade-off between security and latency in the context of the performance?*

Preliminary Solutions:

A security framework as presented in the literature [130] is required to protect the migration process, due to the complexity of the migration content and their states. A single mechanism is inadequate to cater to the security requirements. Furthermore, Blockchain [18] can be employed to secure the migration channels and to guarantee the trust among entities involved with the process.

Future Directives:

Agent-based approaches for forming the migration process scheduling schemes offer the means to recognize and maintain internal states, as the states of the agents and traversing information as interactions between migrating agents [18]. This is a valued research direction for the future. Service migration mechanisms should distinguish the sequence or operating schedule in accordance with the virtualization technology. The possibility of integrating various virtualization techniques in the MEC platforms due to diverse service providers necessitates the requirement for a compliance in security and privacy policies. Moreover, such varied virtualization technologies to be launched in the MEC environments should be standardized to feature migration in their subscription package in terms of performance indicators, such as total migration time, downtime, total network traffic, service degradation, and bandwidth utilization [19].

d) Mobility Management

Lessons Learned:

Mobility is a feature of MEC that expands its scope for impending applications such as V2E and UAV. Mobile delegation initiatives are considered as viable deployments of MEC mobility feature. In spite of facilitating a mobile storage and processing infrastructure accessible at geographically dispersed locations, security is a factor to be considered

circumspectly. Various edge levels of MEC might not inherit similar proportions of specifications due to the demand based resource provisioning of mobile networks. Thus, resource availability for the migrating service or application at the migrated MEC edge level is an obvious issue. A mobile UE App is either connected to a cloned VM or the preceding VM connected via the roaming network. In this case, timing and impersonation attacks are probable during a mobility handover. VNF-based location shift attacks are a common occurrence in this scenario. Moreover, a botnet-based attack utilizing numerous infected UE devices to emanate virtual Mobility Management Entities (vMMEs) in the NFVI based edge platform results in DDoS repercussions [69]. The protocols that are engaged in mobile handovers should employ extra level of security to mitigate such circumstances.

Research Problems:

Security issues with mobility are mostly surfacing with handover situations, where UEs re-initiate the connection with the BS. Further, with service migrations, the mobility of VMs encourages adversaries to exploit their ill-tolerant content flow from the cumbersome high-priority data to be transferred.

- *How do we secure the handover channels to mitigate timing and impersonation attacks?*
- *How do we prioritize security over latency to prevent service disruption?*
- *How do we manage mobility and state-full content transfer in a service migration circumstance?*

Preliminary Solutions:

Dynamic tunneling [131] is an effective way to secure the mobility control channels and the channels under handover phases. The prevailing security protocols and mechanisms do not consider mobility as a factor. Thus, mobility-aware security protocols [132] are improving the odds on balancing the trade-off between security over latency requirements. Furthermore, the mobility-based models formed with PLS [133] primitives are lightening the payloads in the application layer, with guaranteed security at the PHY layer level.

Future Directives:

Distributed Mobility Management (DMM) models that employ mutual authentication schemes are the key to solving the mobility related issues in the MEC deployments. PLS is a convenient approach to secure the mobility processes that are leading to unburden the transmission efficiency with alleviated header content in the upper-level security mechanisms. As mobility is an inherent factor with UAVs and vehicular entities, deploying a high-bandwidth priority data tunnel between MEC edge levels dedicated to mobility processes, is a future directive that would improve speed in the handover processes. Moreover, improved CRP-based authentication schemes robust for impersonation attacks should be investigated.

5) Other Threat Vectors

Lessons Learned:

Charging and billing schemes are imperative for the MEC systems as the billing records should be generated and maintained at both edge and core networks, while those logs should be updated and synchronized in both off-line and online aspects. However, the prevailing literature does not address security as an important aspect for charging systems. Nevertheless, novel research has been conducted to trace the billing activities for establishing services among MEC edge platforms. Research works are carried out in detection and prevention of service disruption attacks such as DoS and DDoS. Mobile or computational offloading represent an obvious deployment scenario for MEC. Security is a subject that has been studied for offloading scenarios, as it is applicable for the domains of edge computing, IoT, and D2D. Most offloading problems are formed as SEECO scenarios for optimizing the energy consumption with applied security measures. Thus, most approaches are proved based on simulations, due to the lack of pragmatic experimental platforms to evaluate the performance. The vulnerabilities in terms of softwarized, migration, offloading, networking, VMs, container, hypervisor, and orchestration aspects are inevitably impacting the MEC system, due to its reliance on virtualization technologies. The problem of security can be identified as a trade-off between security and time efficiency, when it comes to service migration and mobile offloading situations. Thus, employing security measures should consider outbound factors to maintain the service continuity of the MEC service. All these aspects are important for the realization of the MEC paradigm.

Research Problems:

OTVs present a unique threat domain that enable the confiscation of the MEC system from the specialized weaknesses featured by the edge infrastructure.

- *How do we maintain traceability with charging and billing systems in online and off-line transactions?*
- *How do we detect and prevent DoS and DDoS attacks perpetrated at the MEC system?*
- *How do we formulate a model to optimize an offloading problem that consider energy consumption, security, and processing time requirements of the application?*
- *How do we embed security measures into hypervisor or orchestrator layers of the virtualization technologies?*

Preliminary Solutions:

ETSI has identified billing functions as an important inclusion in MEC deployments and specifies the standards to achieving it practically in the MEC context [137]. Various novel means [138]–[141] have been studied to mitigate service-impeding attacks, as they pose a higher threat to the MESs, in terms of violating the 5G user guarantees. Both genetic algorithms [142] and PLS models [143] have been studied for solving the offloading problem as in SEECO context. Security architectures have been proposed for securing orchestration functions [147], [148], [177], [185], while docker containerization based solutions have also been studied [149], [150].

Future Directives:

[186] patented a method for controlling the charging process with edge services. In this approach, a control flow between an apparatus and a processor is formulated, where the apparatus connects to the UE, while the processor conducts the transactions towards the core network. Security could be integrated into the processor, while its capabilities can be enhanced to verify the apparatus legitimacy. Moreover, the enhancement of tracking the charging and billing processes in

the MEC systems, as proposed elsewhere [187], can improve the security aspect of accountability with charging schemes. In addition to the DoS and DDoS attack mitigation approaches, primitives can be embedded into traversing content for detecting and distinguishing service delaying attacks. Further, anti-jamming methods can be studied for wireless channels in the RAN and between BSs. For mobile offloading schemes, researchers should look into experiment with practical setups, in addition to simulations to prove their proposed security mechanisms. Due to the cumbersome nature of the VMs, container technologies are becoming the directive for launching dynamic virtual platforms in edge computing scenarios. Alleviating or minimizing the latency when applying security measures for container technologies for migration and offloading applications is an interesting problem to be addressed in the future.

B. MEC Privacy

Lessons Learned:

MEC architecture provides improved assurance for users regarding their sensitive data compared with cloud computing. Location and context awareness are key factors for MEC subscribers to uphold their trust in Location Based Services (LBSs). As the edge operations of MEC are performed by a telecom operator, adopting privacy preservation mechanisms could be convenient in designing MEC based services, while garnering user trust. Moreover, the capability to perform continuous monitoring functions at the edge enables the detection of privacy violations in real time. However, computational offloading and service migration features are prone to privacy violations. As the current research does not entail setting up privacy objectives on MEC systems, we propose the objectives drawn from the issues identified throughout the survey. The GDPR initiative, however, is a vital legislation put forward to raise the awareness of general public towards privacy rights and regulations. Currently, service providers are furnished with strict guidelines to develop their systems, while constricting them of any negligible acts. O3 is not a goal achieved by current work, that is an imminent use case of MEC. O4 and O7 are widely achieved objectives from the proposed solutions. Moreover, O6 is a critical strategy for being embedded with service approving process of MEC at the ME system level entities that have the potential to mitigate majority of privacy violations.

Research Problems:

Subsection V-B specifies the objectives for achieving privacy-based goals in MEC deployments. Thus, the research problems are formed being focused on them.

- *How do we standardize privacy compliance policies for MEC integrating technologies in a global context?*
- *How do we maintain accountability and transparency, while ensuring privacy?*
- *What are the minimum required resource specifications to furnish privacy enhancing mechanisms?*
- *How do we develop privacy preserving mechanisms for mobile offloading and service migration scenarios?*

Preliminary Solutions:

The EU's GDPR legislation [167] formed a compliance initiative for privacy awareness within the EU domain, which can be extended to the globe. Offloading-based privacy ensuring mechanisms are proposed in the literature [159], [160] that employ MDP-based scheduling for optimizing energy consumption with applied security. Privacy partitioning [161] is a novel approach utilized for applying different privacy mechanisms on various partitions. Privacy models and protocols proposed in [163], [164] could be adopted for the MEC system to ensure anonymity and identity of subscribers. Blockchain [166] is another reliable and trustworthy technology envisioned to be adopted for privacy models. However, solid MEC-based privacy solutions have not been implemented yet due to the lack of standardization in the MEC context. Privacy ensuring mechanisms should be designed for novel integrating technologies, as specified in O3.

Future Directives:

Software Defined Privacy (SDP) is a novel approach formalized by a three-layered technological architecture extending to application, control, and infrastructure layers for preserving privacy in cloud computing based IaaS platforms operated as Software Defined Systems (SDSyss) [188]. SDP is focused on solving the privacy violations of intra-host attacks, transborder data flow, unencrypted archived data, data leakages, and data access violations. Addressed privacy concerns, as they resemble the predicaments in MEC, envision SDP integration to MEC for privacy preservation. Privacy by Design (PbD) is a preemptive strategy proposed in case of assuring privacy is no longer sufficient with formed regulations [189]. The concept was formalized by seven foundational principles to be integrated throughout the entire design process [190]. This is a preferable starting point for IoT device manufacturers to guarantee privacy for their subscribers. Enabling privacy mechanisms in VM-based operations is a directive vital for MEC system, due to its wide adaptation of virtual processing platforms. A checkpointing approach to monitor the status of VM operation is capable of achieving that aspect [191]. The proximate edge computing infrastructure could be utilized to enhance the authentication mechanism of cloud and IoT based services employing blockchain or homomorphic encryption strategies [5]. As SDN is an imminent deployment in MEC, raising the awareness of SDN controllers is a viable directive to preserve privacy in data traversing instances (critical for computational offloading and service migration) [1].

C. Future Technologies to enhance security in MEC

1) Artificial Intelligence (AI) and Machine Learning (ML)

AI, ML, and Deep Learning (DL) approaches combined with data mining are frequently utilized for static/dynamic malware analysis and anomaly detection in the current information systems [192]. It is evident that adversaries possessing legitimate credentials pose a significant threat to the MEC system, where the critical operations are autonomous and virtualized [47]. The heterogeneity of IoT devices requesting the MES subscriptions might deceive the ingress entities, such as UALCMP and CFSP. Once the approval is granted, malicious executable content could effectively exploit the

system, resulting in repercussions to the entire system. Thus, detecting the anomalous behaviour of ME Apps operating in MEHs is a paramount necessity. DL methods are ideal for such detection. Employing AI and ML approaches guarantee a softwarized security mechanisms to be deployed with 5G related technologies in conjunction with MEC such as NFV, SDN, ICN, and NS [193]. Moreover, honeypots deployed with AI and ML platforms act as cyber defenders for deceiving the attackers [54], [192].

2) Reinforcement Learning (RL)

RL is a technique inspired by behavioral psychology for making decisions with continuous feedback extracted from the surrounding environment [194]. This method is different from its predecessor ML, as RL fails to learn from data—it is intended for learning from the experience. The main operation of a RL scheme is to maximize the cumulative reward at different states of the system from a suitable action. MDP is used as the typical mathematical formulation of RL, while Q-Learning method is ideal for exploring an optimum action on a MDP environment through trial and error. RL is adaptable to MEC intelligent offloading schemes [195]. From a security perspective, RL techniques enable IoT devices to select the optimal security protocols based on experience, which is more effective than learning methods based on data [196]. Thus, RL provides a distinct autonomous security solution for MEC deployments.

3) Context Aware Security

Context awareness of mobile-based technologies leverages the advance sensing abilities in smartphones to enable ambient intelligence through smart devices as in Siri, Google Now, and Microsoft Cortana [197]. Most typical utilization of contextual information is the provisioning of location based and personalized services with extracted geo-spatial coordinates [55]. These collaborative context aware applications, however, raise security and privacy concerns related to user data, as explained in section V. However, utilizing the context awareness feature of mobile devices and protocols to aggregate security related information enables deploying adaptive security solutions to communication protocols [198]. This directive dispenses security mechanisms to be employed at the edge level of MEC, specifically to deploy an autonomous security function in MEHs for detecting anomalous behaviour among ME Apps from security parameters derived of contextual information. The Security as a Service (SECaaS) initiatives proposed for edge level infrastructures are standardizing the deployability of security, as an autonomous and intelligent function to strengthen the context-awareness [185]. The patent described in [199] demonstrates different applicable scenarios of context aware security in the MEC deployments.

4) Microservices

Microservices signify an architectural style that structures an application as a collection of services called microservices that offer highly maintainable, loosely coupled, and independently deployable features [200]. In order to evaluate the compatibility of the application to the microservice architecture, a pattern language is used. However, the microservice architecture does not simplify the process. It disseminates the application logic into multiple smaller components, resulting in a much more complex network interaction model between components [201]. In the context of MEC, UE Apps and ME Apps could be seen as microservices. As these microservices are linked with each other for realizing various processes involved in the MEC operation, the security could be employed as a service. Microservice-based authentication mechanisms are vital for ensuring application level confidentiality and integrity in MEC communication protocols.

In the Microservice domain, osmotic computing is a novel initiative introduced to achieve a seamless migration of edge and cloud computing infrastructures [202]. Driven by the Osmosis phenomena, this paradigm features dynamic management of services and microservices across cloud and edge data centres. Microservice execution and migration processes could be secured effectively from an osmotic computing framework that embeds coherent security policies common to the edge and cloud data centres.

5) Blockchain

Blockchain was hyped up recently and has been used in many communication systems. Particularly, blockchain can play a significant role in IoT domain [203]. Several blockchain-based IoT platforms were designed not only to enable secure data sharing, secure authentication, high privacy, but also to provide automated service verification and migration [204]. On the other hand, several research works focused on highlighting the usage of blockchain for cloud computing systems to enable security, privacy and automation [205]. Since MEC proposes to move cloud computing features to the edge, blockchain will be important in the MEC domain as well. Specifically, blockchain can fuel the integration of MEC and IoT to 5G, by offering higher level of security and privacy [206]. There are some research works related to blockchain based Fog systems to improve the security and privacy along with resource and energy management [207], [208]. These platforms can be extended to provide similar level services and functions in the MEC systems as well. However, it is yet to be proposed any MEC based blockchain platforms.

VII. Conclusion

The attributed features of the MEC paradigm—imparted by the serviceable platform launched at the edge of the mobile network—improve the realization of 5G and its impending use cases. The existing literature covers the aspects of communication, offloading, service migration, and IoT integration of the nascent MEC paradigm in a significant manner, considering its novelty and contemporary development in terms of standardization. However, security and privacy considerations are not investigated comprehensively in other work. Thus, this survey addressed the security and privacy aspects of the MEC paradigm in relation to the ETSI standards to direct the research communities on the path towards a feasible MEC deployment. In order to forecast the security vulnerabilities in the MEC system, revealing the threat vectors (TVs) of the entire architecture in addition to the classical security requirements is a cardinal requisite. We considered an MEC deployment scenario which expanded to two edge / host levels governed by a single MEC system level to identify and present

TVs. The classified TVs into four categories: Access, Edge, Core, and Architectural, depending on their vector location and functioning. Furthermore, TVs that cannot be classified under the previous 4 cases were specified as other TVs. Plausible attack vectors were drawn from the identified TVs, while countermeasures were proposed from the prevailing literature. The privacy aspect of MEC is a vital contribution of this survey, which outlines the privacy enhancements that are possible with MEC architecture. We established privacy preservation objectives/goals for MEC after studying privacy concerns inherited by the MEC deployments. Moreover, the future directives that extend to diverse avenues of MEC-enabled technologies were also presented. Due to variant security vulnerabilities revealed from this survey, it is evident that proposing a universal security solution for the holistic system is improbable. Thus, intricate differences could be mitigated in employing security and privacy preservation mechanisms specific to each unique MEC use case.

ACKNOWLEDGMENT

This research is funded by the European Union under RESPONSE 5G (Grant No: 789658) and the Academy of Finland under 6Genesis Flagship (Grant 318927) projects.

REFERENCES

[1] P. Porambage, J. Okwuibe, M. Liyanage, M. Ylianttila, and T. Taleb, "Survey on Multi-Access Edge Computing for Internet of Things Realization," IEEE Communications Surveys & Tutorials, vol. 20, no. 4, pp. 2961–2991, 2018.

[2] A. Reznik, Y. Fang, and S. Ullah, "MEC in an Enterprise Setting : A Solution Outline," ETSI White Paper #30, vol. 2, no. 30, 2018, last accessed 16 May 2019. [Online]. Available: https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp30_MEC_Enterprise_FINAL.pdf

[3] T. Taleb, K. Samdanis, B. Mada, H. Flinck, S. Dutta, and D. Sabella, "On Multi-Access Edge Computing: A Survey of the Emerging 5G Network Edge Cloud Architecture and Orchestration," IEEE Communications Surveys & Tutorials, vol. 19, no. 3, pp. 1657–1681, 2017.

[4] P. S. Ranaweera, M. Liyanage, and A. D. Jurcut, "Novel mec based approaches for smart hospitals to combat covid-19 pandemic," IEEE Consumer Electronics Magazine, 2020.

[5] N. Abbas, Y. Zhang, A. Taherkordi, and T. Skeie, "Mobile Edge Computing: A Survey," IEEE Internet of Things Journal, vol. 5, no. 1, pp. 450–465, 2018.

[6] R. Von Solms and J. Van Niekerk, "From Information Security to Cyber Security," Elsevier Computers & Security Journal, vol. 38, pp. 97–102, 2013.

[7] D. Schatz, R. Bashroush, and J. Wall, "Towards a More Representative Definition of Cyber Security," Journal of Digital Forensics, Security and Law, vol. 12, no. 2, p. 8, 2017.

[8] I. Afolabi, T. Taleb, K. Samdanis, A. Ksentini, and H. Flinck, "Network Slicing and Softwarization: A Survey on Principles, Enabling Technologies, and Solutions," IEEE Communications Surveys & Tutorials, vol. 20, no. 3, pp. 2429–2453, 2018.

[9] J. Ren, D. Zhang, S. He, Y. Zhang, and T. Li, "A Survey on End-Edge-Cloud Orchestrated Network Computing Paradigms: Transparent Computing, Mobile Edge Computing, Fog Computing, and Cloudlet," ACM Computing Surveys (CSUR), vol. 52, no. 6, p. 125, 2019.

[10] A. Yousefpour, C. Fung, T. Nguyen, K. Kadiyala, F. Jalali, A. Niakanlahiji, J. Kong, and J. P. Jue, "All One Needs to Know About Fog Computing and Related Edge Computing Paradigms: A Complete Survey," Journal of Systems Architecture, 2019.

[11] E. Ahmed and M. H. Rehmani, "Mobile Edge Computing: Opportunities, Solutions, and Challenges," Future Generation Computer Systems, pp. 59–63, 2017.

[12] Y. Ai, M. Peng, and K. Zhang, "Edge Computing Technologies for Internet of Things: a Primer," Digital Communications and Networks, vol. 4, no. 2, pp. 77–86, 2018.

[13] I. Parvez, A. Rahmati, I. Guvenc, A. I. Sarwat, and H. Dai, "A Survey on Low Latency Towards 5G: RAN, Core Network and Caching Solutions," IEEE Communications Surveys & Tutorials, vol. 20, no. 4, pp. 3098–3130, 2018.

[14] J. Moura and D. Hutchison, "Game Theory for Multi-Access Edge Computing: Survey, Use Cases, and Future Trends," IEEE Communications Surveys & Tutorials, vol. 21, no. 1, pp. 260–288, 2018.

[15] H. Tanaka, M. Yoshida, K. Mori, and N. Takahashi, "Multi-Access Edge Computing: A Survey," Journal of Information Processing, vol. 26, pp. 87–97, 2018.

[16] P. Mach and Z. Becvar, "Mobile Edge Computing: A Survey on Architecture and Computation Offloading," IEEE Communications Surveys & Tutorials, vol. 19, no. 3, pp. 1628–1656, 2017.

[17] K. Peng, V. Leung, X. Xu, L. Zheng, J. Wang, and Q. Huang, "A Survey on Mobile Edge Computing: Focusing on Service Adoption and Provision," Wireless Communications and Mobile Computing, vol. 2018, 2018.

[18] S. Wang, J. Xu, N. Zhang, and Y. Liu, "A Survey on Service Migration in Mobile Edge Computing," IEEE Access, vol. 6, pp. 23 511–23 528, 2018.

[19] F. Zhang, G. Liu, X. Fu, and R. Yahyapour, "A Survey on Virtual Machine Migration: Challenges, Techniques, and Open Issues," IEEE Communications Surveys & Tutorials, vol. 20, no. 2, pp. 1206–1243, 2018.

[20] Y. Mao, C. You, J. Zhang, K. Huang, and K. B. Letaief, "A Survey on Mobile Edge Computing: The Communication Pserspective," IEEE Communications Surveys & Tutorials, vol. 19, no. 4, pp. 2322–2358, 2017.

[21] X. Yang, Z. Chen, K. Li, Y. Sun, N. Liu, W. Xie, and Y. Zhao, "Communication-constrained Mobile Edge Computing Systems for Wireless Virtual Reality: Scheduling and Tradeoff," IEEE Access, vol. 6, pp. 16 665–16 677, 2018.

[22] S. Wang, X. Zhang, Y. Zhang, L. Wang, J. Yang, and W. Wang, "A Survey on Mobile Edge Networks: Convergence of Computing, Caching and Communications," IEEE Access, vol. 5, pp. 6757–6779, 2017.

[23] 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 Consumer Electronics Magazine, vol. 5, no. 4, pp. 84–91, 2016.

[24] W. Yu, F. Liang, X. He, W. G. Hatcher, C. Lu, J. Lin, and X. Yang, "A Survey on the Edge Computing for the Internet of Things," IEEE access, vol. 6, pp. 6900–6919, 2018.

[25] R. Roman, J. Lopez, and M. Mambo, "Mobile Edge Computing, Fog et al.: A Survey and Analysis of Security Threats and Challenges," Future Generation Computer Systems, vol. 78, pp. 680–698, 2018.

[26] ETSI, "Mobile-Edge Computing–Introductory Technical White Paper," ETSI White Paper #1, 2014, last accessed 16 May 2019. [Online]. Available: https://portal.etsi.org/Portals/0/TBpages/MEC/Docs/Mobile-edge_Computing_-_Introductory_Technical_White_Paper_V1%2018-09-14.pdf

[27] M. Mukherjee, L. Shu, and D. Wang, "Survey of Fog Computing: Fundamental, Network Applications, and Research Challenges," IEEE Communications Surveys & Tutorials, vol. 20, no. 3, pp. 1826–1857, 2018.

[28] M. Satyanarayanan, P. Bahl, R. Caceres, and N. Davies, "The Case for VM-based Cloudlets in Mobile Computing," IEEE Pervasive Computing, no. 4, pp. 14–23, 2009.

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

[30] C. Mouradian, D. Naboulsi, S. Yangui, R. H. Glitho, M. J. Morrow, and P. A. Polakos, "A Comprehensive Survey on Fog Computing: State-of-the-art and Research Challenges," IEEE Communications Surveys & Tutorials, vol. 20, no. 1, pp. 416–464, 2018.

[31] M. Liyanage, P. Porambage, and A. Y. Ding, "Five Driving Forces of Multi-Access Edge Computing," arXiv preprint arXiv:1810.00827, 2018.

[32] U. Shahid and R. Krenz, "Mobile Cloud Development with Software Defined 5G Networks using NFV (Network Function Virtualization Technologies)," International Journal of Scientific & Engineering Research, vol. 6, no. 9, pp. 1552–1555, 2015.

[33] D. Huang and H. Wu, Mobile Cloud Computing: Foundations and Service Models. Morgan Kaufmann, 2017.

[34] F. van Lingen, M. Yannuzzi, A. Jain, R. Irons-Mclean, O. Lluch, D. Carrera, J. L. Perez, A. Gutierrez, D. Montero, J. Marti et al., "The Unavoidable Convergence of NFV, 5G, and Fog: A Model-Driven Approach to Bridge Cloud and Edge," IEEE Communications Magazine, vol. 55, no. 8, pp. 28–35, 2017.

[35] F. B. Jemaa, G. Pujolle, and M. Pariente, "Cloudlet and NFV-based Carrier Wi-Fi Architecture for a Wider Range of Services," Annals of Telecommunications, vol. 71, no. 11-12, pp. 617–624, 2016.

[36] Y. Xu, V. Mahendran, and S. Radhakrishnan, "Towards SDN-based Fog Computing: MQTT Broker Virtualization for Effective and Reliable Delivery," in 8th International Conference on Communication Systems and Networks (COMSNETS). IEEE, 2016, pp. 1–6.

[37] L. Zhao, W. Sun, Y. Shi, and J. Liu, "Optimal Placement of Cloudlets for Access Delay Minimization in SDN-based Internet of Things Networks," IEEE Internet of Things Journal, vol. 5, no. 2, pp. 1334–1344, 2018.

[38] H. Xiang, W. Zhou, M. Daneshmand, and M. Peng, "Network Slicing in Fog Radio Access Networks: Issues and challenges," IEEE Communications Magazine, vol. 55, no. 12, pp. 110–116, 2017.

[39] G. Gür, P. Porambage, and M. Liyanage, "Convergence of icn and mec for 5g: Opportunities and challenges," IEEE Communications Standards Magazine, vol. 4, no. 4, pp. 64–71, 2020.

[40] F. Song, Z.-Y. Ai, J.-J. Li, G. Pau, M. Collotta, I. You, and H.-K. Zhang, "Smart Collaborative Caching for Information-Centric IoT in Fog Computing," Next Generation Wireless Technologies for Internet of Things, vol. 17, no. 11, p. 2512, 2017.

[41] A. C. Baktir, A. Ozgovde, and C. Ersoy, "Enabling Service-Centric Networks for Cloudlets using SDN," in IFIP/IEEE Symposium on Integrated Network and Service Management (IM). IEEE, 2017, pp. 344–352.

[42] M. Wang, P. P. Jayaraman, R. Ranjan, K. Mitra, M. Zhang, E. Li, S. Khan, M. Pathan, and D. Georgeakopoulos, "An Overview of Cloud based Content Delivery Networks: Research Dimensions and State-of-the-art," in Transactions on Large-Scale Data-and Knowledge-Centered Systems. Springer, 2015, pp. 131–158.

[43] A. N. Khan, M. M. Kiah, S. U. Khan, and S. A. Madani, "Towards Secure Mobile Cloud Computing: A survey," Future Generation Computer Systems, vol. 29, no. 5, pp. 1278–1299, 2013.

[44] ETSI, "Mobile Edge Computing (MEC) Framework and Reference Architecture," ETSI White Paper #3, 2016, last accessed 16 May 2019. [Online]. Available: https://www.etsi.org/deliver/etsi_gs/MEC/001_099/003/01.01.01_60/gs_MEC003v010101p.pdf

[45] S. Kekki, W. Featherstone, Y. Fang, P. Kuure, A. Li, A. Ranjan, P. Debashish, F. Jianping, F. Danny, G. Verin, W. Kuo-Wei, K. Kim, A. Rohit, O. Andy, L. M. Contreras, and S. Scarpina, "MEC in 5G Networks," ETSI White Paper #28, vol. 28, no. 28, pp. 1–28, 2018, last accessed 16 May 2019. [Online]. Available: https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp28_mec_in_5G_FINAL.pdf

[46] ETSI, "Multi-access Edge Computing (MEC); Phase 2: Use Cases and Requirements," ETSI White Paper, vol. 2, 2018, last accessed 16 May 2019. [Online]. Available: https://www.etsi.org/deliver/etsi_gs/MEC/001_099/002/02.01.01_60/gs_MEC002v020101p.pdf

[47] P. Ranaweera, A. D. Jurcut, and M. Liyanage, "Realizing multi-access edge computing feasibility: Security perspective," in 2019 IEEE Conference on Standards for Communications and Networking (CSCN). IEEE, 2019, pp. 1–7.

[48] A. D. Jurcut, P. Ranaweera, and L. Xu, "Introduction to IoT Security," IoT Security: Advances in Authentication, pp. 27–64, 2020.

[49] M. Frustaci, P. Pace, and G. Aloi, "Securing the IoT World: Issues and Perspectives," in 2017 IEEE Conference on Standards for Communications and Networking (CSCN). IEEE, 2017, pp. 246–251.

[50] R. Khan, P. Kumar, D. N. K. Jayakody, and M. Liyanage, "A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements and Future Directions," IEEE Communications Surveys & Tutorials, 2019.

[51] 5GPPP-Security-WG, "5G PPP Phase 1 Security Landscape," 5GPP White Paper, 2017, last accessed 11 November 2019. [Online]. Available: https://5g-ppp.eu/wp-content/uploads/2014/02/5G-PPP_White-Paper_Phase-1-Security-Landscape_June-2017.pdf

[52] Y. Jeon, H.-I. Ju, and S. Yoon, "Design of an LPWAN Communication Module based on Secure Element for Smart Parking Application," in 2018 IEEE International Conference on Consumer Electronics (ICCE). IEEE, 2018, pp. 1–2.

[53] L. Chen, L. Chen, S. Jordan, Y.-K. Liu, D. Moody, R. Peralta, R. Perlner, and D. Smith-Tone, Report on Post-Quantum Cryptography. US Department of Commerce, National Institute of Standards and Technology, 2016.

[54] A. Jurcut, T. Niculcea, P. Ranaweera, and N.-A. Le-Khac, "Security considerations for internet of things: A survey," SN Computer Science, vol. 1, pp. 1–19, 2020.

[55] T. Kumar, P. Porambage, I. Ahmad, M. Liyanage, E. Harjula, and M. Ylianttila, "Securing Gadget-Free Digital Services," Computer, vol. 51, no. 11, pp. 66–77, 2018.

[56] S. Gupta, B. L. Parne, and N. S. Chaudhari, "Security Vulnerabilities in Handover Authentication Mechanism of 5G Network," in 2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC). IEEE, 2018, pp. 369–374.

[57] P. Hao and X. Wang, "Integrating PHY Security Into NDN-IoT Networks By Exploiting MEC: Authentication Efficiency, Robustness, and Accuracy Enhancement," arXiv preprint arXiv:1904.03283, 2019.

[58] G. Choudhary, J. Kim, and V. Sharma, "Security of 5G-mobile backhaul networks: A survey," arXiv preprint arXiv:1906.11427, 2019.

[59] X. Zhang, A. Kunz, and S. Schröder, "Overview of 5G security in 3GPP," in 2017 IEEE Conference on Standards for Communications and Networking (CSCN). IEEE, 2017, pp. 181–186.

[60] H. Zhu and C. Huang, "Availability-aware Mobile Edge Application Placement in 5G Networks," in GLOBECOM 2017-2017 IEEE Global Communications Conference. IEEE, 2017, pp. 1–6.

[61] V. Jain, V. Laxmi, M. S. Gaur, and M. Mosbah, "ETGuard: Detecting D2D Attacks using Wireless Evil Twins," Computers & Security, vol. 83, pp. 389–405, 2019.

[62] M. H. Mahalat, S. Saha, A. Mondal, and B. Sen, "A PUF based Light Weight Protocol for Secure WiFi Authentication of IoT devices," in 2018 8th International Symposium on Embedded Computing and System Design (ISED). IEEE, 2018, pp. 183–187.

[63] G. Li and P. Bours, "Studying WiFi and Accelerometer Data Based Authentication Method on Mobile Phones," in Proceedings of the 2018 2nd International Conference on Biometric Engineering and Applications. ACM, 2018, pp. 18–23.

[64] Z. Zhao, G. Min, Y. Pang, W. Gao, and J. Lv, "Towards Fast and Reliable WiFi Authentication by Utilizing Visible Light Diversity," in 2019 16th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON). IEEE, 2019, pp. 1–9.

[65] Y. Zhang, F. Ren, A. Wu, T. Zhang, J. Cao, and D. Zheng, "Certificateless Multi-Party Authenticated Encryption for NB-IoT Terminals in 5G Networks," IEEE Access, vol. 7, pp. 114 721–114 730, 2019.

[66] P. Gope, R. Amin, S. H. Islam, N. Kumar, and V. K. Bhalla, "Lightweight and Privacy-preserving RFID Authentication Scheme for Distributed IoT Infrastructure with Secure Localization Services for Smart City Environment," Future Generation Computer Systems, vol. 83, pp. 629–637, 2018.

[67] S.-C. Cha, M.-S. Chuang, K.-H. Yeh, Z.-J. Huang, and C. Su, "A User-friendly Privacy Framework for Users to Achieve Consents with Nearby BLE Devices," IEEE Access, vol. 6, pp. 20 779–20 787, 2018.

[68] P. Yu, J. Cao, M. Ma, H. Li, B. Niu, and F. Li, "Quantum-Resistance Authentication and Data Transmission Scheme for NB-IoT in 3GPP 5G Networks," in 2019 IEEE Wireless Communications and Networking Conference (WCNC). IEEE, 2019, pp. 1–7.

[69] S. Lal, T. Taleb, and A. Dutta, "NFV: Security Threats and Best Practices," IEEE Communications Magazine, vol. 55, no. 8, pp. 211–217, 2017.

[70] D. Fang, Y. Qian, and R. Q. Hu, "Security for 5G Mobile Wireless Networks," IEEE Access, vol. 6, pp. 4850–4874, 2018.

[71] B. Jaeger, "Security Orchestrator: Introducing a Security Orchestrator In the Context of The Etsi NFV Reference Architecture," in Trustcom/BigDataSE/ISPA, 2015 IEEE, vol. 1. IEEE, 2015, pp. 1255–1260.

[72] R. Guo, H. Shi, Q. Zhao, and D. Zheng, "Secure Attribute-based Signature Scheme with Multiple Authorities for Blockchain in Electronic Health Records Systems," IEEE access, vol. 6, pp. 11 676–11 686, 2018.

[73] J. Kim, D. Kim, and S. Choi, "3GPP SA2 Architecture and Functions for 5G Mobile Communication System," ICT Express, vol. 3, no. 1, pp. 1–8, 2017.

[74] S. Chen, R. Ma, H.-H. Chen, H. Zhang, W. Meng, and J. Liu, "Machine-to-Machine Communications in Ultra-Dense Networks—-A Survey," IEEE Communications Surveys & Tutorials, vol. 19, no. 3, pp. 1478–1503, 2017.

[75] X. Lu, D. Niyato, N. Privault, H. Jiang, and P. Wang, "Managing Physical Layer Security in Wireless Cellular Networks: A Cyber Insurance Approach," IEEE Journal on Selected Areas in Communications, 2018.

[76] S. Wang, Y. Zhao, J. Xu, J. Yuan, and C.-H. Hsu, "Edge Server Placement in Mobile Edge Computing," Journal of Parallel and Distributed Computing, 2018.

[77] A. Rahman, E. Hassanain, and M. S. Hossain, "Towards a Secure Mobile Edge Computing Framework for Hajj," IEEE Access, vol. 5, pp. 11 768–11 781, 2017.

[78] H.-M. Wang, T.-X. Zheng, J. Yuan, D. Towsley, and M. H. Lee, "Physical Layer Security in Heterogeneous Cellular Networks," IEEE Transactions on Communications, vol. 64, no. 3, pp. 1204–1219, 2016.

[79] K. Xiao, W. Li, M. Kadoch, and C. Li, "On the Secrecy Capacity of 5G MmWave Small Cell Networks," IEEE Wireless Communications, vol. 25, no. 4, pp. 47–51, 2018.

[80] C.-L. Chen, M.-L. Chiang, H.-C. Hsieh, C.-C. Liu, and Y.-Y. Deng, "A Lightweight Mutual Authentication with Wearable Device in Location-Based Mobile Edge Computing," WIRELESS PERSONAL COMMUNICATIONS, 2020.

[81] O. N. Hamoud, T. Kenaza, and Y. Challal, "Security in Device-to-Device Communications: A Survey," IET Networks, vol. 7, no. 1, pp. 14–22, 2017.

[82] P. Hao, X. Wang, and W. Shen, "A Collaborative PHY-Aided Technique for End-to-End IoT Device Authentication," IEEE Access, vol. 6, pp. 42 279–42 293, 2018.

[83] Y. Gao, D. C. Ranasinghe, S. F. Al-Sarawi, O. Kavehei, and D. Abbott, "Emerging Physical Unclonable Functions with Nanotechnology," IEEE access, vol. 4, pp. 61–80, 2016.

[84] C. Marchand, L. Bossuet, U. Mureddu, N. Bochard, A. Cherkaoui, and V. Fischer, "Implementation and Characterization of a Physical Unclonable Function for IoT: A Case Study with the TERO-PUF," IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 37, no. 1, pp. 97–109, 2018.

[85] J. Zhang, X. Tan, X. Wang, A. Yan, and Z. Qin, "T2FA: Transparent Two-factor Authentication," IEEE Access, vol. 6, pp. 32 677–32 686, 2018.

[86] N. Islam, S. Das, and Y. Chen, "On-device Mobile Phone Security Exploits Machine Learning," IEEE Pervasive Computing, no. 2, pp. 92–96, 2017.

[87] B. Krupp, N. Sridhar, and W. Zhao, "SPE: Security and Privacy Enhancement Framework for Mobile Devices," IEEE Transactions on Dependable and Secure Computing, vol. 14, no. 4, pp. 433–446, 2017.

[88] H. Gupta, S. Mondal, R. Majumdar, N. S. Ghosh, S. S. Khan, N. E. Kwanyu, and V. P. Mishra, "Impact of Side Channel Attack in Information Security," in 2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE). IEEE, 2019, pp. 291–295.

[89] M. Sabbagh, Y. Fei, T. Wahl, and A. A. Ding, "SCADET: A Side-Channel Attack Detection Tool for Tracking Prime+ Probe," in Proceedings of the International Conference on Computer-Aided Design, 2018, pp. 1–8.

[90] M. Mushtaq, A. Akram, M. K. Bhatti, R. N. B. Rais, V. Lapotre, and G. Gogniat, "Run-time Detection of Prime+ Probe Side-Channel Attack on AES Encryption Algorithm," in 2018 Global Information Infrastructure and Networking Symposium (GIIS). IEEE, 2018, pp. 1–5.

[91] X. Wang, Q. Zhou, J. Harer, G. Brown, S. Qiu, Z. Dou, J. Wang, A. Hinton, C. A. Gonzalez, and P. Chin, "Deep Learning-based Classification and Anomaly Detection of Side-Channel Signals," in Cyber Sensing 2018, vol. 10630. International Society for Optics and Photonics, 2018, p. 1063006.

[92] A. R. Javed, M. O. Beg, M. Asim, T. Baker, and A. H. Al-Bayatti, "AlphaLogger: Detecting Motion-based Side-Channel Attack using Smartphone Keystrokes," Journal of Ambient Intelligence and Humanized Computing, pp. 1–14, 2020.

[93] B. S. Ainapure, D. Shah, and A. A. Rao, "Understanding Perception of Cache-based Side-Channel Attack on Cloud Environment," in Progress in intelligent computing techniques: Theory, practice, and applications. Springer, 2018, pp. 9–21.

[94] S. Dalal and S. Devi, "Security Framework Against Denial of Service Attacks in Wireless Mesh Network Networks," International Journal of Computer Networks and Communications Security, vol. 4, no. 8, p. 237, 2016.

[95] H. Ko, K. Lim, J. Oh, and J.-K. K. Rhee, "Informatic Analysis for Hidden Pulse Attack Exploiting Spectral Characteristics of Optics in Plug-and-Play Quantum Key Distribution System," Quantum Information Processing, vol. 15, no. 10, pp. 4265–4282, 2016.

[96] E. Gündüzhan and K. D. Brown, "Narrowband Satellite Communications: Challenges and Emerging Solutions," John Hopkins APL technical Digest, 2015, vol. 33, 2015.

[97] ETSI, "Network Functions Virtualisation (NFV) Security: Report on Use Cases and Technical Approaches for Multi-layer Host Administration," ETSI White Paper, 2015, last accessed 16 May 2019. [Online]. Available: https://www.etsi.org/deliver/etsi_gs/NFV-SEC/001_099/009/01.01.01_60/gs_nfv-sec009v010101p.pdf

[98] ETSI-NFV-ISG, "Network Functions Virtualisation (NFV) Security: Cataloguing Security Features in Management Software," ETSI White Paper, 2015, last accessed 16 May 2019. [Online]. Available: https://www.etsi.org/deliver/etsi_gs/NFV-SEC/001_099/002/01.01.01_60/gs_NFV-SEC002v010101p.pdf

[99] T. Garfinkel, M. Rosenblum et al., "A Virtual Machine Introspection Based Architecture for Intrusion Detection," in Network and Distributed System Security Symposium, vol. 3, no. 2003, 2003, pp. 191–206.

[100] I. Farris, J. B. Bernabé, N. Toumi, D. Garcia-Carrillo, T. Taleb, A. Skarmeta, and B. Sahlin, "Towards Provisioning of SDN/NFV-based Security Enablers for Integrated Protection of IoT Systems," in 2017 IEEE Conference on Standards for Communications and Networking (CSCN). IEEE, 2017, pp. 169–174.

[101] Z. Hu and Y. Yin, "A Framework for Security on Demand," in 13th International Wireless Communications and Mobile Computing Conference (IWCMC). IEEE, 2017, pp. 378–383.

[102] I. Sfyrakis and T. Gross, "A Survey on Hardware Approaches for Remote Attestation in Network Infrastructures," arXiv preprint arXiv:2005.12453, 2020.

[103] T. Zhang, Y. Zhang, and R. B. Lee, "Cloudradar: A Real-time Side-channel Attack Detection System in Clouds," in International Symposium on Research in Attacks, Intrusions, and Defenses. Springer, 2016, pp. 118–140.

[104] R. Solozabal, A. Sanchoyerto, E. Atxutegi, B. Blanco, J. O. Fajardo, and F. Liberal, "Exploitation of Mobile Edge Computing in 5G Distributed Mission-Critical Push-to-Talk Service Deployment," IEEE Access, vol. 6, pp. 37 665–37 675, 2018.

[105] X. Costa-Perez, A. Garcia-Saavedra, X. Li, T. Deiss, O. Delgado, A. Di Giglio, A. Mourad et al., "5G-Crosshaul: an SDN/NFV Integrated Fronthaul/backhaul Transport Network Architecture," IEEE Wireless Communications, 2017.

[106] T. X. Tran, A. Hajisami, P. Pandealjhuaniy, and D. Pompili, "Collaborative Mobile Edge Computing in 5G Networks: New Paradigms, Scenarios, and Challenges," IEEE Communications Magazine, vol. 55, no. 4, pp. 54–61, April 2017.

[107] European Telecommunications Standards Institute. Available:https://www.etsi.org/. [Online; accessed March 18, 2018].

[108] M. Liyanage, I. Ahmad, M. Ylianttila, A. Gurtov, A. B. Abro, and E. M. de Oca, "Leveraging LTE Security with SDN and NFV," in 2015 IEEE 10th International Conference on Industrial and Information Systems (ICIIS). IEEE, 2015, pp. 220–225.

[109] M. Liyanage, A. B. Abro, M. Ylianttila, and A. Gurtov, "Opportunities and Challenges of Software-Defined Mobile Networks in Network Security," IEEE Security & Privacy, vol. 14, no. 4, pp. 34–44, 2016.

[110] B. Han, V. Gopalakrishnan, L. Ji, and S. Lee, "Network Function Virtualization: Challenges and Opportunities for Innovations," IEEE Communications Magazine, vol. 53, no. 2, pp. 90–97, 2015.

[111] K. Leach, F. Zhang, and W. Weimer, "Scotch: Combining Software Guard Extensions and System Management Mode to Monitor Cloud Resource usage," in International Symposium on Research in Attacks, Intrusions, and Defenses. Springer, 2017, pp. 403–424.

[112] R. Wojtczuk, "Poacher Turned Gamekeeper: Lessons Learned from Eight Years of Breaking Hypervisors," Black Hat USA, 2014.

[113] A. Aljuhani and T. Alharbi, "Virtualized Network Functions Security Attacks and Vulnerabilities," in 7th Annual Computing and Communication Workshop and Conference (CCWC). IEEE, 2017, pp. 1–4.

[114] Z. Yan, P. Zhang, and A. V. Vasilakos, "A Security and Trust Framework for Virtualized Networks and Software-Defined Networking," Security and Communication Networks, vol. 9, no. 16, pp. 3059–3069, 2016.

[115] M. Pattaranantakul, Y. Tseng, R. He, Z. Zhang, and A. Meddahi, "A First Step Towards Security Extension for NFV Orchestrator," in Proceedings of the ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization. ACM, 2017, pp. 25–30.

[116] M. Pattaranantakul, R. He, A. Meddahi, and Z. Zhang, "SecMANO: Towards Network Functions Virtualization (NFV) Based Security Management and Oorchestration," in Trustcom/BigDataSE/I SPA, 2016 IEEE. IEEE, 2016, pp. 598–605.

[117] L. R. Battula, "Network Security Function Virtualization (NSFV) Towards Cloud Computing With NFV Over Openflow Infrastructure: Challenges and Novel Approaches," in Advances in Computing, Communications and Informatics (ICACCI, 2014 International Conference on. IEEE, 2014, pp. 1622–1628.

[118] C. Lorenz, D. Hock, J. Scherer, R. Durner, W. Kellerer, S. Gebert, N. Gray, T. Zinner, and P. Tran-Gia, "An SDN/NFV-Enabled Enterprise Network Architecture Offering Fine-Grained Security Policy Enforcement." IEEE communications magazine, vol. 55, no. 3, pp. 217–223, 2017.

[119] C. Basile, A. Lioy, C. Pitscheider, F. Valenza, and M. Vallini, "A Novel Approach for Integrating Security Policy Enforcement With Dynamic Network virtualization," in Network Softwarization (NetSoft), 2015 1st IEEE Conference on. IEEE, 2015, pp. 1–5.

[120] E. Felstaine, O. Hermoni, and N. Sandlerman, "System, Method, and Computer Program for Managing Security In a Network Function Virtualization (NFV) Based Communication Network," Oct. 4 2016, uS Patent 9,460,286.

[121] N. J. Zaidenberg, M. Kiperberg, R. B. Yehuda, R. Leon, A. Algawi, and A. Resh, "Hypervisor Memory Introspection and Hypervisor Based Malware Honeypot," in International Conference on Information Systems Security and Privacy. Springer, 2019, pp. 317–334.

[122] J. Ni, X. Lin, and X. S. Shen, "Efficient and Secure Service-Oriented Authentication Supporting Network Slicing for 5G-Enabled IoT," IEEE Journal on Selected Areas in Communications, vol. 36, no. 3, pp. 644–657, 2018.

[123] R. Ravindran, A. Chakraborti, S. O. Amin, A. Azgin, and G. Wang, "5G-ICN: Delivering ICN Services Over 5G Using Network Slicing," IEEE Communications Magazine, vol. 55, no. 5, pp. 101–107, 2017.

[124] S. Zhang, "An Overview of Network Slicing for 5G," IEEE Wireless Communications, 2019.

[125] R. Harel and S. Babbage, "5G Security Recommendations Package 2: Network Slicing," 2016, last accessed 16 May 2019. [Online]. Available: https://www.ngmn.org/fileadmin/user_upload/160429_NGMN_5G_Security_Network_Slicing_v1_0.pdf

[126] R. Wen, G. Feng, J. Tang, T. Q. Quek, G. Wang, W. Tan, and S. Qin, "On Robustness of Network Slicing for Next-Generation Mobile Networks," IEEE Transactions on Communications, vol. 67, no. 1, pp. 430–444, 2019.

[127] H. Hantouti, N. Benamar, T. Taleb, and A. Laghrissi, "Traffic Steering for Service Function Chaining," IEEE Communications Surveys & Tutorials, 2018.

[128] K. Fysarakis, N. E. Petroulakis, A. Roos, K. Abbasi, P. Vizarreta, G. Petropoulos, E. Sakic, G. Spanoudakis, and I. Askoxylakis, "A Reactive Security Framework for Operational Wind Parks Using Service Function Chaining," in Computers and Communications (ISCC), 2017 IEEE Symposium on. IEEE, 2017, pp. 663–668.

[129] G. Li, H. Zhou, B. Feng, G. Li, T. Li, Q. Xu, and W. Quan, "Fuzzy Theory Based Security Service Chaining for Sustainable Mobile-Edge Computing," Mobile Information Systems, vol. 2017, 2017.

[130] A. Machen, S. Wang, K. K. Leung, B. J. Ko, and T. Salonidis, "Live Service Migration in Mobile Edge Clouds," IEEE Wireless Communications, vol. 25, no. 1, pp. 140–147, 2018.

[131] J.-h. Lee, "Secure Authentication with Dynamic Tunneling in Distributed IP Mobility Management," IEEE Wireless Communications, vol. 23, no. 5, pp. 38–43, 2016.

[132] D. Shin, V. Sharma, J. Kim, S. Kwon, and I. You, "Secure and Efficient Protocol for Route Optimization in PMIPv6-based Smart Home IoT Networks," IEEE Access, vol. 5, pp. 11 100–11 117, 2017.

[133] J. Tang, M. Dabaghchian, K. Zeng, and H. Wen, "Impact of Mobility on Physical Layer Security Over Wireless Fading Channels," IEEE Transactions on Wireless Communications, vol. 17, no. 12, pp. 7849–7864, 2018.

[134] Y. Siriwardhana, P. Porambage, M. Liyanage, J. S. Walia, M. Matinmikko-Blue, and M. Ylianttila, "Micro-Operator driven Local 5G Network Architecture for Industrial Internet," in IEEE Wireless Communications and Networking Conference (WCNC) 2019. IEEE, 2019, pp. 1–8.

[135] A. Braeken, M. Liyanage, P. Kumar, and J. Murphy, "Novel 5G Authentication Protocol to Improve the Resistance Against Active Attacks and Malicious Serving Networks," IEEE Access, vol. 7, pp. 64 040–64 052, 2019.

[136] Y. Siriwardhana, P. Porambage, M. Ylianttila, and M. Liyanage, "Performance analysis of local 5g operator architectures for industrial internet," IEEE Internet of Things Journal, vol. 7, no. 12, pp. 11 559–11 575, 2020.

[137] F. Giust, G. Verin, K. Antevski, J. Chou, Y. Fang, W. Featherstone, F. Fontes, D. Frydman, A. Li, A. Manzalini et al., "MEC deployments in 4G and evolution towards 5G," ETSI White Paper, vol. 24, pp. 1–24, 2018.

[138] B. Rodrigues, T. Bocek, A. Lareida, D. Hausheer, S. Rafati, and B. Stiller, "A Blockchain-based Architecture for Collaborative DDoS Mitigation with Smart Contracts," in IFIP International Conference on Autonomous Infrastructure, Management and Security. Springer, Cham, 2017, pp. 16–29.

[139] M. V. De Assis, A. H. Hamamoto, T. Abrão, and M. L. Proença, "A Game Theoretical based System using Holt-winters and Genetic Algorithm with Fuzzy Logic for DoS/DDoS Mitigation on SDN Networks," IEEE Access, vol. 5, pp. 9485–9496, 2017.

[140] J. M. Vidal, A. L. S. Orozco, and L. J. G. Villalba, "Adaptive Artificial Immune Networks for Mitigating DoS Flooding Attacks," Swarm and Evolutionary Computation, vol. 38, pp. 94–108, 2018.

[141] K. Bhardwaj, J. C. Miranda, and A. Gavrilovska, "Towards IoT-DDoS prevention using edge computing," in {USENIX} Workshop on Hot Topics in Edge Computing (HotEdge 18), 2018.

[142] B. Huang, Z. Li, P. Tang, S. Wang, J. Zhao, H. Hu, W. Li, and V. Chang, "Security Modeling and Efficient Computation Offloading for Service Workflow in Mobile Edge Computing," Future Generation Computer Systems, vol. 97, pp. 755–774, 2019.

[143] J. Xu and J. Yao, "Exploiting Physical-layer Security for Multiuser Multicarrier Computation Offloading," IEEE Wireless Communications Letters, vol. 8, no. 1, pp. 9–12, 2018.

[144] J. Xu, L. Chen, K. Liu, and C. Shen, "Designing Security-aware Incentives for Computation Offloading via Device-to-Device Communication," IEEE Transactions on Wireless Communications, vol. 17, no. 9, pp. 6053–6066, 2018.

[145] T. Bai, J. Wang, Y. Ren, and L. Hanzo, "Energy-efficient Computation Offloading for Secure UAV-edge-computing Systems," IEEE Transactions on Vehicular Technology, vol. 68, no. 6, pp. 6074–6087, 2019.

[146] I. A. Elgendy, W. Zhang, Y.-C. Tian, and K. Li, "Resource Allocation and Computation Offloading with Data Security for Mobile Edge Computing," Future Generation Computer Systems, vol. 100, pp. 531–541, 2019.

[147] Z. Wang, D. Tao, and Z. Lin, "Dynamic Virtualization Security Service Construction Strategy for Software Defined Networks," in 2016 12th International Conference on Mobile Ad-Hoc and Sensor Networks (MSN). IEEE, 2016, pp. 139–144.

[148] D. Sun, J. Zhang, W. Fan, T. Wang, C. Liu, and W. Huang, "SPLM: Security Protection of Live Virtual Machine Migration in Cloud Computing," in Proceedings of the 4th ACM International Workshop on Security in Cloud Computing, 2016, pp. 2–9.

[149] R. Yasrab, "Mitigating Docker Security Issues," arXiv preprint arXiv:1804.05039, 2018.

[150] Z. Jian and L. Chen, "A Defense Method Against Docker Escape Attack," in Proceedings of the 2017 International Conference on Cryptography, Security and Privacy, 2017, pp. 142–146.

[151] S. Han, X. Xu, S. Fang, Y. Sun, Y. Cao, X. Tao, and P. Zhang, "Energy Efficient Secure Computation Offloading in NOMA-based mMTC Networks for IoT," IEEE Internet of Things Journal, vol. 6, no. 3, pp. 5674–5690, 2019.

[152] Y. Khettab, M. Bagaa, D. L. C. Dutra, T. Taleb, and N. Toumi, "Virtual Security as a Service for 5G Verticals," in 2018 IEEE Wireless Communications and Networking Conference (WCNC). IEEE, 2018, pp. 1–6.

[153] T. Bui, "Analysis of Docker Security," arXiv preprint arXiv:1501.02967, 2015.

[154] OpenFogConsortium et al., "OpenFog Reference Architecture for Fog Computing," OpenFog Architecture Working Group, 2017, last accessed 16 May 2019. [Online]. Available: https://www.openfogconsortium.org/wp-content/uploads/OpenFog_Reference_Architecture_2_09_17-FINAL.pdf

[155] S. N. Shirazi, A. Gouglidis, A. Farshad, and D. Hutchison, "The Extended Cloud: Review and Analysis of Mobile Edge Computing and Fog From a Security and Resilience Perspective," IEEE Journal on Selected Areas in Communications, vol. 35, no. 11, pp. 2586–2595, 2017.

[156] A. Alwarafy, K. A. Al-Thelaya, M. Abdallah, J. Schneider, and M. Hamdi, "A Survey on Security and Privacy Issues in Edge Computing-Assisted Internet of Things," IEEE Internet of Things Journal, 2020.

[157] M. Liyanage, J. Salo, A. Braeken, T. Kumar, S. Seneviratne, and M. Ylianttila, "5G Privacy: Scenarios and Solutions," in 2018 IEEE 5G World Forum (5GWF). IEEE, 2018, pp. 197–203.

[158] T. He, E. N. Ciftcioglu, S. Wang, and K. S. Chan, "Location Privacy in Mobile Edge Clouds: A Chaff-based Approach," IEEE Journal on Selected Areas in Communications, vol. 35, no. 11, pp. 2625–2636, 2017.

[159] X. He, J. Liu, R. Jin, and H. Dai, "Privacy-aware Offloading in Mobile-Edge Computing," in GLOBECOM 2017-2017 IEEE Global Communications Conference. IEEE, 2017, pp. 1–6.

[160] X. He, R. Jin, and H. Dai, "Deep PDS-Learning for Privacy-Aware Offloading in MEC-Enabled IoT," IEEE Internet of Things Journal, 2018.

[161] J. Chi, E. Owusu, X. Yin, T. Yu, W. Chan, Y. Liu, H. Liu, J. Chen, S. Sim, V. Iyengar et al., "Privacy Partition: A Privacy-Preserving Framework for Deep Neural Networks in Edge Networks," in 2018 IEEE/ACM Symposium on Edge Computing (SEC). IEEE, 2018, pp. 378–380.

[162] M. Du, K. Wang, Y. Chen, X. Wang, and Y. Sun, "Big Data Privacy Preserving in Multi-Access Edge Computing for Heterogeneous Internet of Things," IEEE Communications Magazine, vol. 56, no. 8, pp. 62–67, 2018.

[163] X. Jia, D. He, N. Kumar, and K.-K. R. Choo, "A Provably Secure and Efficient Identity-Based Anonymous Authentication Scheme for Mobile Edge Computing," IEEE Systems Journal, 2019.

[164] X. Li, S. Liu, F. Wu, S. Kumari, and J. J. Rodrigues, "Privacy Preserving Data Aggregation Scheme for Mobile Edge Computing Assisted IoT Applications," IEEE Internet of Things Journal, 2018.

[165] P. Zhang, M. Durresi, and A. Durresi, "Mobile Privacy Protection Enhanced with Multi-Access Edge Computing," in 2018 IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA). IEEE, 2018, pp. 724–731.

[166] K. Gai, Y. Wu, L. Zhu, L. Xu, and Y. Zhang, "Permissioned Blockchain and Edge Computing Empowered Privacy-preserving Smart Grid Networks," IEEE Internet of Things Journal, 2019.

[167] EUGDPR. (2018) European General Data Protection Regulation. Last accessed May 16, 2019. [Online]. Available: https://eugdpr.org/

[168] S. Alharby, N. Harris, A. Weddell, and J. Reeve, "The Security Trade-offs in Resource Constrained Nodes for IoT Application," International Journal of Electrical, Computer, Energetic, Electronic and Communication Engineering, vol. 12, no. 1, pp. 52–59, 2018.

[169] U. A. Kashif, Z. A. Memon, S. Siddiqui, A. R. Balouch, and R. Batra, "Architectural Design of Trusted Platform for IaaS Cloud Computing," in Cloud Security: Concepts, Methodologies, Tools, and Applications. IGI Global, 2019, pp. 393–411.

[170] W. Qiang, G. Xu, W. Dai, D. Zou, and H. Jin, "CloudVMI: A Cloud-oriented Writable Virtual Machine Introspection," IEEE Access, vol. 5, pp. 21 962–21 976, 2017.

[171] T. Roberts, M. Wray, and N. Edwards, "Virtual Machine Introspection," Aug. 4 2016, uS Patent App. 15/021,032.

[172] R. A. Mixer, "Security Event Detection through Virtual Machine Introspection," Aug. 18 2016, uS Patent App. 14/622,224.

[173] M. A. Kumara and C. Jaidhar, "Leveraging Virtual Machine Introspection with Memory Forensics to Detect and Characterize Unknown Malware using Machine Learning Techniques at Hypervisor," Digital Investigation, vol. 23, pp. 99–123, 2017.

[174] M. Liyanage, M. Ylianttila, and A. Gurtov, "Software Defined VPLS Architectures: Opportunities and Challenges," in 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC). IEEE, 2017, pp. 1–7.

[175] ——, "Improving the Tunnel Management Performance of Secure VPLS Architectures with SDN," in 2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC). IEEE, 2016, pp. 530–536.

[176] ——, "Fast Transmission Mechanism for Secure VPLS Architectures," in 2017 IEEE International Conference on Computer and Information Technology (CIT). IEEE, 2017, pp. 192–196.

[177] V. N. Imrith, P. Ranaweera, R. A. Jugurnauth, and M. Liyanage, "Dynamic orchestration of security services at fog nodes for 5g iot," in ICC 2020-2020 IEEE International Conference on Communications (ICC). IEEE, 2020, pp. 1–6.

[178] M. F. Novak, Y. A. Samsonov, and J. Wu, "System Integrity Using Attestation for Virtual Trusted Platform Module," Apr. 4 2019, uS Patent App. 15/722,439.

[179] D. E. Turissini, W. R. Carlisle, and B. G. Tregub, "Remote Attestation of a Security Module's Assurance Level," Jan. 24 2019, uS Patent App. 16/039,335.

[180] D. Sattar and A. Matrawy, "Towards Secure Slicing: Using Slice Isolation to Mitigate DDoS Attacks on 5G Core Network Slices," in 2019 IEEE Conference on Communications and Network Security (CNS). IEEE, 2019, pp. 82–90.

[181] J. Ordonez-Lucena, P. Ameigeiras, D. Lopez, J. J. Ramos-Munoz, J. Lorca, and J. Folgueira, "Network Slicing for 5G with SDN/NFV: Concepts, Architectures, and Challenges," IEEE Communications Magazine, vol. 55, no. 5, pp. 80–87, 2017.

[182] T. P. Stammers and M. D. Geller, "Network Slice Selection in a Mobile Network," Jan. 24 2019, uS Patent App. 15/652,246.

[183] J. Lee, S. Jung, and S. Kim, "Method and Apparatus for Applying Assistance Information for Traffic Steering in Wireless Communication System," Jan. 29 2019, uS Patent App. 10/194,357.

[184] I. S. Gandhi and J. Henry, "Traffic Steering in a Heterogeneous Network," Jan. 24 2019, uS Patent App. 15/792,602.

[185] P. Ranaweera, V. N. Imrith, M. Liyanag, and A. D. Jurcut, "Security as a service platform leveraging multi-access edge computing infrastructure provisions," in ICC 2020-2020 IEEE International Conference on Communications (ICC). IEEE, 2020, pp. 1–6.

[186] J. J. A. Rasanen, "Charging and Control of Edge Services," Feb. 25 2020, uS Patent 10,574,833.

[187] D. Sabella, N. M. Smith, N. Oliver, K. A. Doshi, S. Prabhakaran, M. Filippou, and F. G. Bernat, "Multi-Access Edge Computing (MEC) Billing and Charging Tracking Enhancements," May 23 2019, uS Patent App. 16/235,894.

[188] F. Kemmer, C. Reich, M. Knahl, and N. Clarke, "Software Defined Privacy," in 2016 IEEE International Conference on Cloud Engineering Workshop (IC2EW). IEEE, 2016, pp. 25–29.

[189] A. Cavoukian, "Privacy by Design [Leading Edge]," IEEE Technology and Society Magazine, vol. 31, no. 4, pp. 18–19, 2012.

[190] A. Cavoukian et al., "Privacy by Design: The 7 Foundational Principles," Information and Privacy Commissioner of Ontario, Canada, vol. 5, 2009.

[191] P. Yang and K. Gopalan, "System and Method for Security and Privacy Aware Virtual Machine Checkpointing," Jun. 30 2015, uS Patent 9,069,782.

[192] P. Porambage, T. Kumar, M. Liyanage, J. Partala, L. Lovén, M. Ylianttila, and T. Seppänen. (2019) Sec-EdgeAI: AI for Edge Security Vs Security for Edge AI. Last accessed May 16, 2019. [Online]. Available: https://www.researchgate.net/publication/330838792_Sec-EdgeAI_AI_for_Edge_Security_Vs_Security_for_Edge_AI

[193] ——. (2019) Sec-EdgeAI: A Vision for using Artificial Intelligence for Securing the Edge. Last accessed May 16, 2019. [Online]. Available: https://www.researchgate.net/publication/330620630_EdgeAI_A_Vision_for_Privacy-preserving_Machine_Learning_on_the_Edge

[194] R. S. Sutton and A. G. Barto, Reinforcement Learning: An Introduction. MIT press, 2018.

[195] B. Cao, L. Zhang, Y. Li, D. Feng, and W. Cao, "Intelligent Offloading in Multi-Access Edge Computing: A State-of-the-Art Review and Framework," IEEE Communications Magazine, vol. 57, no. 3, pp. 56–62, 2019.

[196] L. Xiao, X. Wan, X. Lu, Y. Zhang, and D. Wu, "IoT Security Techniques based on Machine Learning: How do IoT Devices Use AI to Enhance Security?" IEEE Signal Processing Magazine, vol. 35, no. 5, pp. 41–49, 2018.

[197] P. K. Das, D. Ghosh, P. Jagtap, A. Joshi, and T. Finin, "Preserving User Privacy and Security in Context-aware Mobile Platforms," in Censorship, Surveillance, and Privacy: Concepts, Methodologies, Tools, and Applications. IGI Global, 2019, pp. 1203–1230.

[198] H. Lin, Z. Yan, and Y. Fu, "Adaptive Security-related Data Collection with Context Awareness," Journal of Network and Computer Applications, vol. 126, pp. 88–103, 2019.

[199] K. J. Roach, A. Hrybyk, J. S. Morrison, K. M. Kauffman, E. B. Jones, M. Lohrum, and K. R. Good, "Method and Apparatus for Context Aware Mobile Security," May 5 2015, uS Patent 9,027,076.

[200] C. Richardson. (2014, Mar) What are Microservices? Last accessed May 16, 2019. [Online]. Available: https://microservices.io/

[201] Y. Sun, S. Nanda, and T. Jaeger, "Security-as-a-Service for Microservices-based Cloud Applications," in 2015 IEEE 7th International Conference on Cloud Computing Technology and Science (CloudCom). IEEE, 2015, pp. 50–57.

[202] M. Villari, M. Fazio, S. Dustdar, O. Rana, and R. Ranjan, "Osmotic Computing: A New Paradigm for Edge/Cloud Integration," IEEE Cloud Computing, vol. 3, no. 6, pp. 76–83, 2016.

[203] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On Blockchain and its Integration with IoT: Challenges and Opportunities," Future Generation Computer Systems, vol. 88, pp. 173–190, 2018.

[204] T. Hewa, M. Ylianttila, and M. Liyanage, "Survey on blockchain based smart contracts: Applications, opportunities and challenges," Journal of Network and Computer Applications, p. 102857, 2020.
[205] C. Esposito, A. De Santis, G. Tortora, H. Chang, and K.-K. R. Choo, "Blockchain: A Panacea for Healthcare Cloud-based Data Security and Privacy?" IEEE Cloud Computing, vol. 5, no. 1, pp. 31–37, 2018.
[206] A. Manzoor, A. Braeken, S. S. Kanhere, M. Ylianttila, and M. Liyanage, "Proxy re-encryption enabled secure and anonymous iot data sharing platform based on blockchain," Journal of Network and Computer Applications, p. 102917, 2020.
[207] Y. Jiao, P. Wang, D. Niyato, and K. Suankaewmanee, "Auction Mechanisms in Cloud/Fog Computing Resource Allocation for Public Blockchain Networks," IEEE Transactions on Parallel and Distributed Systems, 2019.
[208] T. Kumar, E. Harjula, M. Ejaz, A. Manzoor, P. Porambage, I. Ahmad, M. Liyanage, A. Braeken, and M. Ylianttila, "Blockedge: blockchain-edge framework for industrial iot networks," IEEE Access, vol. 8, pp. 154 166–154 185, 2020.

Pasika Ranaweera is currently pursuing his PhD studies in School of Computer Science, University College Dublin, Ireland. He obtained his Bachelor Degree in Electrical and Information Engineering in 2010 from University of Ruhuna, Sri Lanka and Master's Degree in Information and Communication Technology (ICT) in 2013 from University of Agder, Norway. Pasika is focused on enhancing the security measures in Multi-access Edge Computing (MEC) and Internet of Things (IoT) integration. His research directives extend to the areas lightweight security protocols, 5G and MEC integration technologies, Privacy preservation techniques, and IoT security. https://ucdcs-research.ucd.ie/phd-student/pasika-sashmal-ranaweera/

Anca D. Jurcut is an Assistant Professor in the UCD School of Computer Science since 2015. She received a BSc in Computer Science and Mathematics from West University of Timisoara, Romania in 2007 and a PhD in Security Engineering from the University of Limerick (UL) in 2013 funded by the Irish Research Council for Science Engineering and Technology. She worked as a postdoctoral researcher at UL as a member of the Data Communication Security Laboratory and as a Software Engineer in IBM in Dublin in the area of data security and formal verification. Dr. Jurcut research interests include Security Protocols Design and Analysis, Automated Techniques for Formal Verification, Network Security, Attack Detection and Prevention Techniques, Security for the Internet of Things, and Applications of Blockchain for Security and Privacy. Dr. Jurcut has several key contributions in research focusing on detection and prevention techniques of attacks over networks, the design and analysis of security protocols, automated techniques for formal verification, and security for mobile edge computing (MEC). https://people.ucd.ie/anca.jurcut

Madhusanka Liyanage (M.Eng, M. Sc, Dr.Sc) is currently an assistant professor/ad astra fellow at University College Dublin, Ireland and an adjunct professor at the University of Oulu, Finland. He received his B.Sc. degree (First Class Honours) 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 Doctor of Technology degree in communication engineering from the University of Oulu, Oulu, Finland, in 2016. From 2011 to 2012, he worked a Research Scientist at the I3S Laboratory and Inria, Shopia Antipolis, France. He was also a recipient of prestigious Marie Skłodowska-Curie Actions Individual Fellowship during 2018-2020. During 2015-2018, he has been a Visiting Research Fellow at the CSIRO, Australia, the Infolabs21, Lancaster University, U.K., Computer Science and Engineering, The University of New South Wales, Australia, School of IT, University of Sydney, Australia, LIP6, Sorbonne University, France and Computer Science and Engineering, The University of Oxford, U.K. He is also a senior member of IEEE. In 2020, he has received "2020 IEEE ComSoc Outstanding Young Researcher" award by IEEE ComSoc EMEA.

He has co-authored over 100 publications including three edited books with Wiley and one patent. Moreover, He has received two best Paper Awards in the areas of SDMN security (at NGMAST 2015) and 5G Security (at IEEE CSCN 2017). Additionally, he has been awarded two research grants and 19 other prestigious awards/scholarships during his research career. Liyanage has worked for more than twelve EU, international and national projects in ICT domain. He held responsibilities as a leader of work packages in several projects including SIGMONA and Naked approach projects. Currently, he is the Finnish national coordinator for EU COST Action CA15127 on resilient communication services and also serving as management committee member for three other EU COST action projects namely EU COST Action IC1301, IC1303, CA15107 and CA16226. Liyanage has over seven years' experience in research project management, research group leadership, research project proposal preparation, project progress documentation and graduate student co-supervision/mentoring, skills. For last four years, 2015, 2016, 2017 and 2018, he won the Best Researcher Award at the Centre for Wireless Communications, University of Oulu for his excellent contribution in project management and project proposal preparation. In 2020, he was selected as the best researcher at School of Computer Science, University College Dublin, Ireland. Additionally, two of the research projects (MEVICO and SIGMONA projects) received the CELTIC Excellence and CELTIC Innovation Awards in 2013, 2017 and 2018 respectively.

Dr. Liyanage's research interests are 5G, SDN, IoT, Blockchain, MEC, mobile and virtual network security. More Info: :http://madhusanka.com