# Realizing Multi-Access Edge Computing Feasibility: Security Perspective

**Conference Paper** · October 2019

CITATIONS
0

READS
221

**3 authors:**

Pasika S Ranaweera
University of Ruhuna
**9** PUBLICATIONS **31** CITATIONS
SEE PROFILE

Anca D Jurcut
University College Dublin
**22** PUBLICATIONS **63** CITATIONS
SEE PROFILE

Madhusanka Liyanage
University College Dublin
**92** PUBLICATIONS **617** CITATIONS
SEE PROFILE

# Realizing Multi-Access Edge Computing Feasibility: Security Perspective

Pasika Ranaweera*, Anca Delia Jurcut†, Madhusanka Liyanage‡
*†‡School of Computer Science, University College Dublin, Ireland
‡Centre for Wireless Communications, University of Oulu, Finland
Email: *pasika.ranaweera@ucdconnect.ie, †anca.jurcut@ucd.ie, ‡madhusanka@ucd.ie, ‡madhusanka.liyanage@oulu.fi

***Abstract*—Internet of Things (IoT) and 5G are emerging technologies that envisage a mobile service platform capable of provisioning billions of communication devices which enable ubiquitous computing and ambient intelligence. These novel approaches are guaranteeing gigabit-level bandwidth, ultra-low latency and ultra-high storage capacity for their subscribers. To achieve these limitations, ETSI has introduced the paradigm of Multi-Access Edge Computing (MEC) for creating efficient data processing architecture extending the cloud computing capabilities in the Radio Access Network (RAN). Despite the gained enhancements to the mobile network, MEC is subjected to security challenges raised from the heterogeneity of IoT services, intricacies in integrating virtualization technologies, and maintaining the performance guarantees of the mobile networks (i.e. 5G). In this paper, we are identifying the probable threat vectors in a typical MEC deployment scenario that comply with the ETSI standards. We analyse the identified threat vectors and propose solutions to mitigate them.**

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

## I. Introduction and Motivation

Internet of Things (IoT) devices are thriving with the possibility of proliferated processing capability in miniaturized devices. With improved smart device usage literacy of general public, social internet platforms are launching cumbersome bandwidth consuming applications to elevate their subscriptions. Thus, deployments of billions of smart devices demand access capacity and bandwidth requirement from the access interfaces of mobile Base Stations (BSs). The guaranteed performance metrics of 5G in terms of latency below 1 ms, reliability of 99.99999%, and data rates of 10 Gbps are challenging to achieve with the current data storage and processing infrastructure [1]. Existing conventional cloud computing architecture fails to compensate these guarantees due to its distant geographical placement and bottlenecks endured with multitude of devices that access simultaneously [2]. Thus, an architectural alteration is required to cater these revolutionary requisites. To address these challenges, European Telecommunications Standards Institute (ETSI) has introduced the 'Mobile Edge Computing' (MEC) paradigm, which was renamed as 'Multi-Access Edge Computing' in 2017 [3]. Prime concept of MEC is to transfer the storage and processing functions that are currently provisioned by cloud computing to the edge of the mobile network.

### A. MEC Architecture

The reference architecture presented in [4] was divided into system level and host level as depicted in Fig. 1. Mobile Edge Orchestrator (MEO) is the main hypervisor in a MEC deployment. Operation Support System (OSS) is responsible for granting access to user subscription requests forwarded from User Equipment (UE) via the User Application Life-Cycle Management Proxy (UALCMP). The entity Customer Facing Service Portal (CFSP) is handling the access of third-party services assigned by the Mobile Network Operator (MNO). MEO, OSS, UALCMP, and CFSP are placed in the MEC system level. An approved MEC service request from the UE Application (UE App) is instigating a Mobile Edge Service (MES) under a specified Mobile Edge Application (ME App) executing in the Virtualization Infrastructure (VI) in a Mobile Edge Host (MEH). MEHs are launching ME Apps as Virtual Machines (VMs). Both MEPM and VIM are updating the MEO with relevant status of virtual resource utilization.

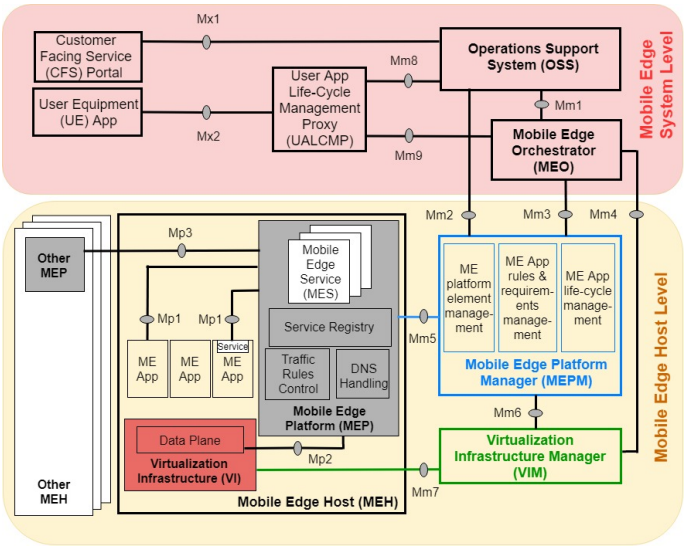


Fig. 1: MEC Reference Architecture

### B. Motivation

MEC is a paradigm that depends entirely on the mobile network deployment. Due to this dependency, integrating

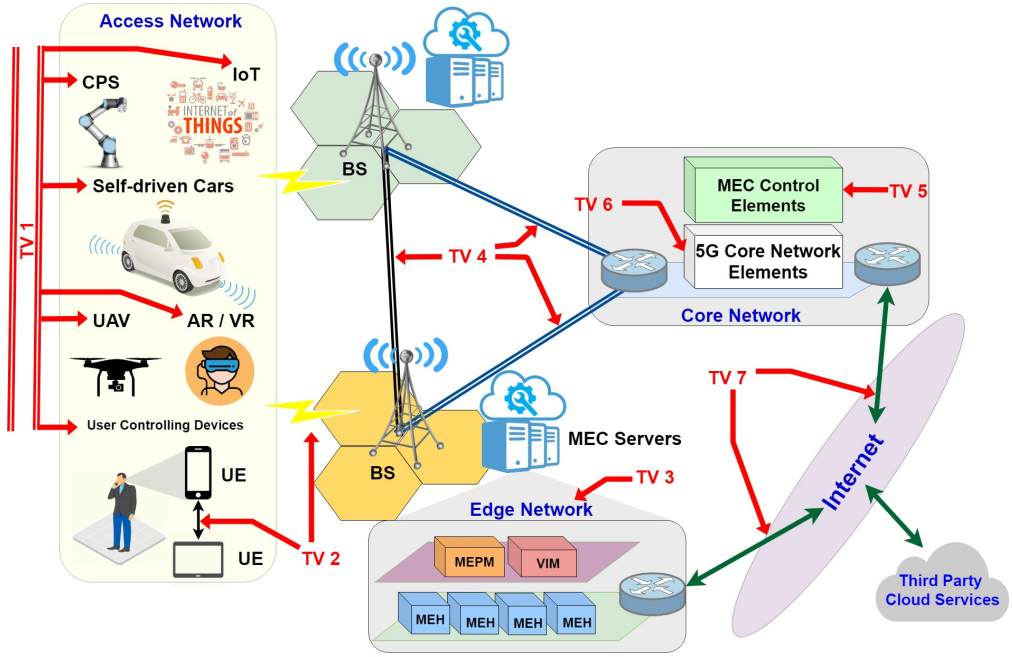


Fig. 2: Threat Vectors in a MEC Deployment

upcoming 5G technology to MEC is a certitude that should be perpetrated circumspectly [5]. Thus, implementing security for heterogeneous services overlaid on top of the 5G technology an intricate task. In addition, extended access capacity at the edge with wireless channels and mobile offloading/ delegation schemes are elevating the probable penetrative and vulnerable vectors in the edge network that would be subjected for exploitation by the adversaries [6]. Materials available for MEC paradigm are limited and more generic in terms of certain aspects. Security is one such aspect that has not been addressed by the researchers specifically in relation to the standardization, due to the heterogeneous deployment scenarios applicable in the radio access network. Therefore, the main motivation of this paper is to identify the threat vectors of the MEC system in accordance to the ETSI standards and investigate the integration technologies to propose solutions for the identified security issues.

The rest of the paper is organized as follows. Section II of this paper reveals the threat vectors in MEC system, while Section III proposes security mechanisms to mitigate them. Section IV discusses the standardization authorities on MEC security and their roles in 5G before concluding the paper in Section V.

## II. Threat Vectors of MEC

Localized nature of the MEC servers are emanating different set of attacks in compared with conventional centralized server placements in cloud computing. We have identified eight Threat Vectors (TVs) based on a typical MEC deployment scenario illustrated in Fig. 2.

*1) Threat vector 1 (TV 1) - Vulnerabilities in User Equipment (UE)*

Any device in direct contact with the MEC system through the BS can be considered as a UE. Even an individual sensors or a sensory system executing a service request towards the MEC system via a UE App is recognized as a UE. The sensitivity of the content in the user controlled devices such as smart phones, tabs, computers, Virtual Reality (VR) Head Mounted Displays (HMDs), or wearable sensors are varying and critical for preserving both security and the privacy of users [1], [7]. Most common type of attack on UE devices is the physical tampering that enable the attacker to take control of the UE device and its resources. Hardware Trojans are capable of perpetrating similar consequences. Various side channel attacks are probable for recovering secure credentials of UEs as presented in [8]. Moreover, attackers injecting malicious codes to the UE operating system result in the execution of various softwareized attacks [9]. A compromised UE or UE App is capable of exploiting the MEC system in three different ways. As most UEs are scarce on resources in terms of storage, processing, and network utilization; attackers could deplete the resources of the UE for disrupting the MES. Similarly, MES could be manipulated to allocate more resources at the MEH from UE side. In addition, attacker has the ability to convey malicious content to the MEH servers. Entities which instigate UE Apps under the influence of third-party services, approved for operation by the MNO are applicable under this TV. Such services are creating unique attack vectors to be dealt with as in vehicles, automated industrial Cyber-Physical Systems (CPS), smart grids, and Unmanned Aerial Vehicles (UAVs) which are represented in [10], [11] respectively.

*Possible Solutions:*

In order to detect the malicious content or malware in a UE, an Intrusion Detection System (IDS) capable of operating in a low-resource environment such as the Qualcomms Snapdragon Smart Protect system is viable [12].

*2) Threat vector 2 (TV 2) - Attacks on communication channels within the access network*

Communication channels established in the access network are formed between a UE and a BS or between UEs in an ad-hoc manner. As the radio channels are established through the air-interface, it is the most exposed link in a mobile network. The exposed nature is enabling the attack vectors Man-in-the-Middle (MitM), eavesdropping, Sybil, spoofing, relay, Denial of Service (DoS), and Smurf [3], [13]. The intended objective of the masquerading type attacks would be to instill a UE with a compromised UE App capable of penetrating and exploiting the MEC system. Technologies such as Multiple-Input-Multiple-Output (MIMO), millimeter Wave (mmWave), carrier-aggregation, and Wi-Fi offloading are deployable in radio channels in the future [14]. The possibility of launching autonomous vehicles, UAVs, and Augmented Reality (AR)/ VR applications are proliferating the heterogeneity and capacity of traffic traversing in this channel. Moreover, mobile delegation or offloading feature of MEC is inviting elevated traffic from the subscribers [15]. These factors are raising compatibility and interoperability issues in the communication protocols established towards the BS with their diverse adaptations.

Technologies such as Low-Power Wide Area Networks (LPWAN), Narrowband IoT (NB-IoT), Wi-Fi, Zigbee, and Bluetooth are employed for forming Device-to-Device (D2D) type ad-hoc channels [1]. Apart from the interposing type attacks, insertion of malicious nodes inside a D2D network is an attack vector that contrives a significant effect to the system. These attacks however, do not directly impact the MEC system. Though, a UE with direct access to the BS could be confiscated via a D2D channel.

*Possible Solutions:*

Employing security solutions in the Network or an upper layer requires a considerable overhead to the traversing traffic. Thus, Physical Layer Security (PLS) methods are widely employed for securing the mobile communication and offloading channels due to their resource constraints [16]–[18]. Strategies such as Light-weight security protocols, Elliptic Curve Cryptography (ECC), Identity Based Encryption (IBE), and security protocols for direct Machine Type Communication (MTC) and UE engagement as proposed in [19], could be utilized for forming authentication mechanisms through this channel [20]. Moreover, Physical Unclonable Functions (PUF) are offering possibilities to derive bio-metric resembled unique features for IoT devices, which are enhancing the security of authentication and data transferring mechanisms conducted in UE enrolled communication channels [21].

*3) Threat vector 3 (TV 3) - Vulnerabilities in the Edge Network*

Mobile Edge Network (MEN) or the host level of the MEC system is the salient functional infrastructure of the MESs. It composes of MEPM, VIM, and MEHs that launch the storage and provisioning services for the MEC subscribers. MEHs are operating in a closed environment with limited connectivity maintained with the MEC system level, the Internet, and subscribed UEs. Thus, occurrence of interposing attacks are minimal compared to the access network. Though, attack vectors targeting the virtualization technologies such as VM manipulation, VM escape, Virtual Network Function (VNF) location shift, Domain Name System (DNS) amplification, and security-log troubleshooting are probable [22], [23]. These type of attacks are impacting the seamless operation of orchestration entities in the host level. Specifically, VIM is a conspicuous target of the adversaries. A compromised VIM leads to the disruption of MESs. Moreover, threats emanated in the access network could be propagated to the MEHs via the communication channels. VM migration and mobile offloading are two such instances where a malicious content could penetrate a MEH [15], [24]. As the user data are stored in MEHs in the MEC edge level, they are vulnerable for physical attacks perpetrated by adversaries capable of entering the BS premises. Typical BSs are not adequately secured against unauthorized entry to the premises. Moreover, tendency to deploy MEC services as minor MEC servers with micro-cell coverage as explicated in [25], is causing issues for MNOs with respect to provisioning physical security.

*Possible Solutions:*

Solutions such as Trusted Platform Manager (TPM) and Virtual Machine Introspection (VMI) are two methods proposed for countering the virtualization based attack vectors [23]. Encrypting the VNF drives protects their integrity against physical attacks. As the MEC host level networking infrastructure is speculated to be implemented utilizing SDN (Software Defined Networking) and NFV (Network Function Virtualization) technologies, security frameworks/ models proposed in [26]–[29] are considerable for deploying with the data network in MEHs.

*4) Threat vector 4 (TV 4) - Attacks on communication links among EDGE and CORE entities*

There are few threats associated with the links that the MEC system is maintaining withing the edge and core levels. Typically in mobile networks, these connections are established using RF, microwave, fiber-optic, or satellite technologies. Therefore, interposing attacks specialized for such transmission technologies are prime threats under this vector. Attack vectors such as Sybil, electromagnetic pulses, DoS, DDoS (Distributed DoS), fiber tapping, hidden pulse, and jamming are probable for above mentioned technologies [30]–[33]. Eventhough the long distance transmission links are typically secured with encoding and encryption schemes, a successful exploitation could incur significant damage to the MEC system. As these links are mostly conveying control statistics and service log information towards the MEC system level entities, ensuring their integrity its critical. Security of these channels are imperative in service migration instances where a VM or a container is migrated to another edge level for continuing a service that feature mobility or global

scalability [24].

*Possible Solutions:*

As pointed out earlier, encoding schemes used with the transmission links are stronger due to the higher bit rates featured with long range transmission. Though, an encrypted communication approaches as Virtual Private Networks (VPNs) could be employed for securing the communication between edge and core or edge and edge levels [34].

*5) Threat vector 5 (TV 5) - Vulnerabilities in MEC Control Elements*

MEO, OSS, UALCMP, and CFSP are the control elements considered under this threat vector. As the MEC subscription request handling entities, UALCMP and CFSP are prone for DoS, DDoS, and relay attacks forwarded via the edge level. The OSS is subjected to masquerading and spoofing attack vectors that intend to acquire accessibility by pretending to be a legitimate entity. Seamless operation of the MEO is dependent of the information it receives from MEPM and VIM regarding the hosted services in terms of their resource utilization. A service impeding attack perpetrated to any other entity in linked to the MEO is causing it to intermit its operations. Moreover, MEO is vulnerable to attack vectors plausible for virtualized environments explicated in TV 3.

*Possible Solutions:*

To safeguard the internal constructs of the MEO, hypervisor introspection methods could be employed [23]. For Linux based virtualization deployments, Security Enhanced Linux (SELinux) would act as a kernel hardening tool. TPMs are essential for certifying the trust of entities engaging with the system level entities [27].

*6) Threat vector 6 (TV 6) - 5G Core Network Entities*

MEC is an integration technology to 5G. Therefore, proper functioning of the 5G core is critical for both mobile and MEC networks. Signalling is a paramount function among core network entities. As an instance of Network Functions (NFs) such as the User Plane Function (UPF) is launched at the MEH for managing the communication in the Local Area Data Network (LADN), seamless operation of the channels lying between edge and core levels and its security is important. The impending 5G core entities are developed using softwarized or virtualized approaches as Virtual Network Functions (VNFs) [35]. Thus, they are vulnerable for attacks such as DoS/DDoS, VNF manipulation, VNF location shift, and other softwarized attacks [23], [36].

*Possible Solutions:*

Auto-configurable security mechanism is proposed in [37] for securing authentication and communication between VNFs. Moreover, framework/ architecture proposed in [38], [39] are capable of securing typical VNF functions in a NFV environment.

*7) Threat vector 7 (TV 7) - The Internet Connectivity*

The connections maintained by MEC system level and edge level entities to the Internet for reaching different MEC domains or third party cloud services are considered under this TV. In a scenario in which a third party consumer is leveraging the MEC edge level, to pre-process their data prior to conveying them to the corresponding cloud service; MEH is capable of extending its reach to the cloud service via the Internet [40]. In addition, it is essential to establish connections to MEC system level entities (i.e. MEO and OSS) from third party clouds for status updating. These extensions are subjected to MitM, relay, packet sniffing, and spoofing attacks [3]. In spite of the attractiveness in the perspective of the adversaries, MEC edge and system levels possess adequate resources to employ strong security mechanisms. Similarly, MEC system level establishes its connections to the other MEC domains through the Internet.

*Possible Solutions:*

In case of a connectivity that extends to reach distant MEC domains, VPN based secure communication tunneling mechanism could be employed for assuring remote site security. Access controlling function for MEH and cloud services could be handled by forming Demilitarize Zones (DMZs) with proper firewall and access control policies [23].

## III. Approaches to Secure MEC by Design

In this section, we discuss the possible security solutions that might aid in preventing security issues in MEC based systems. TABLE I summarizes the proposing security solutions and their relation to the identified threat vectors in Section II.

### *A. Virtual Machine Introspection (VMI)*

VMI or hypervisor introspection methods are employed for detecting anomalous patterns in the behavior of VMs or hypervisors. VMIs are monitoring the activities of the VMs in terms of processor and memory utilization. LibVMI is such a tool that acts as a host based Intrusion Detection System (IDS) for VMs [23]. Functionally extended VMIs as in the one proposed in [41] are capable of interrupting the VM execution or isolating the running programs if the VM states are deviating from the normal operational standards. VMIs could be launched at both edge and core levels to inspect the behaviour of ME Apps, MEPM, and MEO. It would be possible to detect any attack that intends to compromise the virtualized entities. Moreover, proper introspection methods are improving the performance of hypervisors.

### *B. Trusted Platform Manager (TPM)*

TPM is an entity that verifies the software integrity of executable programs through validation of operational statistics such as firmware, Operating System (OS) kernel, Basic Input/ Output System (BIOS), and boot loader [23]. Moreover, TPM could be employed as an authentication handling agent for softwarized entities that intend to subscribe functions from the MEC serviceable platform [42]. Specifically, ME Apps could be attested with TPMs either internally or in a service migration instance where ME Apps (or MEHs) from a guest domain is migrated to the hosting domain. Moreover, TPMs are capable of validating the VNFs. Thus, TPM deployments in the 5G core would enhance their security and performance. In case of a third-party service request forwarded by an autonomous entity, TPM functionalities could be useful for CFSP to determine the legitimacy of the particular service.

### C. Virtual Private Local Area Network Service (VPLS)

VPLS is a technology that was developed for interconnecting industrial sites with a Multi-Protocol Label Switching (MPLS) provider network [43]. The tunneling nature of VPLS is guaranteeing the security and integrity of transmitted information. Moreover, MPLS backbone of VPLS is optimizing the network performance for alleviating the latency and jitter. In order to overcome the tunnel management limitations of VPLS architectures, SDN has been proposed as a solution [44]. MEC envisages to deploy a SDN based networking infrastructure for establishing the communication within and among the edge levels. Thus, Software Defined VPLS (Soft-VPLS) approach is adaptable for securing the communication channels between edge and core levels of the MEC deployments. These channels are transmitting mobile network signalling statistics (i.e. 5G), MEC control statistics, MEC service requests, MEC service approvals, user data, and executable content in migration or an offloading circumstance. With Soft-VPLS, each traffic category could be classified and conveyed via different tunnels. Enhanced tunnel management capability would improve the overall performance of the channels in addition to the heightened security. Moreover, the Internet connectivity (i.e. TV 7) could be secured with Soft-VPLS adaptations.

### D. Artificial Intelligence (AI)

AI methods are frequently used for developing autonomous security solutions for prevailing information systems. They are widely successful with malware and anomaly detection adaptations [45]. An autonomous security mechanism is intrinsic for the MEC system; due to the heterogeneous nature and the enormous number of connecting devices. Adapting AI methods to MEC entities would be convenient due to their softwareized and virtualized nature. Various initiatives are launched for adapting AI for edge computing based security developments [46], [47]. AI based IDS could be launched at the edge level for monitoring the network behaviour and traversing content in the LADN. AI based malware detection schemes for smart mobile devices (i.e. UEs) are proposed in [48], [49]. Moreover, AI and machine learning are employed for developing VMI methods [50].

### E. Blockchain

Blockchain is a secure and decentralized data management framework emerged with the Bitcoin digital currency concept [51]. This concept overcomes the limitations (i.e. single point of failure) of centralized data management systems with improved security; attributed from the dispersed data fragments/ blocks. Even with the locational and context awareness facilitated to the MEC subscribers, outsourcing private data to another party is still raises concerns. In order to overcome these privacy predicaments, Blockchain is an evident solution. Wide range of Blockchain based developments are proposed in [52], [53] for edge computing scenarios. In MEC point of view, Blockchain could be adoptable for securing authentication of UEs, service migration channels, mobile offloading channels, and for maintaining service status parameters hindered from the adversaries. The performance of MEC system however, should be evaluated prior to integrating this technology for avoiding an inefficient servicing platform.

### F. Network Slicing (NS)

In NS, a physical network is logically compartmentalized into different slices for enabling diversified services to operate simultaneously [54]. With that approach, expenditure for resource utilization could be alleviated significantly. NS offers the features of virtualization support, function modularization, end-to-end connectivity, and better isolation compared with other resource sharing concepts [55]. According to this concept, a singular slice is composed of Network Slice Instances (NSIs) and a Network Slice Manager (NSM) [56]. Variant ME Apps provisioned to service diverse UE Apps are sharing the same LADN in a MEH. The NS concept could be applied in such a situation to simplify the service provisioning. A simplified networking deployment is improving the chances of security solution adaptations. Either a MEH or a ME App could be assigned as a NSM for embedding security mechanisms in it. The Next Generation Mobile Networks (NGMN) alliance is actively working towards NS security for adapting the concept to the 5G use cases [56].

### G. Context Aware Security

The idea of context awareness is drawn from the ambient intelligence plausible with prevailing smart devices that possess advanced sensory capabilities [57]. These features of current UEs are enabling services customized for personal and locational context. Similarly, ambient intelligence could be leveraged to enhance the security of UEs from the security related contextual data gathered from the sensory installations. Such an approach would be ideal for securing the communication channels discussed under TV 2. Adaptive security protocols could be employed for securing these channels [58]. Moreover, MEHs are capable of deploying context aware security mechanisms to detect ME Apps with anomalous behavior.

### H. Physical Unclonable Functions (PUFs)

PUF is a method of extracting a bio-metric resembled imprint from non-human entities (i.e. devices) considering their unique features attributed from the fabrication process. Various parameters in circuitry such as RF carrier frequency offset, in-phase quadrature phase imbalance, and transient effect ring oscillator are used as PUFs of UEs. Similar to biometrics, PUFs could be utilized for developing authentication protocols for UEs as presented in [21], [59]. Due to their uniqueness, PUF based authentication messages do not incur heavy overhead comprised of authentication credentials. Thus, an efficient and more secure security protocols could be developed with this adaptation.

## IV. Standards

As the main standardization authority, ETSI Industry Specification Group (ISG) for MEC is publishing the security

TABLE I: Summary of security solutions and their correspondence to threat vectors

| Security Solution | Applicable Threat Vectors | | | | | | |
|---|---|---|---|---|---|---|---|
| | TV 1 | TV 2 | TV 3 | TV 4 | TV 5 | TV 6 | TV 7 |
| Virtual Machine Introspection | | | ✓ | | ✓ | | |
| Trusted Platform Manager | | | ✓ | | ✓ | ✓ | |
| Virtual Private LAN Service | | | | ✓ | | | ✓ |
| Artificial Intelligence | ✓ | | ✓ | | ✓ | | |
| Blockchain | | ✓ | ✓ | ✓ | ✓ | | |
| Network Slicing | | | ✓ | | ✓ | | |
| Context Aware Security | | ✓ | ✓ | | | | |
| Physical Unclonable Functions | | ✓ | | | | | |

requirements for MEC paradigm [60]. Eventhough ETSI is a well-established organization, MEC paradigm should comply with other organizations / institutions due to its reliance on 5G technology. Organizations such as 5G Infrastructure Public Private Partnership (5G-PPP), Third Generation Partnership Project (3GPP), International Telecommunication Union Standardization Sector (ITU-T), and NGMN alliance are actively enrolled with developing and publishing security standards for 5G. As ITU is the organization pioneering in setting the standards for mobile networks, their security standards are vital for realizing MEC [61]. 5G-PPP Projects such as ANASTACIA [62] and MATILDA [63] funded under the EU Horizon 2020 (H 2020) initiative are working in relation to MEC and security standardization focused in different application scenarios. NGMN alliance is more focused on standardizing security in network slicing concept. In terms of privacy, General Data Protection Regulation (GDPR) initiative plays a large role in standardizing the privacy rights of MEC subscribers [64].

## V. Conclusion

This paper have presented the current status of the MEC paradigm from the security perspective. Security is a critical factor for realizing the potential of MEC for a feasible deployment. We identified seven threat vectors in a MEC deployment scenario. Then attack vectors corresponding to those threat vectors were also revealed, where existing security solutions were mapped with them. Next, state-of-the-art security mechanisms were explicated in the context of applying them for MEC in its design stages. Our intentions are to initiate a discussion on security concerns of MEC paradigm with this research directive. We believe that our identified threat vectors and our proposed solutions would lead to a pragmatic MEC deployment in the near future.

## Acknowledgement

This work is party supported by European Union in RESPONSE 5G (Grant No: 789658) and Academy of Finland in 6Genesis Flagship (grant no. 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] M. Liyanage, I. Ahmad, A. B. Abro, A. Gurtov, and M. Ylianttila, Comprehensive Guide to 5G Security. Wiley Online Library, 2018.

[3] 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.

[4] 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

[5] 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.

[6] D. He, S. Chan, and M. Guizani, "Security in the Internet of Things Supported by Mobile Edge Computing," IEEE Communications Magazine, vol. 56, no. 8, pp. 56–61, 2018.

[7] M. S. Elbamby, C. Perfecto, M. Bennis, and K. Doppler, "Toward Low-latency and Ultra-reliable Virtual Reality," IEEE Network, vol. 32, no. 2, pp. 78–84, 2018.

[8] A. Nahapetian, "Side-channel Attacks on Mobile and Wearable Systems," in 2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC). IEEE, 2016, pp. 243–247.

[9] P. Kocher, D. Genkin, D. Gruss, W. Haas, M. Hamburg, M. Lipp, S. Mangard, T. Prescher, M. Schwarz, and Y. Yarom, "Spectre Attacks: Exploiting Speculative Execution," arXiv preprint arXiv:1801.01203, 2018.

[10] 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.

[11] H. Ge, D. Yue, X. Xie, S. Deng, and C. Dou, "A Unified Modeling of Multi-sources Cyber-attacks with Uncertainties for CPS Security Control," Journal of the Franklin Institute, 2019.

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

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] D. Wang, B. Bai, K. Lei, W. Zhao, Y. Yang, and Z. Han, "Enhancing Information Security via Physical Layer Approaches in Heterogeneous IoT With Multiple Access Mobile Edge Computing in Smart City," IEEE Access, vol. 7, pp. 54 508–54 521, 2019.

[19] F. Conceicao, N. Oualha, and D. Zeghlache, "Security Establishment for IoT Environments in 5G: Direct MTC-UE Communications," in 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC). IEEE, 2017, pp. 1–5.

[20] 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.

[21] 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.

[22] 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.

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

[24] 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.

[25] W. Zhang, Y. Huang, D. He, Y. Zhang, Y. Zhang, R. Liu, Y. Xu, Y. Wu, and L. Zhang, "Convergence of a Terrestrial Broadcast Network and a Mobile Broadband Network," IEEE Communications Magazine, vol. 56, no. 3, pp. 74–81, 2018.

[26] 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.

[27] 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.

[28] 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.

[29] M. S. Siddiqui et al., "Policy based Virtualised Security Architecture for SDN/NFV Enabled 5G Access Networks," in 2016 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN). IEEE, 2016, pp. 44–49.

[30] K. Lim, K. M. Tuladhar, and H. Kim, "Detecting Location Spoofing using ADAS Sensors in VANETS," in 2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC). IEEE, 2019, pp. 1–4.

[31] R. T. Devereaux, "Unplugging the Grid: Energy Surety via Wireless Power," Strategic Planning for Energy and the Environment, vol. 38, no. 2, pp. 7–16, 2018.

[32] C. Huang, P. Y. Ma, B. J. Shastri, P. Mittal, and P. R. Prucnal, "Robustness of Optical Steganographic Communication Under Coherent Detection Attack," IEEE Photonics Technology Letters, vol. 31, no. 4, pp. 327–330, 2019.

[33] Z. Feng and C. Hua, "Machine Learning-based RF Jamming Detection in Wireless Networks," in 2018 Third International Conference on Security of Smart Cities, Industrial Control System and Communications (SSIC). IEEE, 2018, pp. 1–6.

[34] S. Alharbi, P. Rodriguez, R. Maharaja, P. Iyer, N. Subaschandrabose, and Z. Ye, "Secure the Internet of Things with Challenge Response Authentication in Fog Computing," in 2017 IEEE 36th International Performance Computing and Communications Conference (IPCCC). IEEE, 2017, pp. 1–2.

[35] 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.

[36] T. Alharbi and M. Portmann, "The (In) Security of Virtualization in Software Defined Networks," IEEE Access, 2019.

[37] H. Kim, P. Park, and J. Ryou, "Auto-configurable Security Mechanism for NFV," KSII Transactions on Internet & Information Systems, vol. 12, no. 2, 2018.

[38] A. M. Zarca, J. B. Bernabe, R. Trapero, D. Rivera, J. Villalobos, A. Skarmeta, S. Bianchi, A. Zafeiropoulos, and P. Gouvas, "Security Management Architecture for NFV/SDN-aware IoT Systems," IEEE Internet of Things Journal, 2019.

[39] 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.

[40] S. Kekki et al., "MEC in 5G Networks," ETSI White Paper #28, vol. 28, no. 28, pp. 1–28, 2018, last accessed 16 June 2019. [Online]. Available: https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp28_mec_in_5G_FINAL.pdf

[41] 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.

[42] ETSI-NFV-ISG, "Network Functions Virtualisation (NFV): Virtual Network Functions Architecture," ETSI NFV White Paper, 2014, last accessed 16 May 2019. [Online]. Available: https://www.etsi.org/deliver/etsi_gs/NFV-SWA/001_099/001/01.01.01_60/gs_NFV-SWA001v010101p.pdf

[43] M. Liyanage, M. Ylianttila, and A. Gurtov, "Fast Transmission Mechanism for Secure VPLS Architectures," in 2017 IEEE International Conference on Computer and Information Technology (CIT). IEEE, 2017, pp. 192–196.

[44] ——, "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.

[45] 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

[46] X. Lin, J. Li, J. Wu, H. Liang, and W. Yang, "Making Knowledge Tradable in Edge-AI Enabled IoT: A Consortium Blockchain-based Efficient and Incentive Approach," IEEE Transactions on Industrial Informatics, 2019.

[47] Oulu, "Multi-Access Edge Computing (MEC) Artificial Intelligence (AI)," Feb 2018, last accessed May 16, 2019. [Online]. Available: http://www.edgeai.info/project/mec-ai/

[48] R. Zhang, X. Chen, J. Lu, S. Wen, S. Nepal, and Y. Xiang, "Using AI to Hack IA: A New Stealthy Spyware Against Voice Assistance Functions in Smart Phones," arXiv preprint arXiv:1805.06187, 2018.

[49] D. Kong, "Science Driven Innovations Powering Mobile Product: Cloud AI vs. Device AI Solutions on Smart Device," arXiv preprint arXiv:1711.07580, 2017.

[50] 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.

[51] Z. Xiong, Y. Zhang, D. Niyato, P. Wang, and Z. Han, "When Mobile Blockchain Meets Edge Computing," IEEE Communications Magazine, vol. 56, no. 8, pp. 33–39, 2018.

[52] Y. Dai, D. Xu, S. Maharjan, Z. Chen, Q. He, and Y. Zhang, "Blockchain and Deep Reinforcement Learning Empowered Intelligent 5G Beyond," IEEE Network, vol. 33, no. 3, pp. 10–17, 2019.

[53] M. Liu, F. R. Yu, Y. Teng, V. C. Leung, and M. Song, "Distributed Resource Allocation in Blockchain-based Video Streaming Systems with Mobile Edge Computing," IEEE Transactions on Wireless Communications, vol. 18, no. 1, pp. 695–708, 2018.

[54] 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.

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

[56] 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

[57] 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.

[58] 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.

[59] 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.

[60] A. Neal, B. Naughton, C. Chan, N. Sprecher, and S. Abeta, "Mobile Edge Computing (MEC); Technical Requirements," ETSI, Sophia Antipolis, France, White Paper no. DGS/MEC-002, 2016.

[61] ITU-T. (2015) Security in Telecommunication and Information Technology. Last accessed 18 June 2019. [Online]. Available: https://www.itu.int/dms_pub/itu-t/opb/tut/T-TUT-SEC-2015-PDF-E.pdf

[62] S. bianchi, "ANASTACIA Project," 2017, last accessed June 16, 2019. [Online]. Available: http://www.anastacia-h2020.eu/

[63] F. Davoli, "The MATILDA Project," 2017, last accessed June 16, 2019. [Online]. Available: http://www.matilda-5g.eu/

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