Wiley 5G Ref

MEC and Cloud Security

Aaron Yi Ding (TU Delft)

Abstract

Security is crucial for 5G mobile systems. As Multi-access Edge Computing (MEC) and cloud technologies are going to be utilized by 5G to support various services including IoT, health, smart grid and transportation, there is a strong demand for comprehensive investigation of the security aspects of MEC and cloud in 5G context. The core security concerns for 5G MEC and cloud include trust on hardware components and connected devices, system software, networking and communication, micro edge service, and distributed security logging at scale. Besides discussion of threat models and challenges, four promising research directions are also highlighted, covering trust management, machine learning based security enforcement, microservice management, and hardware assisted security enhancement in 5G networks. The illustrations focus on current security challenges and corresponding solutions for 5G MEC and cloud. The analysis and outlook shed light on future 5G security development and integration of MEC and cloud technologies. The content is of special interest to 5G engineers, researchers, service developers, and policy makers from industry, academia and government.

Keywords

Multi-access Edge Computing (MEC), Edge Security, Cloud Security

Main text

Introduction

The 5th generation cellular network technology (5G) is generating new opportunities for various applications in IoT, multimedia, smart grid and mobility domains (Ding and Janssen, 2018). Given its role as a critical infrastructure for both industry and society, 5G security has always been a top priority (Liyanage, et al., 2018). Besides conventional confidentiality, integrity and availability (CIA) issues, 5G is facing new security challenges coming from new technologies, services (e.g., industrial IoT, autonomous driving), regulations, and change of user demands.

Besides embracing cloud solutions, 5G is rapidly integrating Multi-access edge computing (MEC) which is standardized by European Telecommunications Standards Institute (ETSI). MEC aims to bridge the gap between cloud and IoT by providing high bandwidth and low latency access to 5G resources. Those advantages will facilitate mobile operators to open their networks to a new edge-driven ecosystem and corresponding value chains. In this regard, cloud computing enables 5G providers to flexibly outsource storage and processing functionalities. MEC further fills the gap between centralized cloud and distributed computing resources in terms of scalability, location awareness, and mobility. MEC allows to filter extremely large amounts of data to support efficient data processing at scale. Together with cloud intelligence, MEC and cloud can accelerate decision making based on both the locally processed data with context awareness and centralized management overview. This advantage is vital for various 5G enabled services such as fully-autonomous driving, remote surgeries, and HD mobile video conferencing, which demand reliability, availability and ultra-low latency. In addition, MEC offers localized caching and storage, which are necessary to support fine-grained offloading in terms of data traffic and computational load (Ding, et al., 2015, Cozzolino, et al., 2017).

Although MEC and cloud offer several appealing features to 5G ecosystem, the security aspects of those technologies must be fully conceived. As shown in studies on D2D (Haus, et al., 2017) and IoT communications (Hafeez, et al., 2017), security must be enforced at the start of system development and deployment. For MEC and cloud in 5G, security concerns include both technical and societal aspects, such as trustworthiness of MEC and cloud, IoT-oriented security threats, secure infrastructure access, and distributed security logging at scale. Since 5G is going to serve as a fundamental infrastructure, its security, safety, reliability and resilience are of critical importance to our future digitalized society.

Given the rapid process of consolidating both edge and cloud to better support 5G systems (Morabito, et al., 2018), this article focuses on the integrated view of applying MEC and cloud to 5G. Therefore, the term "5G MEC-Cloud" or "MEC-Cloud" is utilized to represent a unified discussion for edge and cloud security in the 5G context. The article is organized as follows. First, an overview is presented which covers features and synergies of 5G MEC-Cloud. Second, in-depth discussions on MEC-Cloud security are presented, which include threat models, key security challenges, considerations, and future directions. Finally, the article concludes with an outlook on key concerns that are pragmatic and valuable to 5G engineers, researchers, service developers, and policy makers from industry, academia and government.

5G MEC-Cloud Overview

[A] Edge and Cloud Computing for 5G

For 5G, edge and cloud are complementary technologies that can promote the operational efficiency, computational capability, service diversity, and low-latency access to 5G radio network resources. The advantages of integrating both edge and cloud will allow 5G operators to open up their infrastructure and service offering towards a more advanced and dynamic ecosystem. By utilizing edge and cloud, new requirements from end-users and large-scale Internet of Things (IoT) deployment can also be met. These modern requirements span across communication, mobility, scalability, trust and privacy, in addition to the traditional demands of latency, security, and load balancing. In particular for IoT with high demand to offload data processing and storage, edge and cloud can enable 5G to flexibly accommodate various IoT applications, ranging from urban sensing, smart farming, e-health, industrial control, and intelligent vehicles.

As a rising paradigm, edge computing, especially the Multi-access edge computing (MEC) is currently standardized by the European Telecommunications Standards Institute (ETSI). The fundamental principle of edge computing is to complement cloud resources by bringing computing closer to devices and date sources. As part of 5G roadmap, MEC exploits a systematic integration of wireless access technologies, which is in line with the 5G evolution towards ultra-dense deployment of small-cells, such as micro, pico, and femto cells. This will directly enhance the access capacity and quality of the connections. As an example, MEC offers 5G with dual/multiple connectivity where smart devices are able to communicate simultaneously through both conventional macro and the newly small cells. Furthermore, computational offloading schemes (Cuervo, et al., 2010) (Kosta, et al., 2012) (Cozzolino, et al., 2017) on the edge will speed up computation and communication.

With a mature ecosystem, the cloud computing exploits the economies of scale through centralization and aggregation, which effectively press down the marginal cost of administration, operation, and maintenance. One clear advantage for 5G comes from the outsourcing of setting up data centers with significant capital cost. Instead, computing power can be obtained from large cloud service providers in a pay-as-you-go manner. In addition, cloud computing can support 5G with elasticity, which can adjust the resource utilization to avoid under-provisioning and overprovisioning under very dynamic settings. Depending on the requirements, the service model of 5G cloud can be served via Infrastructure as a Service (IaaS), Platform as a Services (PaaS) or Software as a Service (SaaS). Figure 1 presents an architectural overview of 5G MEC-Cloud, where 5G cloud and 5G MEC form a two-tier structure to harness the benefits of both cloud and edge in terms of resource utilization, elasticity, and flexibility.

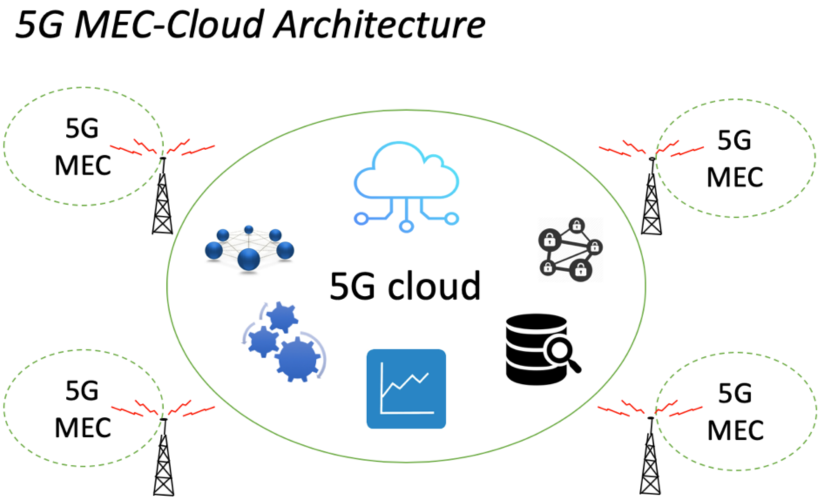

Figure 1: 5G MEC-Cloud Architecture

Given the recent progress in consolidating edge and cloud to better support 5G, numerous applications can benefit from such technology fusion, ranging from smart home to industrial IoT (IIoT) as illustrated in Table 1. The benefits of MEC-Cloud result from harnessing the power of both centralized and distributed resources for abstraction, programmability interoperability, and elasticity. In addition, there are four enabling technologies that support the vision of 5G MEC-Cloud, including Network Function Virtualization (NFV), Software Defined Networking (SDN), Information Centric Networking (ICN) and Network Slicing (NS) (Liyanage, Porambage and Ding, 2018). By using those fast-evolving technologies, it is possible to optimize existing mobile infrastructure and implement novel ones for 5G. For instance, to realize MEC-Cloud operational environment, it is necessary to run virtualized servers at various locations at the edge of 5G mobile networks. 5G base stations can be the physical hosts for such virtualized servers, which not only host edge services but also related services such as NFV and SDN. The setting can reduce the deployment costs and provide a common management infrastructure for all virtualized services. Furthermore, this can also enrich the mobile operators' existing business models by opening to versatile 3rd party service providers.

Table 1: MEC-Cloud can benefit 5G enabled services

5G enabled services	**MEC-Cloud benefits**
Smart home	Reduced communication latency, easy instantiation and fast relocation. Moreover, MEC-Cloud can process sensitive data locally for privacy preservation.
Smart urban sensing	Data can be processed at the edge of the network with location awareness and low latency, i.e., closer to sensor and hence removing the burden of sending raw data over a network with limited bandwidth.
Intelligent vehicles	Improving the operational functions such as real-time traffic monitoring, continuous sensing in vehicles through infrastructure.

Augmented Reality	Migrating computationally expensive tasks to edge servers will increase the computational capacity of AR/VR devices and extend their battery-life. MEC-Cloud also offer scalability by enabling high capacity and low latency wireless coverage for high populated places like smart cities or stadiums with a massive density of users to enjoy the AR/VR experience.
Interactive gaming	Improving user experience for delay-sensitive game users by offloading the resource-intensive applications to the MEC-Cloud servers that are located in the proximity.
Smart retail	MEC-Cloud servers can process local data generated by retailing systems such intelligent payment solutions, facial recognition systems, smart vending machines.
Smart farming	Reducing the overhead on data access, synchronization and storage by using on-site MEC-Cloud servers to analyze collected farming data without real-time uploading to a remote cloud
Smart energy	Mitigating bandwidth bottlenecks and communication delays due to poor network connectivity and huge volume of data generation by allowing the computation to be performed closer to the data source. MEC-Cloud also reduces the attack propagation by enforcing security nearby the end power devices.
Industrial IoT	MEC-Cloud can enable real-time edge analytics for future IIoT applications by addressing the challenges of predictive maintenance and M2M communication in terms of low power operation and reconfiguration.

[B] Features and Synergies

The 5G MEC-Cloud is envisioned to be a federation of computing resources deployed across edge networks and provider data centers. The deployed MEC-Cloud servers can function independently and also collaborate with each other. The cloud computing part in MEC-Cloud can take the auxiliary role by offering reliable and powerful computing resources. In the 5G context, the general features of MEC-Cloud include virtualization, storage, networking and multi-tenancy.

- Virtualization – an important feature in deploying services in heterogeneous settings. Virtualization allows the physical resources to be readily shared by multiple system services/applications. By creating the virtual instance or device such as operating systems, network interfaces, and storage devices, 5G can utilize existing infrastructure and hardware in more than one single execution environment.
- Storage – MEC-Cloud storage offers a hybrid of central and distributed storing possibility for maintain, manage and backup data. The hybrid setting also allows flexible access from end-users in an on-demand fashion.
- Networking – to allow seamless connection among different servers of different purposes (e.g., data processing, storage) in largely distributed manner. Secure networking is a mandatory feature of MEC-Cloud through both physical and virtual private networks, through which end-users can access their data and 5G services.
- Multi-tenancy – to support multiple 5G customers who do not share data but still share the same physical infrastructure and computing resources through a secure execution environment. This feature leads to optimal utilization of 5G resources including radio access, data storage, and computing power.

To understand the differences and similarities between MEC-Cloud and conventional data center cloud, Table 2 highlights the key properties including ownership, deployment, hardware types, service offering, architecture, mobility, latency, and location awareness. The consolidation of edge and cloud into the 5G MEC-Cloud has one goal: to bring cloud alike capability to the edge of 5G access networks. The technologies enabling MEC-Cloud support multi-tenant virtualization infrastructure. With network slicing and SDN, the MEC-Cloud infrastructure can dynamically adjust provision capacity to various demands in terms of location, speed, and/or privacy.

Table 2: Comparing MEC-Cloud and conventional cloud on key properties

Features	**5G MEC-Cloud**	**Cloud / Data Centers**
Ownership	5G providers	Private cloud providers
Deployment	Network edge and 5G core	Network core
Hardware types	Heterogeneous	Homogeneous
Service offering	Lightweight virtualization	Virtualization
Architecture	Decentralized and distributed	Centralized
Mobility	Yes	Limited
Latency	Low	Average
Location awareness	Yes	Limited

One important property for 5G is mobility, which is needed by mobile devices. MEC-Cloud supports mobility through several strategies such as hierarchical mobility management and live migration of lightweight virtual servers. Besides mobility, MEC-Cloud provides necessary scalability and availability for future 5G IoT deployment. This is crucial given the fact that devices and servers can be geographically wide spread. MEC-Cloud can organize the distributed resources to assure that certain services can be efficiently set up and provided on-demand at the spot where needed. In practical setting, edge servers will provide redundancy at local level and function as proxy for the central cloud in case of temporary failure in core date centers. MEC-Cloud also offers third-party service providers to closely work with 5G providers to deploy edge specific services that can be integrated to telecommunication infrastructure.

As to the synergies of edge and cloud, the decentralization and proximity to date/devices bring obvious benefits but also deserve attention in terms of synchronization, interoperability, accountability and usability. Given the cloud-edge-device architecture, both hard and soft states of services need to be timely synchronized across all the tier. Since edge servers can be managed by different infrastructure providers, it is necessary to form standards as to how the different parties in the MEC-Cloud architecture can collaborate with each other, how to discover services, and how to manage the life cycles of virtualized services in such distributed environment.

One important synergy MEC-Cloud is the management of virtual resources. The key concern is the optimization of resource utilization, e.g., to define when and where a virtual service instance needs to be set up, replicate, migrate, or merged. Another synergy concern is resource offloading where users can delegate the execution of tasks to external entities. As edge hardware in 5G is typically resource constrained, a fine-grained offloading design is needed to allow maximal usage of available resources.

MEC and Cloud Security in 5G

[A] Threat Models

Given the core of MEC-Cloud consists of several enabling technologies such as NFV, SDN and network slicing, security in 5G MEC-Cloud covers not only these fundamental building blocks but also to orchestrate different security schemes dedicated for each of these technologies. This requires unified management of available security mechanisms to achieve seamless integration. In particular for 5G inherent mobile feature, security at networking and system level shall support mobility and can function in a decentralized manner without relying on centralized administration.

Besides potential threats emerged from edge computing, it is equally important to consider the security threats that are embedded in the enabling technologies and also the application domains. In this regard, IoT is a typical example for 5G that generates attack surface due to its scale and heterogeneity. Due to the tight relation of IoT in our infrastructure and daily services, the implication for MEC-Cloud security is that the protection must consider all the layers of technologies not only about MEC-Cloud but also the threats from IoT.

Table 3: Threat models of MEC-Cloud

Category	**Threats**
Network Infrastructure	DoS, man-in-the-middle attacks, rogue mobile routers
Core Servers	Privacy leak, service manipulation, rogue core server
Edge Servers	Physical damage, privacy leak, privilege escalation, service manipulation, rogue edge server
Virtualization	DoS, resource misuse, privacy leak, privilege escalation
End Devices	Data injection, service manipulation

In order to comprehend the security landscape of MEC-Cloud, security threats need to been investigated according to crucial aspects of edge and cloud (Roman, 2018). Table 3 summarizes the threats in MEC-Cloud under five categories, including network infrastructure, core servers, edge servers, virtualization and end devices. The threats affect both edge and cloud computing which are the core of 5G MEC-Cloud.

- *Network Infrastructure*

  MEC-Cloud depends on the communication networks and protocols to connect various devices and servers, via both wired and wireless media. The infrastructure is a clear target for the adversaries and denial of service (DoS) is a common threat for all types of communication networks. The threat can take the form of distributed denial-of-service (DDoS) and wireless jamming.

  As a typical threat to take control of network, Man in the Middle is used by adversaries to launch further actions such as traffic injection, manipulation and eavesdropping. In 5G mobile networks, such threat is difficult to detect and affect several elements in MEC-Cloud including data and virtual images that are exchanged through the network.

  Another threat for infrastructure is the rogue mobile routers. Since the deployment at the edge of network, adversaries can install their fake base stations. This threat is similar to the Man in the Middle threat where the rogue agents can impersonate, eavesdrop, and misguide the users in the network.

- *Core Servers*

  One major part of MEC-Cloud is the cloud support from the core. In practical setting, both edge and cloud can be manged by a single company or provider but can still share the infrastructure among several providers. In this context, privacy leakage is a common threat since it is hard to guarantee the information stored would be exposed to unauthorized adversaries.

Service manipulation in core servers is often from internal adversaries with privileges that can produce fake information to disturb the operation of MEC-Cloud. This threat has similar limitation as privacy leakage since the adversaries can only affect part of the system owing to the decentralized and distributed setting of MEC-Cloud.

Rogue core servers form another threat which assumes that part of the core servers can be targeted by attackers. The rogue core servers are often compromised by the upper layer of software since the core infrastructure is typically protected. The rogue core servers mainly cause management disturbance and hence need fault tolerance scheme to tackle such threat.

- *Edge Servers*

  The edge servers in MEC-Cloud are mini data centers that host management services and virtual images. The attack surface of edge servers ranges from public APIs to physical tampering. Regarding physical damage, certain hardware elements of MEC-Cloud may not be guarded as compared with conventional data center. The examples are edge servers managed by SME or small organizations. The physical damage threat requires the adversaries to approach the hardware to destroy it. Due to this physical vicinity requirement, the impact is of local scope in that only the services in proximate to the attack will be affected.

  Privacy leakage is one threat for edge servers but with limited scope. As edge servers often process and store only the information from users in the proximity of the service area. When there is migration of users or information, the leakage can be extended above the geographical coverage.

  Privilege escalation is used by adversaries to take control services offered by edge servers. This type of threat is caused by the fact that edge servers could be managed by administrators with limited security knowledge nor training. Therefore, the edge infrastructure could be mis-configured and lack of maintenance. The privilege issue also arises from internal adversaries that result from social engineering, which is even harder to mitigate.

  After gaining privileges, service manipulations can be another threat. Consequently, adversaries are able to launch complicated attacks such as DDoS using the manipulated resources in the existing infrastructure.

  The rogue edge server is a threat that can be produced by either injection of servers into the infrastructure or manipulation of existing ones. This threat has severe impact in that adversaries gain control over services in specific locations and hence having access to manipulate the information passing through those spots. If the rogue edge server is happening in frequently used network section, the damage can be further escalated.

- *Virtualization*

  As MEC-Cloud is built upon virtualization, not only the virtualized hypervisors can be hacked, but also the virtual images with functionality can be the target as well. The DoS threat in this category is caused by malicious virtual functions that can deplete the computing, network or storage resources. For edge setting, this threat is challenging to tackle since the hardware hosting edge servers are often of less resources.

Misuse of resources is another threat that is in the common form of botnet or bitcoin mining. This type is generated by adversaries that control the resources where they do not damage the MEC-Cloud infrastructure but use the resources for other purposes.

Privacy leakage is also a threat in virtualization category due to the open APIs offered by virtualization can provide lots of contextual meta data about the status of the hardware and the network. Such information can be used by adversaries to derive other types of attacks.

Privilege escalation threat is from the vulnerabilities of hypervisors and tampered virtual images. Due to potential isolation failure, compromised virtual service can manipulate other resources outside the regulated range. This threat can be escalated given that virtual images can migrate inside the MEC-Cloud infrastructure and hence quickly spread the threat.

- *End Devices*

  The end user devices are important part of the MEC-Cloud since the devices also consume the resources offered by 5G. The mobile devices also participate in the distribution of the resources in the overall ecosystem. Injection of information is a user driven threat where an end-device from adversary can be programmed to spread bogus data and even disturb the other devices sharing the same wireless communication link. Service manipulation is another threat from end devices where edge can be formed also by a cluster of end devices in device-to-device manner. In such case, adversaries that obtain control over one of the devices can gain access to other devices due to the fact that trust is often formed without strong verification.

[B] Security challenges and considerations for integrating MEC and Cloud to 5G

In 5G, one of the key challenges for deploying MEC-Cloud is security. In this regard, edge computing users in 5G face security challenges as being potentially vulnerable to security exploits since more and more IoT devices and applications are using the edge for data processing and storage. Such exposure of user data in MEC could introduce weak link where sensitive data can be breached. For example, IoT devices are typically programmed to trust other connected local devices and share data after simplified security check. In case such trust is natively enforced, it becomes difficult for MEC-Cloud to identify misbehaving ones. This can further create a disordered perimeter which prohibits security mechanism such as firewall to detect MEC security threats. In particular, it is challenging to balance the low-latency requirement and still being able to identify, authenticate and authorize data access in such distributed environment.

Besides general confidentiality, integrity and availability (CIA) requirements, MEC-Cloud need to consider the following general factors: 1) privileged user access: offloading sensitive data to the MEC-Cloud can lead to the loss of direct physical and personal control over the data. 2) regulatory compliance: MEC-Cloud run by 5G providers should be willing to undergo external audits and security certifications. 3) data location: the exact physical location of user's data is less transparent in MEC-Cloud, which may introduce confusion on specific jurisdictions and commitments on local privacy requirements. 4) data segregation: since data is usually stored in a shared space each user's data shall be separated from others with efficient encryption schemes. 5) resilience: MEC-Cloud needs to offer proper recovery mechanisms for data and services in case of technical l failures or other disasters. 6) investigative support: since logging and data for multiple customers may be co-located, investigating illegal or malicious activities can be a time-consuming process. 7) long-term viability: to assure that users' data is safe and accessible even if the MEC-Cloud providers may become out of business. 8) device identity: as devices in MEC-Cloud typically authenticate themselves via a cryptographic key, the protection of device identity keys is of paramount importance. 9) attestation: to prove that a device in MEC-Cloud is running up-to-date and patched code.

Given extensive discussions on edge and IoT security challenges (Hopkins, et al., 2019), (Hafeez, et al., 2018), (Singh, et al., 2016), there are six major categories for 5G deployment ranging from hardware components to distributed logging that need to be tackled in order to establish a sustainable ecosystem of MEC-Cloud.

- *Hardware component*

  As edge computing rests on edge hardware, there is a trend toward increasing computing power together with lower power consumption. This trend is enabling a rise in the capability of edge devices but not security yet. The cause is due to the fact there is little motivation at the current stage of edge computing since most of company prioritize the time-to-market instead of pushing security-first products. Even when hardware security features are available, the incorporation of such security support into the software is often missing. The trust of edge hardware is the very underpinning of secure edge computing but it only has value if integrated fully.

  There are hardware-based methods to build trusted edge computing nodes such as Trusted Platform Module (TPM) and hardware security module. Although such mechanisms for hardware trust can serve as a foundational building block for software security layers to depend on, there is a gap where the trust cannot be extended into the software infrastructure at the edge. This gap can affect the overall security of MEC-Cloud. Since deploying secure edge services to untrusted hardware can lead to fatal consequence, the hardware trust shall be the starting point on which all the other software components can be built.

  In particular to distributed edge hardware, one key challenge is to the integrity of a reliable source of information about the condition of the device. Using insecure/untrusted information about edge hardware can result in potential vulnerabilities. For administration and orchestration, it is desirable to verify the information concerning CPU spec, RAM and disk storage of MEC-Cloud devices from a trusted entity. Such information can be valuable for detecting potential violations such as unexpected CPU consumption. Other attributes such as battery level or GPS coordinates can be combined as well. For example, a sudden change of device's GPS coordinates could be used to lock certain functionality of the software given the risk that such static device could have been compromised.

  For 5G IoT deployment concern, physical security of MEC-Cloud cannot be taken for granted as to data center environment. For devices out in the field, accessing the hardware is hard to control. It is hence useful to treat low-level components as viable targets. In this regard, even firmware and debugging interfaces, which are often considered as protected, can be vulnerable to leak sensitive hardware data. This calls for the usage of hardware security such as TPM to form the base of hardware trust and to validate that status of hardware components. Besides components that can be covered by TPM, other parts including USB ports and external buses not covered by TPM can be the next targets. For MEC-Cloud, it is equally important to protect those peripheral from unauthorized access, which is still an open challenge. As to intrusion detection mechanisms on edge hardware, it is typically related to the scenario of physical case opening. Given that certain intrusion can be linked to digital sphere such as disabling the boot of hardware or causing misleading notification to MEC-Cloud hardware owner. It is hence useful to restrict software functionality in case of detecting malicious access so that further damage can be alleviated.

On top of the hardware trust, the authenticity of the hardware shall be further ensured. Even when edge hardware contains a root of trust technology implementation, and even if that root of trust is integrated with software layers above it, there may still be a foundational breach of security if the authenticity of the hardware cannot be assured. For example, a MEC-Cloud device that masks espionage functionality as a trusted device may appear as a normal one. For 5G infrastructure, these threats are typically reserved for nation-state threat level and such security challenge can go beyond the technology or architecture scopes. For business operations and supply chain management, this is still a valid concern given that the cost of replacing deployed edge devices can be higher than centralized setting. In addition, the chance of detecting such rogue hardware can be limited since the owner may not be able to physically verify certain devices that are deployed under remote and challenging conditions.

- *Connected devices*

One advantage for MEC-Cloud is that computing resources can process data closer to the source. For 5G IoT use cases, the source of data is often physically apart from the MEC-Cloud hardware, e.g., sensing devices such as sensors and cameras deployed in the same network shared with MEC-Cloud. For mission and safety critical scenarios, it is important to establish trust over the entire network of connected devices. Currently, this is one open challenge that is seeking scalable solutions.

Although it is necessary to establish trust among connected hardware, it is hard to verify the identity of large amount of sensing or actuators in 5G managed networks. In the regard, device identities shall be semantically defined to allow automatic verification. Currently there is a lack of standardized approach, which is creating problem given the diversity of edge and IoT hardware devices. Even for devices that entail certain identity, spoofing such unverified identity can still compromise the security. One potential approach is to define unified format for data exchange among connected hardware, but we still face the danger where malicious devices use proper format while the data is falsified. One example here is a smart home system that reacts to temperature reading for window opening. By generating false temperature readings, windows can be opened by attackers for stealing purposes.

In MEC-Cloud, once data enters the system, it can be stored, copied, forwarded, or used for analytics. When the data is passing through the network, it is hard to guarantee its integrity. This is similar for management commands between administration node and controlled devices. For instance, if door opening command can be spoofed or intercepted, it may result in intrusion and losses. For 5G industrial and mission-critical scenarios, commands such as "shut down" or "delete" can lead to catastrophic consequences. Even though we can add verification but it will introduce latency, which is unfavourable for many latency sensitive services. In addition, protecting data and commands typically involve encryption but the problem of establishing a trusted communication channel in such distributed environment is yet to be solved. At the same time, managing connected devices includes several procedures. In practice, open APIs are used to manage and query device related information. For services that involve production, one security challenge about how to prevent false information from generating wrong actions. In such cases, losses can be tangible in terms of money, time, materials.

- *System software*

System software security in MEC-Cloud is similar to the status of hardware security since existing methods are not integrated with service and infrastructure in 5G context. Regarding secure boot at system level, hardware approach such as TPM can be used to verify drivers and boot loaders. However, such attestation also relies on BIOS software that executes the required procedures. It is hence necessary to protect the integrity of BIOS on MEC-Cloud devices to form a secure chain between hardware and operating system.

Given the tight linkage of system software and hardware, rogue software can falsify or cancel the process of monitoring before other actions are invoked. It is hence a challenge as to how can actions be enforced as soon as detection of unauthorized software gets into the operating system. In addition, digital signatures for MEC-Cloud devices such as edge nodes and sensors can be used to verify device identifies but such methods rely on private keys. In cases where MEC-Cloud hardware can be physically accessed, attackers could copy such private key and then impersonate with the stolen identity. One challenge here is how to ensure the trusted identity is of integrity. If blind trust is placed, it can motivate attackers to harness such false sense of trust.

Although hardware level security implemented by Intel and AMD provides a starting point, such security systems are often in the form of a black box including the add-on features and potential vulnerabilities that might be exploited. In 5G deployment, once a MEC-Cloud server is started, it is necessary to update the security mechanisms at system software level. However, a secure delivery of updates also depends on the distribution servers which must be verified and trusted. This is yet not fully covered from communication perspective. For instance, using secure transport protocols such as TLS can effectively protect the data exchange in terms of integrity. Furthermore, even after update package is pushed to the edge nodes, it is still crucial to verify the signature of any software updates before installing the binaries.

- *Networking and communication*

  Networking issues in MEC-Cloud are due to the complexity of distributed architecture which is hard to protect in the same manner as to data centers with fixed cable connectivity. In this aspect, opening network ports with APIs is a common practice. Although such scheme is effective in a closed and centralized environment, it is challenging to copy the design to 5G scenarios where wireless communications are the dominant choice. For MEC-Cloud servers, open ports can expose vulnerability for local denial-of-service attack. Therefore, port-based access shall be limited to the minimum. To avoid exposing public ports, one common approach is to use VPNs to interconnect different MEC-Cloud servers. However, similar to the case of using fixed private keys, such fixed VPNs in a distributed environment may cause security issues since a stolen VPN connection (e.g., by physical tampering) can give attackers direct access to the private networks.

  In existing network design, credentials (e.g., in access control list) are used to prevent non-authorized connections from utilizing the APIs via open ports, but those credentials are often not tied to any particular network identity in most cases. Under such circumstance, even without access credentials, being physically on the network may allow an attacker to harness the software with invalid requests to form denial-of-service attacks. This challenge is critical for MEC-Cloud since physically tampering the network in distributed and wireless setting is of less effort in comparison with data center networks. Given the control role assigned to dedicated MEC-Cloud servers which entail credential stores, it is challenging to protect those servers from being physically hacked or attacking by rogue devices in the same network.

As MEC-Cloud heavily rely on wireless communications, wireless specific attacks such as jammers can result in similar damage as to denial-of-service attacks in the wired networks. Preventing such attacks requires changes to the firmware but it is challenging and of high cost to low-cost IoT devices. Most edge use cases make use of devices from multiple vendors. To date there has been no unified approach to solve this problem.

Another security issue in communication comes from the IoT devices. Sensing and actuation components in MEC-Cloud can be hacked to become part of the attack vector, and meanwhile they are also the target of attacks. For example, battery-powered sensors can be maliciously turned off by requesting them to respond to invalid requests via wireless so that the power of sensors are quickly drained in using wireless interfaces. This is special challenge for wireless driven MEC-Cloud.

- *MEC-Cloud service*

  MEC-Cloud runs virtualized and lightweight software, which is commonly referred as microservice. The integrity of such microservice need to be secure in order to guarantee a reliable operation environment. To prevent MEC-Cloud servers from running arbitrary codes, microservice images must be verified in terms of integrity. Especially for multi-tenant environment, such verification also needs to be efficient so to avoid using extra hardware resources that can affect other users sharing the same hardware. On shared hardware, unauthorized microservices shall be efficiently detected and removed. In addition, reports must be generated if there is any attempt to launch unauthorized microservices.

  Since microservices need configuration and credentials to function, it is important to avoid embed these sensitive data within the service images. One practical method is to obtain credentials via secure channel during runtime, and at the same time verify the integrity and identify. Furthermore, hardware components attached to MEC-Cloud servers such as serial port and wireless interfaces shall be accessible by microservices only when necessary. Since third-party software will be used by MEC-Cloud, access control must be enforced as well.

  Regarding authorization boundary, microservices running on dedicated servers can still conduct activities that are outside the expected range. For example, even microservices can access the data in an authorized way, but if they transfer the data to undefined or malicious entities outside the control boundary, the protection of data simply fails. It is hence important to monitor unwanted connections to ensure the MEC-Cloud infrastructure has a clear boundary for data privacy.

- Distributed logging at scale

  Logging and audit are important to ensure MEC-Cloud services are properly functioning and in compliance with contracts, laws and regulations. However, as the number of connected devices is increasing, the scale itself is becoming a challenge. In particular for MEC-Cloud environment, logging is often conducted in a distributed manner, i.e., over various deployed hardware, and can be diverse in terms of format. Even if the logging can be aggregated in a centralized location, it is challenging to meet the diverse goals from legal requirements by going through layers of hardware and software stacks. The multi-tenancy of MEC-Cloud further complicates the logging and audit since more volume and meta data need to be obtained to conduct fine-grained analysis.

Since logging in MEC-Cloud are partially decentralized, another consideration is the location awareness of logging. This is important for cases where many logging records are similar or duplicated. One approach to tackle this issue is by deploying logging analysis tools directly over such distributed logging data. In particular for storage overhead of logging, it is important to dynamically adjust the sampling ratio to capture threats while avoid unnecessary logging.

[C] Open Research Directions

Since the development of MEC-Cloud security is in its starting phase, the challenges and threats generate requirements for dedicated solutions. Specific for 5G, there are four open directions that deserve further investigations.

- *Trust Management* – for MEC-Cloud, trust goes beyond the basic authentication and shall handle the uncertainty as to what behaviours a device may take. Since the power of MEC-Cloud services comes from collaboration, which depends on trust, we need a reliable and deployable trust management solutions that can calculate trust metrics/reputation in an autonomous and distributed way. The interoperability is crucial for trust management of MEC-Cloud given the data and devices are geographically distributed.

- *Machine Learning (AI) based Security Enforcement* – given opportunities and data from the edge, machine learning is a potential domain to explore for security enforcement of MEC-Cloud. Due to the increasing amount of security exploits on resource constrained devices which will be the case for MEC-Cloud infrastructure, several security approaches for intrusion detection and classification can benefit from the data-driven suggestions/prediction of machine learning (Hafeez, 2018). Furthermore, the combination of cloud and edge in MEC-Cloud provides nature support for the mode of centralized model training and edge-based predication. Given the opportunity to obtain high-quality data from the network edge at scale, machine learning based security could help strike a balance between accuracy and latency.

- *Microservice Management* – fault tolerance and resilience are the key to success of 5G given the crucial role it will play in our society. The microservice is the core of MEC-Cloud that can promote the flexibility of service organization and diversity. Meanwhile, there is a lack of unified approach to securely delivery of secrets that are needed to manage a wide range of microservices in a decentralized manner. On top of migrating microservices, there is an urgent demand to allow guaranteed remote shutdown especially for safety or mission-critical services.

- *Hardware Assisted Security* – protecting hardware and hypervisor is a core subject for MEC-Cloud. Given the active research on trust platform module (TPM), the virtualized environment of MEC-Cloud calls for more dedicated solutions (Tian, 2017). Meanwhile, it is equally important to investigate hardware acceleration for security by using dedicated components such as GPU and FPGA (Volos, 2018).

Conclusion

Securing MEC-Cloud is crucial for the success of 5G deployment at large scale. The analysis on security requirements and the extensive discussions of existing solutions represent a clear interest and strong will from both academia and industry to address the open issues of the MEC-Cloud security in 5G. Although cloud security has been studied in the past, the combination of edge and cloud technologies has introduced new threats and risks. In particular for 5G IoT services, potential vulnerabilities are growing at an exponential rate as magnified by the rapid fusion of cyber and physical territory, the diversity of hardware, the heterogeneity of deployment scenarios, and lack of privacy awareness. All those add up the complexity to secure the inherently distributed 5G MEC-Cloud.

The discussions in this article serve as a stepping stone to expose key issues and reflect on the 5G specific security challenges for MEC-Cloud. By focusing on 5G domain, the presented overview and outlook shed light on the future development of security solutions that will tackle the threats and meet the dedicated requirements. As the field of MEC-Cloud matures, more robust and secure solutions are expected to be devised, and 5G customers will then embrace the benefits of MEC-Cloud. Nevertheless, the security of 5G MEC-Cloud is still in its initial stage. We need further investigations and research to address the open issues.

References

Fernandes, D. A. B. and et al. (2014) Security issues in cloud environments: a survey. International Journal of Information Security, 13(2), Springer-Verlag, pp 113-170.

Roman, R. and et al. (2018). Mobile edge computing, Fog et al.: A survey and analysis of security threats and challenges. In Future Generation Computer Systems, 78 (2), Elsevier, pp. 680-698.

Hopkins, K. and Bergquist, J. and Ortner, B. and Kröger, M. and Wong, S. (2019). Edge Security Challenges. White Paper.

Hafeez, I. and et al. (2018). Real-time IoT Device Activity Detection in Edge Networks. In Proceedings of the 12th International Conference on Network and System Security (NSS '18). Springer, pp. 221-236.

Singh, J. and et al. (2016). Twenty Security Considerations for Cloud-Supported Internet of Things. In IEEE Internet of Things Journal, 3(3), IEEE, pp. 269-284.

Ding, A.Y. and Janssen, M. (2018). Opportunities for Applications Using 5G Networks: Requirements, Challenges, and Outlook. In International Conference on Telecommunications and Remote Sensing. ACM, pp. 27-34.

Liyanage, M. and et al. (2018). A Comprehensive Guide to 5G Security. 1st edition. Wiley.

Ding, A. Y. and et al. (2015). Vision: Augmenting WiFi Offloading with An Open-source Collaborative Platform. In Proceedings of the 6th International Workshop on Mobile Cloud Computing and Services (MCS '15). ACM, pp. 44-48.

Cozzolino, V., Ding, A. Y. and Ott, J. (2017). FADES: Fine-Grained Edge Offloading with Unikernels. In Proceedings of ACM SIGCOMM Workshop on Hot Topics in Container Networking and Networked Systems (HotConNet '17). ACM, pp. 36-41.

Cuervo, E. and et al. (2010). MAUI: making smartphones last longer with code offload. In Proceedings of the 8th international conference on mobile systems, applications, and services (MobiSys'10). ACM, pp. 49-62.

Kosta, S. and et al. (2012). ThinkAir: Dynamic resource allocation and parallel execution in the cloud for mobile code offloading. In Proceedings of IEEE International Conference on Computer Communications (INFOCOM'12). IEEE, pp. 945-953.

Liyanage, M., Porambage, P. and Ding, A. Y. (2018). Five Driving Forces of Multi-Access Edge Computing. arXiv:1810.00827 [cs.NI], October 2018.

Haus, M. and et al. (2017). Security and Privacy in Device-to-Device (D2D) Communication: A Review. In IEEE Communications and Surveys, 19(2), IEEE, pp. 1054-1079.

Tian, H. and et al. (2017). SGXKernel: A Library Operating System Optimized for Intel SGX. In Proceedings of the Computing Frontiers Conference (CF'17), ACM, pp. 35-44.

Volos, S. and et al. (2018). Graviton: Trusted Execution Environments on GPUs, 13th USENIX Symposium on Operating Systems Design and Implementation (OSDI 18).