Cloud and MEC security

Chapter · January 2018

DOI: 10.1002/9781119293071.ch16

4 authors:

Jude Okwuibe
University of Oulu
14 PUBLICATIONS **138** CITATIONS
SEE PROFILE

Madhusanka Liyanage
University College Dublin
93 PUBLICATIONS **624** CITATIONS
SEE PROFILE

Ijaz Ahmad
University of Oulu
37 PUBLICATIONS **513** CITATIONS
SEE PROFILE

Mika Ylianttila
University of Oulu
203 PUBLICATIONS **2,858** CITATIONS
SEE PROFILE

16

Cloud and MEC Security

Jude Okwuibe, Madhusanka Liyanage, Ijaz Ahmad, and Mika Ylianttila

Centre for Wireless Communications, University of Oulu, Oulu, Finland

16.1 Introduction

The extreme capacity and performance demands of 5G networks will necessitate major changes in the way we produce and utilize digital services. 5G will usher in a massive array of new devices, services and use cases driven by technology developments and socio-economic transformations into the mobile network arena. Records will be set on every metric; ubiquitous ultra-broadband, virtual zero latency and gigabit experience will be the key defining features of the 5G networks. Certain key technologies and methods become pertinent towards the evolution to 5G; among these are *Cloud Computing* and *Multi-Access Edge Computing (MEC)*.

The relevance of cloud computing to mobile network has been on upward spiral over the last decade. Cloud computing provides on-demand computing resources and services on a scalable platform to both large and small organizations. At present, popular social media sites such as Facebook, Twitter, YouTube and Netflix are basically running on clouds. Besides, users are increasingly accustomed to carrying multiple mobile devices to meet their different lifestyle and work demands. This buttresses the need for cloud services in two ways; first, to ensure that user data is synchronized on all devices and second, to enable low storage devices to perform storage intensive operations leveraging on the cloud for virtual storage. This not only reduces cost of devices, but also extends battery life and improves overall user experience.

Another initiative for advancing the efficiency and dynamism in mobile networks is MEC. MEC is one of the most recent approaches towards the extension of cloud computing capabilities to the edge of the network. The main idea of the MEC initiative is bringing the clouds closer to the edge of the network as well as to the users.

A Comprehensive Guide to 5G Security, First Edition. Edited by Madhusanka Liyanage, Ijaz Ahmad, Ahmed Bux Abro, Andrei Gurtov, and Mika Ylianttila.

Other similar approaches are Cloudlets, Fog, Edge computing[1], as well as their hybrids. MEC combines elements of Information Technology (IT) and telecommunication networking, hence extending cloud computing capabilities and IT services to the edge of cellular networks. This minimizes network congestion and also improves the overall performance of the network.

Bootstrapping MEC and cloud computing with their various deployment models to 5G networks come with many benefits to both the cloud service providers (CSPs) and to businesses. Such benefits include providing internet-based services to both small and large organizations at a highly reduced cost, hence creating a level playing field for different levels of investments. Other benefits include cutting down operational costs through reduced backhaul capacity requirement, eliminating resource redundancy through the provision of pay-as-you-use services, providing access to applications based on need; that is, businesses can now easily increase or decrease their capacities without incurring any unwarranted costs, flexible and rapid application deployment, secure radio access provisioning to application developers and content providers, as well as faster response time for cloud applications through reduced end-to-end (E2E) network latency and thus better Quality of Experience (QoE) for fast moving user equipment.

However, these remarkable benefits are not offered without cost. Transitioning to MEC and cloud computing poses a number of security risks to the industry, most of which are covered in this chapter. On the side of cloud computing, the idea of relieving clients of direct control, and transferring both infrastructure and resource management to the CSP could lead to trust issues on the network. Moreover, the centralization of resources requires CSPs to frequently update their cloud security and privacy protection mechanisms, so as to keep pace with the rapid evolution of cloud computing technology [1]. On the side of MEC, the security and privacy concerns are even more threatening, given that MEC is still in its infancy. Security concerns are mainly in the context of the *cloud-enabled* IoT (Internet of Things) environment. Security technologies are geared towards the MEC nodes, for example, MEC servers and other IoT nodes. Threats such as *man-in-the-middle (MitM)* and *malicious mode problems* have been identified [2]. Here, we describe in detail, and in the context of 5G networks, the security vulnerabilities of both cloud computing and MEC. We define different use cases of each technology and outline different associated privacy and security threats, and then we propose adequate solutions to address these security concerns.

16.2 Cloud Computing in 5G Networks

The fifth generation of mobile network standards (5G) will support a massive number of connected devices and provide wireless connectivity for a wide range of new applications and use cases. Unlike the previous generations of mobile networks, the

1 There is a common misappropriation between edge computing and mobile edge computing. In contrast, edge computing comprises all technologies that leverage on distributed IT architecture to provide a means of collecting and processing data at local computing devices rather than in the cloud or remote data center, while mobile edge computing is one instance of edge computing at cellular base stations where cloud computing capabilities are moved to the edge of the cellular network. Other instances of edge computing are peer-to-peer ad hoc networking, fog/cloud/cloudlets, autonomic self-healing networks and dew computing.

5G network design is inspired by the need for more user-centric services across all network paraphernalia. Both existing and evolving systems, such as LTE-Advanced and WiFi, will be harnessed together with other revolutionary technologies in order to meet the anticipated performance demands of 5G. The Radio Access Technologies (RATs) of 5G will consist of existing RATs, licensed and unlicensed, supported by some novel RATs to support specific deployment scenarios and use cases, especially for ultra-dense deployments [3,4].

In all its ramifications, experts have shown that 5G mobile networks will be heavily supported by cloud services [3–5], whether for self-backhauling or for direct device-to-device (D2D) connectivity. Already cloud-based applications and storage are becoming common in modern networks; this is evident in the recent growth of uplink data in mobile networks. By integrating large-scale cloud architectures, 5G mobile networks need to be able to deliver services flexibly at unprecedented speeds to match the predicted growth in mobile data traffic that will be generated by mobile cloud services. In addition, the radio access infrastructure of 5G will largely depend on cloud architecture technologies for on-demand resource processing, storage and network capacity provisioning [5].

16.2.1 Overview and History of Cloud Computing

The actual origin of the term "cloud" in the context of computing has remained unclear in the literature; however, most technology historians agree that the idea of the cloud came originally from basic *virtualization* of IT infrastructures [7–10]. Prior to adopting the conventional term "cloud", IT specialist had long practiced the art of replacing actual IT infrastructures with their virtual equivalents. This was initially adopted as a cost-saving strategy, but soon it also became a feasible means of improving flexibility and enhancing the speed of communication networks [6].

The initial idea of what we commonly refer to as "cloud computing" today can be traced back in the 1950s, when firms and organizations began to adopt and optimize the use of large-scale mainframe computers by allowing multiple users simultaneous access to both hardware resources and shared central processing units (CPUs). Companies like IBM and DEC were known for such solutions at the time. Going through the 1960s to the mid-1990s, the idea of cloud computing had evolved through various significant phases and milestones. This includes the *ARPANET* in the late 1960s and 1970s, the *CSNET* in the early 1980s and the *Telescript* in the mid-1990s. However, the most remarkable evolution was seen in the late 1990s, when the *Web 2.0* was introduced; for the first time in computing history, enterprise applications were able to be delivered over the internet [8]. Salesforce.com was a key player at this time, being one of the first companies to experiment with the idea of delivering contents over the web. About the same time, the *Virtual Private Network (VPN)* was born, allowing interconnection between multiple private networks over a public shared network such as the Internet.

The modern version of cloud computing came in the early 2000s after the dot-com bubble burst, with Amazon taking the lead with the implementation of a fully web-based retail service in 2002. Another milestone to cloud computing was seen in 2006 when Google launched its *Google Docs* services, which brought cloud computing services directly to end users [10,11]. In late 2000s, the advent of low-cost, high-capacity network and storage devices and infrastructures led to a wider adoption of the cloud

concept, with big players like NASA, Microsoft, IBM and Oracle all getting on board. At present, Oracle is in a bid to further the course of the cloud into the next generation of computing. With the goal of integrating all key IT service layers to the cloud, that is, the Applications (SaaS), the Platform (PaaS), and the Infrastructure (IaaS), this will become a key component of the modern cloud computing architecture.

16.2.2 Cloud Computing Architecture

The architecture of the cloud presented in Figure 16.1 consists of the essential components and characteristics, as well as the deployment and service models of modern-day cloud computing infrastructure. Together, these components are able to provide clients with the essential features for which the cloud is designed; such features as on-demand self-service, resource pooling, rapid elasticity, disaster recovery and broad network access [12].

The overall cloud architecture is grouped into two sections, the *front-end* and *back-end* platforms, both connected via a virtual network interface or the Internet, as shown in Figure 16.2.

- The *front-end* platform, also referred to as the client platform, consists mainly of applications and interfaces required to access the cloud system. Applications may vary, depending on the nature of cloud services. Email services, for instance, rely on the use of traditional web browsing apps like Chrome, Firefox, and Microsoft Edge, while file management cloud services may rely on the Windows Explorer application.

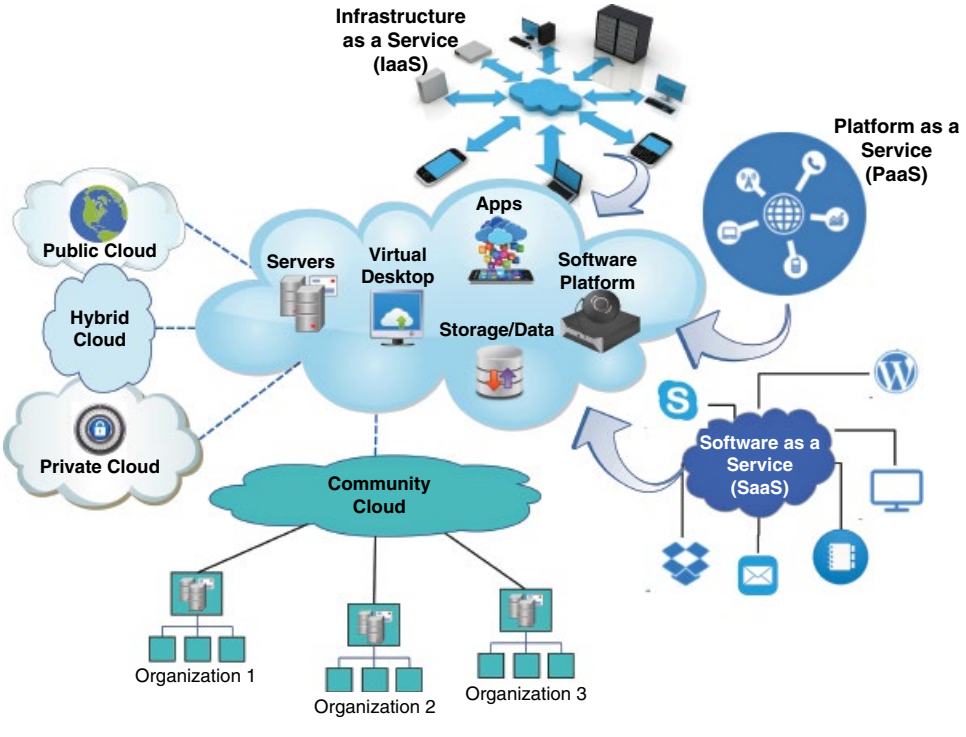

Figure 16.1 A view of the cloud architecture.

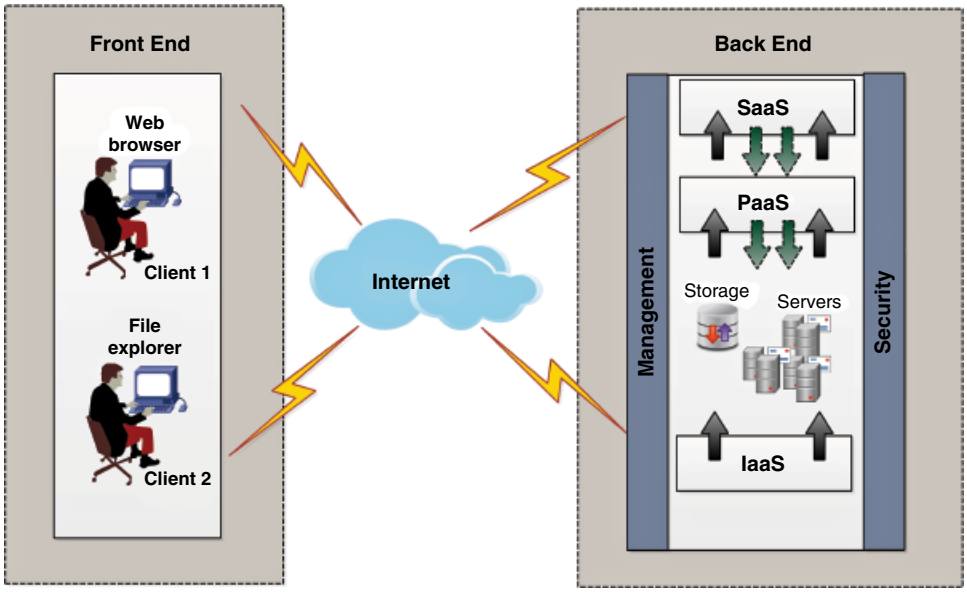

Figure 16.2 Front-end and back-end view of the cloud architecture.

- The *back-end* platform is the core part of the cloud computing architecture, also referred to as the "cloud". The back-end platform is managed by the cloud service providers; it includes the servers, the cloud storage systems, and the virtual machines. It is in the back-end platform that the protocols designed to run the cloud computing platform run. It is also on this platform that the security mechanisms and traffic control of the cloud platform are provided.

16.2.3 Cloud Deployment Models

Due to several foreseen security and privacy concerns in the cloud environment, different deployment models have been designed to meet different levels of security and privacy for both the cloud infrastructure and stored user data. Four main deployment models are identified:

1) *Private Cloud*: The cloud infrastructure in this model is designed to serve the exclusive needs of a given enterprise or organization. These infrastructures may be hosted within or outside the enterprise and can be managed by either the enterprise or a third party. This deployment model demands more capital investment (CAPEX), especially for the hardware requirements. It is also most vulnerable to security and privacy threats, given that access must be exclusive to only the enterprise and with third-party service providers, trust issues may also arise.
2) *Public Cloud*: Provides cloud infrastructure for use by the general public. Public clouds share similar or the same architectural features as other deployment models. The key difference comes in their security and privacy policies. Public clouds are the most recognizable model of cloud computing. CSPs, such as Google and Microsoft,

and Amazon Web Service (AWS), offer several free cloud services to the public and these services are easily accessible over the Internet.

3) *Hybrid Cloud*: Integrates two or more distinct cloud servers to provide cloud infrastructure for different use cases. The idea is to combine the benefits of multiple deployment models. Cloud servers in hybrid clouds could be either a combination of private, public or community clouds. One of the popular use cases of hybrid clouds is in enhancing security and privacy on the cloud without incurring the overhead costs (CAPEX) of building a private cloud. In this case, non-critical resources like test workloads can be hosted in the public cloud, while critical resources like user data and workloads are hosted internally.
4) *Community Cloud*: A multi-tenant model that provides cloud computing infrastructures to multiple organizations within a specific community, who share common interests or concerns. Similar to the hybrid model, the infrastructures in this model could be placed within or outside these communities, and could be managed either internally or by a third party. Usually, the cost of running community clouds are distributed among selected members of the community and not each individual user [12,13].

16.2.4 Cloud Service Models

Different levels of abstraction constitute the back-end platform of the cloud architecture. These abstractions are grouped into the different service levels, depending on what resources are offered as a service for a given abstraction level, and this is depicted in Figure 16.2. According to National Institute of Standards and Technology (NIST), the three standard cloud service models are *Platform as a Service (PaaS), Software as a Service (SaaS)*, and *Infrastructure as a Service (IaaS)* [12]:

- *Platform as a Service (PaaS)*: The transmission of platforms directly as services on the cloud is one of the integrated set of IT solutions that cloud computing provides. Typically, computer programs and mobile applications rely on some sort of middleware platform; this could be a set of hardware, combined with an Operating System (OS) and some libraries. PaaS provides this platform from the cloud, hence allowing users to develop and run applications without the overhead cost (CAPEX) of building and maintaining separate platforms [12,14].
- *Software as a Service (SaaS)*: Presently, SaaS is the most widely-used cloud service model in the IT industry. Using SaaS, a software application is hosted on the cloud and licensed to multiple users who are normally isolated from each other. Such services could be offered for free or on a pay-per-use basis over the web. Access is usually through some lightweight client interface such as a web browser [14]. Companies such as Adobe, Google, Microsoft, Facebook and Salesforce have been offering such services, some for decades now. Software applications such as MS Word, Excel, Whatsapp, Skype, and several others are now offered as SaaS through traditional web browsers.
- *Infrastructure as a Service (IaaS)*: This is the earliest and most fundamental cloud service model in computing. Long before the term IaaS was used, organizations were already optimizing their large-scale mainframe computers by allowing multiple users simultaneous access to both hardware resources and shared CPUs. IaaS may include virtual machines (VMs), servers, storage, network connectivity, firewalls and VLANs, all offered to users as provisioned services.

16.2.5 5G Cloud Computing Architecture

Cloud computing is one of the key technologies that will drive the evolution towards 5G mobile networks. According to the 5G Infrastructure Public-Private Partnership (5G PPP) Architecture Working Group, the overall 5G network architecture will be driven by an extreme demand for flexibility and programmability across all non-radio network segments, ranging from the fronthaul to the backhaul networks. Flexibility and programmability will also extend to mobile networks, access networks, core networks, and aggregation networks, as well as other evolving network segments such as the mobile edge networks, IoT networks, satellite networks, and the software defined cloud networks [15,16].

The 5G evolution will advance the convergence of multiple heterogeneous network environments, hence integrating a wide variety of network technologies for radio access and also introducing some novel access technologies to support specific deployment scenarios and use cases. Cloud computing capabilities will be leveraged to provision services at different network segments of the 5G network, from the Core Network (CN) segment to the Radio Access Network (RAN) segments, as shown in Figure 16.3.

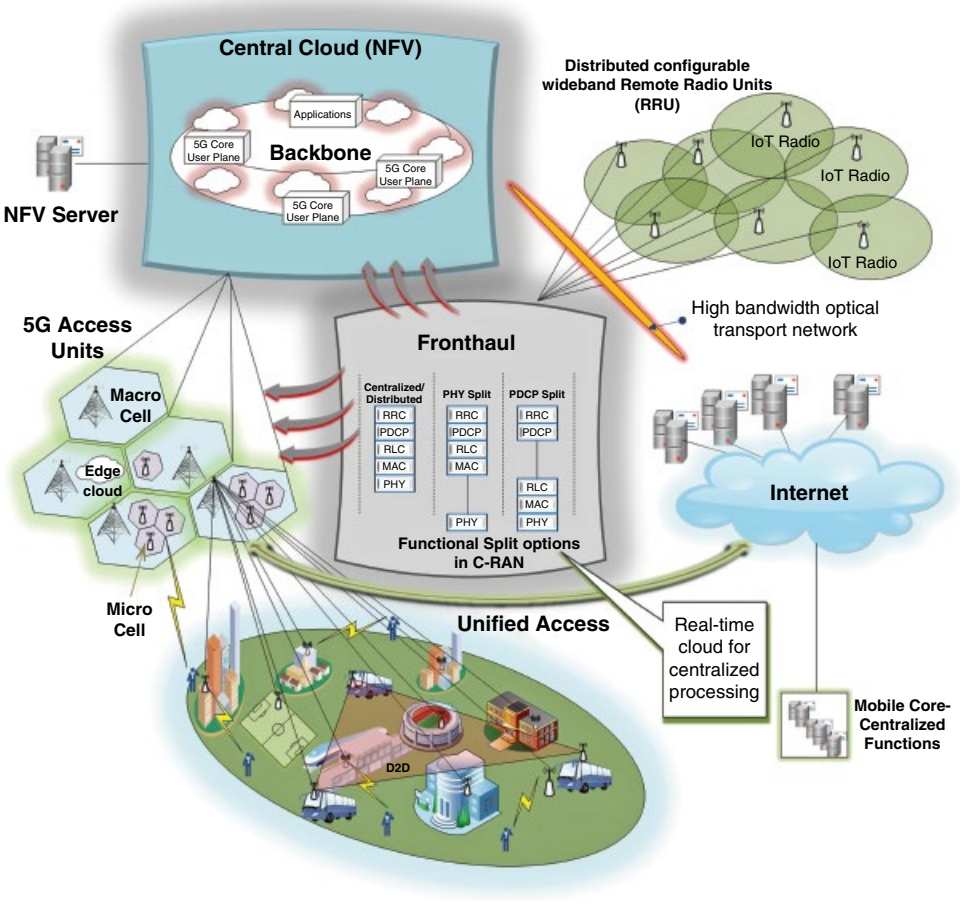

Figure 16.3 5G cloud computing architectures.

- *Cloud Computing in 5G Core Network*: The majority of 5G service plane and core network functions are anticipated to be deployed on cloud computing infrastructures. Cloud computing will be leveraged to handle various core network and service plane functions that are typical on cellular networks. These include multi-domain orchestration, service invocation, end-to-end (E2E) network slicing, and other service-tailored networks functions [16]. Traditional core network functions such as Authentication, Authorizations, and Accounting (AAA), security, traffic control and mobility management are also expected to be provisioned by cloud services.
- *Cloud Computing in 5G RAN*: The 5G framework proposes a novel radio access infrastructure based on cloud architecture technologies, using a scheme called Cloud RAN (C-RAN). Apparently, 5G mobile network will integrate existing RANs with novel access technologies in order to meet its performance and capacity demands; this combination will form the overall 5G RAT family. C-RAN is a novel access technology designed to extend Network Functions Virtualization (NFV) capabilities to the radio interface of future cellular networks. The overall idea of C-RAN is to promote spectral efficiency and multilayer interworking to support different use cases and technologies in 5G networks. C-RAN combines real-time virtualization and centralized baseband unit (BBU) pools to achieve large-scale centralized base station deployment on cellular networks [17].

16.2.6 Use Cases/Scenarios of Cloud Computing in 5G

Experts have defined and are already experimenting with numerous use cases of 5G networks. These use cases come from all major industries across the world, including manufacturing, healthcare, telecommunications, energy, TV and media, transportation, as well as other infrastructures. Although different use cases may tend to have different characteristics; however, for ease of understanding and clarity, METIS[2] and other groups like the 5G-PPP Architecture Working Group recognize a first-level grouping of 5G use cases into three main categories, namely *Extreme Mobile Broadband (xMBB)*, *Massive Machine-type Communications (mMTC)*, and *Ultra-reliable Machine-type Communications* [16,18]. Although this grouping provides a more or less generic view of all anticipated use cases in 5G networks, it is typical for several use cases to require similar network characteristics; hence, virtually all use cases will fall under one of these categories. Here we discuss each of these categories in the context of cloud computing:

- *Extreme Mobile Broadband (xMBB)*: This group of use cases requires reliable provisioning of gigabytes on-demand bandwidth to support extreme business agility and guaranteed moderate rates to support less demanding applications on 5G networks. Typical use cases under this group are Virtual Interactive Presence and Augmented Reality (VIPAR) used in telemedicine, augmented reality, and telepresence. The key enablers to this group of use cases are C-RAN and Mobile Cloud Computing (MCC). By ensuring unified dynamic operations on the radio

2 Mobile and wireless communications enablers for Twenty-twenty (2020) Information Society.

access networks, cloud computing sets to enable broader network access to such applications through rapid elasticity and resource pooling.

- *Massive Machine-type Communications (mMTC)*: The main characteristic of this use case category is the massive number of connected devices. These use cases depend on the interworking of billions of sensors and actuators to support a huge number of low-cost and energy-constrained devices. Typical use cases under this group are mission-critical machine type communications such as remote surgery, industrial process automations, smart grids and intelligent transport systems. With the emphasis on latency, reliability and availability, the role of mobile edge clouds becomes essential in these uses cases.
- *Ultra-reliable Machine-type Communications (uMTC)*: These use cases are mainly characterized by high reliability and availability. Time-critical services and applications such as industrial control applications, V2X[3], tactile network applications, autonomous driving, remote control over robots, IoT and other critical machine-type communications fall under this category. The major requirements for these use cases are fast discovery, immediate communication establishment, sporadic data handling and reliable feedbacks. The key enablers for the uMTC use cases are cloud storage and unified radio interface which is found in C-RAN [18].

16.3 MEC in 5G Networks

Virtualization and programmability introduces a major paradigm shift in the evolution towards the next generation of mobile networks. With virtualization, certain network functions, which are usually provisioned by proprietary network elements, are replaced with some form of virtual infrastructure like the cloud, with the aim of providing on-demand; cost-efficient and service oriented network services on-the-fly. Mobile Edge Computing (MEC) is an archetype of such virtualization at the edge of cellular networks, with an aim to reduce congestion at the core of the network; MEC is envisioned to be one of the driving technologies towards the 5G evolution.

16.3.1 Overview of MEC Computing

MEC is a new technology that is currently being standardized by the ETSI[4] MEC Industry Specification Group (ISG), a European standard institute for Information and Communications Technologies (ICT). ETSI envisions that by providing IT and cloud computing capabilities within the RAN at the edge of mobile networks, developers and content providers can have direct access to real-time radio access information, this will also promote ultra-low latency, provide higher bandwidth and ensure improved overall user experience [19].

The MEC architecture is mainly a complementary unification of information technology and telecommunication domains in a virtualized platform served through a MEC hosting infrastructure, as shown in Figure 16.4. MEC mainly incorporates

3 Vehicle-to-Vehicle/Infrastructure.
4 European Telecommunications Standards Institute.

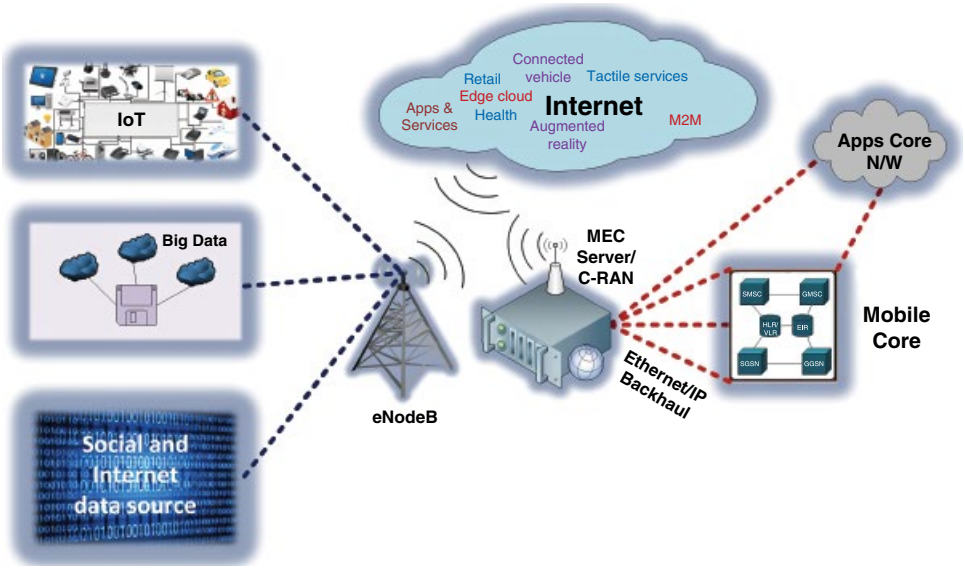

Figure 16.4 MEC system reference model.

application server platform into mobile base stations, its key characterizing features being proximity to data source, application services, RAN technologies and users [20]. MEC offers the following benefits:

- *Reduced Latency*: Extending computing resources to the edge of the network means faster arrival for network packets, and hence faster starts for streamed and real-time contents. MEC eliminates lengthy round trip delays to central servers and provides local support for application services, making the network more suitable for time-sensitive applications such as augmented reality and tactile networks thus allowing mobile devices to run computation-intensive and latency-critical applications more effectively. This also translates into improved QoE for the consumers [20].
- *Higher Efficiency Gains*: By storing contents locally at the edge of mobile networks closer to user applications, the need for frequent traveling of data through the backhaul channel is largely reduced, hence increasing efficiency gains. Contents targeted for the backhaul channel are more efficiently transmitted through opportunistic networking techniques, thereby reducing the signal load of the core network.
- *Backhaul Capacity Gains*: This comes from the reduced volume of signaling on the core network. Content caching has shown the potential for up to 35% reduction in backhaul capacity requirement [22]. Caching of local Domain Name System (DNS) could result to as much as 20% reduction in content download time [21].
- *Cost Savings*: This comes in multiple folds; first we have major cost savings on data delivery and in processing power and energy requirements; this constitutes a major part of the CAPEX for service providers. Then we also have some critical backhaul expenditure savings, which translates into reduced OPEX.
- *Real-time RAN Information*: This benefit is mainly experienced by application designers and content providers. With MEC, operators can open their RAN edge to authorized third parties, hence providing real-time network information at the edge

of the network, where they can easily be accessed and used by developers to optimize user applications. In turn, the RAN provider is able to utilize information from such third parties to make more efficient resource allocations decisions on the network.

16.3.2 MEC in 5G

Network softwarization will be a major driving force for the evolution towards 5G. Emerging technologies such as Software Defined Networking (SDN), Network Functions Virtualization (NFV), Fog Computing and MEC, will play a critical role in this process. The overall target of these technologies is to advance agility, flexibility and scalability at various points on the network. MEC extends IT services and cloud-computing capabilities to the edge of the network away from centralized nodes. It also extends similar functionalities to the radio access networks and to the mobile subscribers. For operators, MEC platform enables them to provide new services through the open RAN edge; this allows application designers to offer over-the-top (OTT) services using the MEC servers.

It suffices to say that MEC as a technology is still relatively in its infancy. However, according to 5G-PPP, MEC is one of the key technologies and architectural concepts that will drive the evolution to 5G networks. Other related technologies are SDN and NFV. MEC will contribute by no small measure in the realization of the cardinal objectives of 5G in terms of throughput, latency, scalability and automation [23]. MEC will serve as a key enabler to edge applications on 5G, while NFV[5] will be focused on the network functions. With the emphasis on infrastructure re-use, these twin concepts could quite readily be combined in a complementary fashion; hence the 5G design makes provision for a dual hosting of both Virtual Network Functions (VNF) and MEC using the same saver. The benefit to this modality comes from optimal infrastructure re-use, which constitutes a major savings on investment [25]. The MEC server is designed for optimal softwarization of functions and efficient infrastructure utilization [26]. As shown in Figure 16.5, all MEC applications and application platform services are software applications running on hardware components. With this design, it is possible to lower the cost of hardware components by combining off-the-shelf components with function virtualizations. For instance, the MEC virtualization manager layer depicted in Figure 16.5 provides IaaS facilities, which will provision for flexible and efficient multi-tenancy, run-time and hosting environment for MEC application platform services [27].

The need for MEC comes natural with the convergence of IT and telecommunications networking. MEC proposes a paradigm shift in existing communication ecosystems that will enable a new vertical business segment and services for both consumers and enterprise customers. By allowing for content caching at the network edge, the core network is relieved of congestion, hence providing a more efficient platform for resource-demanding applications and use cases at the edge, such as augmented reality, video analytics, location services, IoT and other such use cases [24]. The next subsection provides more information on some of these use cases.

---

5 NFV and MEC tend to co-exist in many technical contexts, because they are similar in various ways and also have similar origin; however, they are unique in the network segments they target, while NFV is targeted towards a variety of network functions and applications, i.e. routing, security, firewall, and VPNs. MEC is mainly targeted towards functions associated with wireless services at the edge of the RAN.

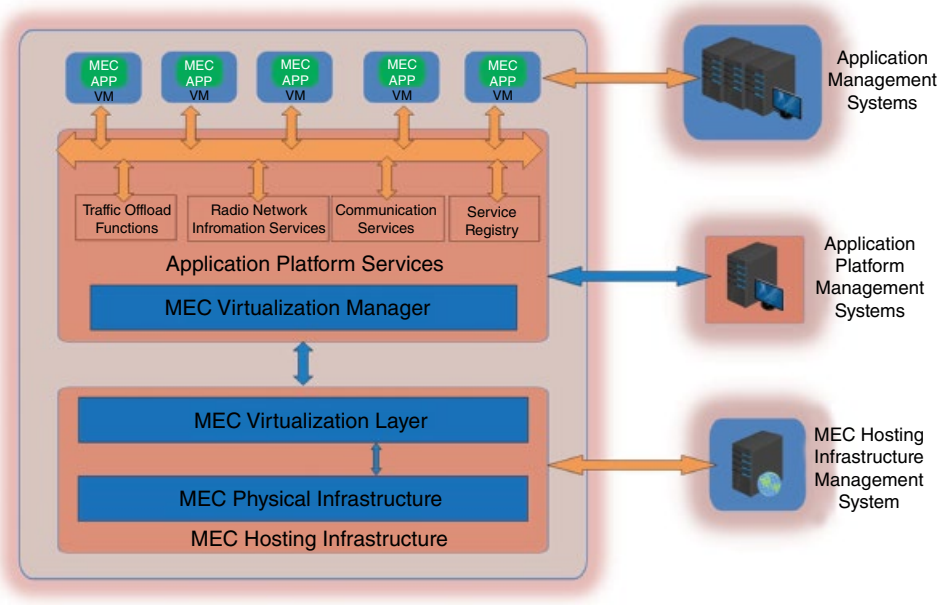

Figure 16.5 MEC server platform.

16.3.3 Use Cases of MEC Computing in 5G

The open architecture of MEC makes is a suitable option for a number of novel applications and use cases. However, given that MEC is still in its infancy, most of its potential use cases and scenarios are not typical in the current networking environment. With existing network infrastructure, a few use cases are already being tested and verified; among these are active device location tracking and distributed content and Domain Name System (DNS) caching:

- *Active Device Location Tracking*: This use case combines a third-party geo-location algorithm with an MEC-based application to perform real-time network measurement. This enables the tracking of devices without reliance on conventional Global Positioning System (GPS) devices.
- *Distributed Content and DNS Caching*: Just like the caching services in conventional web browsers speeding up access to frequently visited sites, this use case is made effective by minimizing the load at the server through caching, hence providing faster data delivery to customers. According to a report by BT TSO – Research & Technology, content caching has the potential to reduce backhaul capacity requirements by up to 35%. Local Domain Name System (DNS) caching can reduce web page download time by 20% [29].

Other experimental use cases of MEC include:

- *Video Analytics*: which uses a video management application to process and store video data, and using some predefined algorithms; it occasionally collects new video streams and compares with pre-recorded streams to detect changes in the environment. Typical applications under this use case are the smart city and public security [28].

- *Augmented Reality*: Here the MEC server uses real-time tracking and content caching to support augmented reality contents on mobile devices. The key driver for this use case is reduced round-trip-time (RTT) and higher throughput.
- *RAN-Aware Content Optimization*: By providing accurate real-time subscriber RAN information to the content optimizer, MEC helps providers achieve dynamic content optimization, and improved QoE and overall network efficiency, which stirs novel services and revenue opportunities on the network [28].

16.4 Security Challenges in 5G Cloud

With the advent of 5G networks, myriads of new businesses, trust models, new mobile technologies and new service delivery models will gain momentum on a global scale. 5G will play active roles in almost all aspects of our day-to-day life. This evolution will attract a corresponding evolution in the threat landscape and increase privacy in concerns at different application areas, hence security and privacy will play a central role in the evolution towards 5G.

The security and privacy concerns in 5G will span beyond technologies involving regulation and legal frameworks. Certain use cases pose special security concerns due to the nature of the applications they support. For instance, in online business, security concerns are indispensable to all parties, as a breach in security can lead to major flaws in trust among transacting parties and this could stagnate the adoption of certain novel technologies in 5G. Moreover, one of the cardinal goals of 5G is to realize a communication network that is more user-centric than previous generations. An indicator to this goal is that users become more aware of the nature of services they receive and the corresponding security vulnerabilities associated with these services. Hence, a highly optimized service with a porous security or privacy model could easily be rejected by users. With big data analytics, such security and privacy concerns become even more threatening. With unification of multiple communication domains, a security breach in one network segment could result to a ripple-effect across other segments. In this section, we discuss the security vulnerabilities that come with the cloudification of services on different segments of the 5G networks.

16.4.1 Virtualization Security

As discussed in previous sections, virtualization is the main driving force to cloud computing. Obviously, cloud computing will leverage on multiple virtualized systems in order to optimize available resources and deliver on its proposed benefits. The term "cloud" was initially adopted in science to represent a high level of abstraction in describing a collection of resources whose complexities are left undefined in a given context. This interpretation still remains relevant in defining cloud computing. Users still lack a clear understanding of the modalities to the processing and storage of their data, the location of storage, and the security of the entire process.

Security concerns with virtualization may range from potentials for data misplacement to Denial of Service (DoS) attacks. In [30], Lindstrom outlines five key security concerns of virtualization, which he called the *five immutable laws of virtualization security*:

1) An attack on a virtualized system is tantamount to attacking the actual hardware components that is virtualizes;
2) Security vulnerability of a virtualized system is the combination of actual system vulnerabilities and the vulnerabilities of the hypervisor[6];
3) Security on virtualized systems can be improved by separating functionality and content, e.g. separating the user data from the network functions;
4) Aggregating multiple virtualization platforms on the same physical systems will increase risk, except if the hypervisor is configured to avert this risk; and
5) A trusted virtualized system on a mistrusted infrastructure is at higher risk than a mistrusted virtualized system on a trusted infrastructure.

16.4.2 Cyber-Physical System (CPS) Security

CPS integrates multiple networking, computing and physical resources on different spatial scales controlled by computer-based algorithms. CSPs consist of several communication technologies, sensors and actuators all linked together over a software system. Typical applications CPSs include monitoring and control of physical and organizational or business processes, for example, SCADA[7], integration of different technical disciplines and application domains, for example, smart grids, distributed or interconnected systems of systems, as well as other sensor based smart communication systems [31].

Cloud-based Cyber-Physical Systems (CCPS) use *Cyber-Physical Clouds (CPC)* for the virtualization of network components like sensors and actuators. These virtualized components function as conventional cloud resources that can be provisioned for cloud services. CPCs are prone to several identified security attacks, such as *HTTP* and *XML Denial of Service (HX-DoS)* attacks. HX-DoS combines HTTP and XML messages flooded at rates deliberately meant to overwhelm the cloud CPS infrastructures. This attack can be lunched on any cloud service models, that is, IaaS, SaaS and PaaS. In [32], authors present a defense system called Pre-Decision, Advance Decision, Learning System (ENDER); this system is designed to identify the HX-DoS messages before they are received by the targeted system. Another common attack on CPC is Slowly-increasing Polymorphic DDoS Attack Strategy (SIPDAS), identified in [33]. SIPDAS mainly characterizes DoS attacks that dynamically modify their behavior to evade pattern detection algorithms. Possible control measure to this attack is to frequently check the consumption of computational resources, as well as the intensity of incoming requests [33].

16.4.3 Secure and Private Data Computation

With cloud computing, user data is usually stored in the CSP data centers, which are usually unknown to the user. The security of such user data is crucial in any network environments and even more critical in cloud computing, given that user data could more easily be moved to any location on the globe over the clouds. It is therefore the responsibility of the CSP to ensure that both their infrastructures, user data and applications are protected.

---

6 In a virtualized system, the hypervisor is the software or firmware that controls the system. In this case, it is the cloud operating system. More common hypervisors are VMware and VirtualBox.

7 Supervisory Control and Data Acquisition

Several possibilities of attacks exist in this realm. One of the most threatening is the *insider attack*; this is considered as one of the largest threats in cloud computing as a whole [34]. Insiders in this context are the CSP staff with access to the physical servers on which user data is stored. Possible ways to mitigate this risk is for the CSP to ensure well coordinated routine background checks for such employees. Other related security threats are:

- *Abuse and nefarious use of cloud*: where CSPs offer cloud access to anonymous users who may turn out to be criminals or malicious code authors;
- *Insecure interfaces and APIs*: where CSPs provide customers with porous APIs, e.g. APIs that allow for anonymous access or clear-text authentication;
- *Shared infrastructure*: where different CSPs share common infrastructures such as CPU caches and GPUs, hence extending user data security risks beyond the actual CSP;
- *Data loss or leakage*: could be in the form of deletion or alteration of data without adequate backup facilities for recovery [34].

16.4.4 Cloud Intrusion

Cloud intrusion affects the availability, confidentiality and integrity of cloud resources and services. Intrusion could come in various forms, depending on the level of sophistication of the intruder and the nature of loopholes and weak links on the cloud environments. Intrusion may range from hobbyist hackers, to organized crime, to corporate espionage, or even nation-state sponsored intrusions.

The most conventional means to mitigating the possibilities of cloud intrusion is by building *intrusion detection systems (IDS)* and other control mechanisms in the cloud computing environment. The IDS monitors the cloud environment for malicious activities and policy violations. IDS could be attached to any of the cloud service models – IaaS, SaaS, PaaS; it can also be extended to network hosts as well as the hypervisor. In [35], Cox discussed evolving and advanced IDSs required in the cloud environment; these include the hypervisor-based intrusion detection system, traditional host intrusion detection system (HIDS), and network intrusion detection system (NIDS), and he recommends HIDS to be deployed on both the front and back end of the cloud architecture, while NIDS and hypervisor-based intrusion detection system should be completely left to the back-end where the CSPs operate. Another workable but rather passive approach to addressing such challenges is building intrusion-tolerant cloud applications, which are capable of ignoring potential malevolent requests. The limitation to this approach is that intruders could easily circumvent the mechanisms of such controls over time; hence the CSP will need to keep pace with evolving intrusion patterns.

16.4.5 Access Control

The cloud environment is a large open distributed system; therefore migrating to cloud technologies implies certain levels of access sharing on both data and network infrastructures. The main function of access control is to ensure that only authorized users are granted access to data and network infrastructure. Additional functions may include

monitoring and recording of unauthorized users attempting to access the system. Several access control models have been identified, ranging from traditional Mandatory Access Control (MAC), to Discretionary Access Control (DAC) and Role Based Access Control (RBAC)[36].

These access control models are mainly based on user identity, where a unique identifier is applied to each user, and upon successful authentication, users are granted access to corresponding resources. In the cloud environment, there is a need for a flexible access control mechanism to support various kinds of domains and policies. Access control goes beyond controlling access to resources and the system itself; it also includes the management of users, files and other resources. Typical access control system consists of functions such as authentication, authorization and accountability. In [37], the authors discuss the loopholes in the above access control methods and why they may not be suitable for the cloud computing environment. The MAC model does not guarantee complete secrecy of information, since it does not support the separation of duties and privileges, moreover it does not always support dynamic activation of access rights for certain tasks. The DAC model, which tends to be more flexible, lacks adequate mechanisms for managing improper rights, hence less risk-aware, and this makes it unsuitable for the access control level require in cloud computing. RBAC seems more advantageous in many cases; however, it also lacks adequate dynamism to its access control methods, for instance, it lacks the ability to classify information according to sensitivity levels, which will be a major requirement in the cloud environment, given that certain information is less sensitive than others. RBAC also lacks delegation mechanisms needed in organizations for situations where certain staff members are absent.

16.5 Security Challenges in 5G MEC

The MEC network environment comprises multiples diverse technologies, including wireless networking, distributed computing, and the virtualization of networking equipment and computing servers all interoperating in an open ecosystem where service providers can deploy their applications. The heterogeneity and diversity of the MEC environment opens up a series of avenues for malicious attacks and privacy issues that could constitute a major threat to the entire MEC system. By extending IT services and cloud computing capabilities to the edge of mobile networks, the MEC platform tends to have a limited size of hosts at the mobile edge, which cannot enjoy the same level of protection as conventional large data centers, hence the need for more robust security measures to mitigate these security challenges on such network edges.

In addition, the MEC system is still in its infancy, hence the security concerns are mainly in the context of a *cloud-enabled* IoT environment. Security technologies are geared towards the MEC nodes, for example, MEC server and other IoT nodes. Threats such as *man-in-the-middle (MitM)* and *malicious mode problems* have been identified [2,38]. In [38], the authors present a broad threat description model for the MEC system; this section discusses the threat landscape of the MEC system and why security is one of the greatest challenges of the MEC system. In Section 16.7, we suggest workable mitigation techniques that could be used to avert these security challenges.

16.5.1 Denial of Service (DoS) Attack

DoS attack is an age-long threat in various computing and networking arenas. DoS creates an artificial scarcity or lack of online resources and network services. DoS attacks could happen in the form of distributed denial-of-service (DDoS) or wireless jamming and could be launched on both the virtualization and network infrastructures. In the case of MEC systems, DoS attacks have limited scope, as described in [38], as a DoS attack on the network edge will affect only the attacked vicinity and not the entire network. So also an attack on the core network infrastructure might not lead to a complete disruption in the functionality of the edge data centers. This is due to the autonomous and semi-autonomous nature of their protocols and services.

Another loophole in the MEC architecture that makes it vulnerable to DoS attack is the combination of multiple Virtual Machines (VMs) spread across several mobile edge hosts. This formation increases the possibilities of compromising multiple VMs simultaneously, leading to large-scale attacks such as DDoS [39]. On the pros side, the MEC mobile network infrastructure by virtue of its design is inherently suited for deploying extended defense perimeters capable of mitigating the DDoS attack within multiple fronts. Such defense mechanism allows for fragmented deployments at the network edge, hence capable of defending against smaller attacks before they get any further chances of escalating.

16.5.2 Man-in-the-Middle (MitM)

The MitM attack is characterized by the presence of a third malicious party interposed between two or more communicating parties or entities and secretly relaying or altering the communication between such parties; a common example is the MitM attack between a server and a client. For the MEC scenario, a MitM attack is categorized as an infrastructure attack [38], where the malicious attacker tries to hijack a certain segment of the network and begins to launch attacks, such as eavesdropping and phishing, on connected devices.

The potency of an MitM attack on mobile networks has been proven in various works and literature [40,41]. In these works, MitM attack was launched between 3G and WLAN networks. Such attacks would be even more threatening for the MEC scenario, given that MEC relies heavily on virtualization, hence launching an MitM attack on multiple VMs could very easily affect all other elements on both sides of the attack.

16.5.3 Inconsistent Security Policies

In mobile networks, the need to preserve user-security parameters when they roam from one operator network to another is of utmost importance. In the case of MEC, it is highly possible that all the security services are not updated very frequently and per-user basis. MEC servers can also be limited with resources, thus making it more challenging to facilitate such services. When a user moves from one operator network to another, latency sensitive services are utilized, and such user might be provided with these services through the visited operator MEC, but will his security or the security of the service he is using be ensured? This buttresses the need for security policy sharing among network operators on a much faster scale, to ensure that users traffic on the access networks are effectively attached to the MEC their services are migrating to.

Furthermore, inconsistent or irreconcilable ingress/egress firewall security policies among roaming partners can equally prevent some roaming traffic bound for the Internet from working correctly, if at all they happen to work. This is particularly important in 5G scenarios, where local breakouts will be much more prevalent. These local break-out scenarios will cause roaming IP traffic to be routed over a visited network, where firewall security policies will very likely differ from the same policies deployed in the home network. The reasons motivating the need for local break-out scenarios in 5G are due to the need to reduce latencies and the planned deployment of wireless functionality together with subscriber content at the edge of the network, such as in MEC.

16.5.4 VM Manipulation

This attack is typical for all virtualized and edge computing systems. In MEC, VM manipulation mainly affects the virtualization infrastructures [38].The adversary in VM manipulation is mostly a malicious insider with enough privileges or a VM that has escalated privileges[8]. Such adversary tends to launch multiple attacks to the VMs running inside it.

VM manipulation opens up the affected VMs to numerous other potential attacks such as logic bombs, malware and other such malicious elements that could compromise the security of other data centers when such VM migrates to other physical location on the network [38]. In [42], authors present an attack called DKSM (Direct Kernel Structure Manipulation), which can effectively alter the existing VM introspection solutions into providing false information. VM introspection is a specialized technique for determining specific aspects of a guest VM execution from outside the VM; however, with DKSM attack, the VM introspection solution gets subverted.

16.5.5 Privacy Leakage

Illegitimate access to the MEC environment by an adversary could compromise the privacy of certain information on both the network and the service infrastructures. On the network infrastructure, the MEC paradigm limits the scope of privacy leakage through some specialized functions at the edge data center. The data center mainly stores information from local entities and is also able to extract more sensitive information regarding the user through context awareness; hence, it will be possible to detect a malicious adversary on the network edge [38].

On the service infrastructure, the possibilities of adversaries accessing the information stored at the upper layer of the edge infrastructure could warrant substantial concerns for privacy leakage. However, similar to the case of network infrastructure, the potential damage of such a privacy breach is limited by the amount of information the adversary is able to gain access to. Typically, edge data centers allow for bypass of the central system and the exchange of information directly with each other, hence when information is processed at the lower layer, there are chances that the upper layer would only receive a subset of the processed information, thereby limiting the information made available to potential adversaries [38].

8 Privilege escalation happens when a malicious VM takes control of certain elements of the host.

16.6 Security Architectures for 5G Cloud and MEC

16.6.1 Centralized Security Architectures

The main benefit of centralization is the global visibility of network resource stats and policy synchronization. There are, of course, challenges with centralization, such as latency constraints, scalability and availability challenges; however, large systems that are not very latency sensitive, and centralized systems have more benefits as stated. Centralized control coupled with programmability enables run-time adoption of the network to the changing environment and business requirements. For example, if the traffic behavior changes, it will be beneficial to change the system behavior towards the traffic as well. SDN is one such candidate that enables centralized control of the network with programmability. The logically centralized control enabled by SDN brings dynamism in network security systems by harvesting intelligence from the network equipment through programmable Application Programming Interfaces (APIs). Using NFV, virtual security functions can be placed at any network perimeter, whenever the need arises using the programmable interfaces of SDN such as OpenFlow. In clouds and MEC scenarios, the security framework working as an SDN application can monitor the traffic or resource requests coming towards MEC or cloud infrastructures at a run time to validate the requests. In OpenFlow, each new request is forwarded to the centralized controller, where it can check the authenticity of the user. The controller can check the user credentials through the management plane or other integrity verification system such as HSS in the cellular domain. If the user is authentic, his request is served. If the user is malicious, his subsequent flows are either dropped or forwarded to another system for further analysis and counter actions [43]. Furthermore, the network administrator can prioritize and de-prioritize traffic, redirect or block traffic, change the security policies, and see the user behavior through software from the centralized control point without configuring individual devices. This minimizes the operational expenses (OpEx) for network operators. An integrated environment leveraging SDN-based centralized control framework is presented in Figure 16.6. With the centralized control platform, security services and

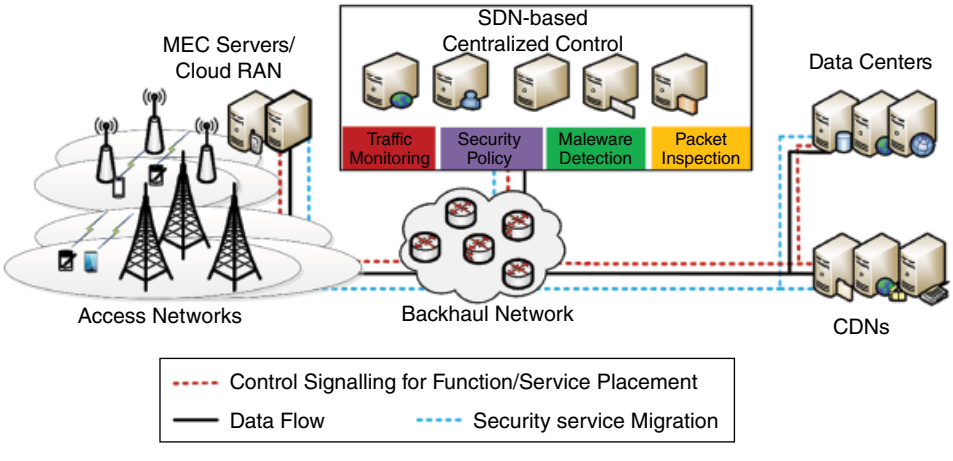

Figure 16.6 Centralized security architecture for mobile clouds and MEC security.

functions can be placed at the network edge through programmable APIs in the edge. This will enhance security of systems, such as C-RAN and MEC in the edge.

16.6.2 SDN-based Cloud Security Systems

The rise of SDN will change the dynamics around securing the data centers by offering opportunities to research for enhanced security [43,44]. Cloud computing systems consist of various resources, which are shared among users with the help of hypervisors. Hence, it provides an opportunity for adversaries to spread malicious traffic to erode the performance, consume more resources or stealthily access resource of other users. With the centralized and global view of network behavior and user activities, SDN provides cost-effective mechanisms to counter such threats. For example, the CloudWatcher [45], working as an SDN application, uses the SDN control platform to provide monitoring services to large and dynamic clouds. CloudWatcher provides mechanisms to control network flows, in order to guarantee their inspection through security systems. Similarly, the SnortFlow [46] uses the OpenFlow SDN model to provide intrusion detection and response systems for clouds. SnortFlow uses Snort-based Intrusion Prevention System (IPS) to detect intrusions and OpenFlow controller to generate actions for the detected flows. For data centers, the Automated Malware Quarantine (AMQ) [44] is an SDN-based solution that detects potential threats and isolates insecure network devices to stop them from adversely affecting the network. Using two modules on top of the SDN controller, such as the Bot Hunter and threat responder, the AMQ detects threats and isolates those threats using the SDN controller.

By coupling NFV with SDN, the above solutions can be used for securing any type of cloud, either in the edge or the data center. As shown in Figure 16.6, modules such as the Bot Hunter in AMQ, or the CloudWatcher, can be deployed in the network edge using the programmability offered by SDN and virtual function placement by NFV.

16.7 5GMEC, Cloud Security Research and Standardizations

The standards that will define 5G are yet to be outlined. The standardization of 5G is a multi-stakeholder process involving a huge numbers of operators, regulators, vendors, policy-makers and representatives of 5G users. However, research and standardization are currently ongoing in several technology areas related to 5G. A more detailed description of standardization activities in 5G is contained in Chapter 2 of this book. In this section, we discuss on standardization activities related to MEC and cloud computing:

- *European Telecommunications Standards Institute (ETSI[9])*: ETSI was created in 1988 to be the main standardization organization in ICT within Europe. It comprises of several technical committees and Industry Specification Groups (ISGs). Its key partners are 3GPP[10] and OneM2M[11]. ETSI holds a crucial position in both research

9 ETSI. http://www.etsi.org/
10 3rd Generation Partnership Project (3GPP). http://www.3gpp.org/about-3gpp
11 One M2M. http://www.onem2m.org/

and standardization of technologies related to cloud computing and MEC. For instance, it was after ETSI launched the ISG for Mobile-Edge Computing in 2014 that MEC acquired its current meaning [47].

Back in 2013, ETSI delivered a report on cloud computing standards, where the Cloud Standards Coordination (CSC) initiative was launched [48], with an ambitious goal of creating 2.5 million new European jobs in the field of cloud computing by the year 2020. The goal of the CSC was to define the key roles of cloud computing, the potential use cases, standardization organizations, and the classification of respective activities for both users and service providers for the entire cloud life-cycle. Also in 2014, the ETSI MEC ISG was formed, with an aim of standardizing the MEC environment and also defining different possible service scenarios and technical requirements for MEC.

- *National Institutes of Standards and Technology (NIST)*: Founded in 1901 as a measurement standards laboratory in the United States and later became a part of the US department of defense, NIST provides measurement standards for a wide variety of technologies. NIST has also become a key player in the standardization efforts of 5G related technologies like cloud computing. For instance, earlier in July 2011, NIST CCSRWG[12] released what it called the *NIST Cloud Computing Standard Roadmap* [49]. This roadmap was designed to accelerate the secure adoption of cloud computing by the federal government through standard developments and guidelines in collaboration with other standard bodies.

  The NIST Definition of Cloud Computing, identified cloud computing as:

  > …a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

  is generally the most widely accepted definition of cloud computing. The NIST Cloud Computing Reference Architecture and Taxonomy Working Group has developed a reference architecture for high-level conceptual model of cloud computing, which are generally used in discussions regarding structures, requirements, and operations of cloud computing [49].
- *Next Generation Mobile Networks (NGMN) 5G Security Group*[13]: NGMN Alliance is a mobile telecommunications association that comprises of mobile operators, vendors, manufacturers and research institutes. This group has gained substantial recognition by both IEEE and 3GPP at different levels. NGMN Alliance announced the launch of a global initiative for 5G earlier in 2014, with the aim of spearheading the development of technologies and standards required for future communication networks [50]. The NGMN 5G security group focuses on expanding communication infrastructures through the use of integrated platforms to advance mobile services in 5G and LTE-advance communication networks. In the last quarter of 2016, the NGMN 5G security group released a comprehensive report on 5G security, MEC, low latency, and consistent user experience. This report provided more bases on how MEC and low latency

12 NIST Cloud Computing Standards Roadmap Working Group
13 NGMN. https://www.ngmn.org/de/about-us/vision-mission.html

combination will support varieties of new use cases and services on 5G. The other role of NGMN includes addressing spectrum requirements, establishing more transparent IPR regime, providing guidance to equipment developers and standardization bodies, establishing clear functionality and performance targets as well as providing an information exchange forum for the industry.

16.8 Conclusions

The large-scale adoption of 5G technologies does not only depend on its ability to deliver the anticipated performance and flexibility promises such as throughput, flexible RAN and latency, but more so on its ability to guarantee the security of all parties involved; users and service providers alike. With the amalgamation of myriads of technologies and use cases, emerging technologies like cloud computing and MEC would be the main targets of adversaries. In this chapter, we have presented the threat landscape for MEC and cloud computing in the context of 5G technologies. Threats such as manipulation of virtual machines, privacy leakage, DDoS, and MitM will become even more prevalent, given that 5G will rely heavily on virtualization and edge technologies. We have further proposed certain control measures and techniques that can mitigate these threats and provide highly guaranteed security on the network. This is particularly important, because in order for 5G to support the vast number of new applications and use cases that have been proposed, MEC and cloud technologies seem indispensable in any case, hence adequate security measures need to be put in place to affirm the confidence of both users and service providers in both technologies.

References

1 Security in cloud computing, *International Journal of Information Security*, 13(2), 95–96, 2014 [Online]. Available at: http://dx.doi.org/10.1007/s10207-014-0232-2
2 Vassilakis, V. *et al*. (2016) Security analysis of mobile edge computing in virtualized small cell networks. In: *Proceedings of the IFIP International Conference on Artificial Intelligence Applications and Innovations*. Springer International Publishing, Thessaloniki, Greece.
3 NSN, Nokia (2013) Solutions and Networks: Looking Ahead to 5G. White paper, *Nokia Solutions and Networks Oy, Finland*.
4 NSN, Nokia (2013) 5G Use Cases and Requirements. White paper, *Nokia Solutions and Networks Oy, Finland*.
5 Wen, T. and Zhu, P. (2013) *5G: A Technology Vision*. Huawei.
6 Intel IT Center (2013) *Planning Guide: Virtualization and Cloud Computing Steps in the Evolution from Virtualization to Private Cloud Infrastructure as a Service*.
7 Bojanova, I., Zhang, J. and Voas, J. (2013) Cloud computing. *IT Professional*, 15(2), 12–14.
8 Mohamed, A. (2009) A history of cloud computing. *Computer Weekly*, 27.
9 Intel IT Center (2013) Planning guide. *Virtualization and Cloud Computing: Steps in the Evolution from Virtualization to Private Cloud Infrastructure as a Service*.

10 Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R. *et al*. (2010) A view of cloud computing. *Communications of the ACM*, 53(4), 50–58.

11 Eze Castle Integration (2013) *The History of Cloud Computing*. Boston, MA.

12 Mell, P. and Grance, T. (2011) *The NIST Definition of Cloud Computing*. NIST, Gaithersburg.

13 Jadeja, Y. and Modi, K. (2012) Cloud computing-concepts, architecture and challenges. *Proceedings of the International Conference on Computing, Electronics and Electrical Technologies (ICCEET)*, IEEE.

14 Savolainen, E. (2012) Cloud service models. *Seminar on Cloud Computing and Web Services*, vol. 10. University Of Helsinki, Department of Computer Science, Helsinki.

15 Tsai, W-T., Sun, X. and Balasooriya, J. (2010) Service-oriented cloud computing architecture. *Proceedings of the Seventh International Conference on Information Technology: New Generations (ITNG)*, IEEE

16 5GPPP Architecture Working Group (2016). *View on 5G Architecture*, June. Available at: https://5g-ppp.eu/wp-content/uploads/2014/02/5G-PPP-5G-Architecture-WP-For-public-consultation. pdf

17 Ericsson White Paper. Cloud RAN: *The Benefits of Virtualization, Centralization and Coordination*. No, 284 23-3271, September 2015.

18 Tullberg, H. *et al*. (2015) METIS SYSTEM CONCEPT: The shape of 5G to come. *IEEE Communications Magazine* (Online). Available at: https://www.metis2020.com/wp-content/uploads/publications/IEEE_CommMag_2015_Tullberg_etal_METIS-System-Concept.pdf

19 Hu, Y.C. *et al*. (2015) *Mobile Edge Computing – A Key Technology Towards 5G*. ETSI White Paper 11.

20 Patel, M. *et al*. (2014) *Mobile-edge Computing Introductory Technical*. White Paper, Mobile-edge Computing (MEC) industry initiative.

21 Mobile Edge Computing: The Edge is the Future. iGillott Research Inc. (2015). White Paper. Version 1.0. 12400 Austin TX 78738.

22 ETSI Group Specification (2016) *Mobile Edge Computing (MEC); Technical Requirements*, ETSI GS MEC 002 V1.1.1 (2016-03), March.

23 5G PPP. 5G Vision: The Next Generation of Communication Networks and Services (2015) [Online]. Available at: https://5g-ppp.eu/wp-content/uploads/2015/02/5G-Vision-Brochure-v1.pdf#page 8

24 ETSI, M. (2014) *Mobile-Edge Computing*. Introductory Technical White Paper.

25 Jarich, P. (2016) *Building 5G: Mobile Edge Computing*. Current Analysis Network Matter. Blog.

26 Tran, T.X., Hajisami, A., Pandey, P. and Pompili, D. (2016) *Collaborative Mobile Edge Computing in 5G Networks: New Paradigms, Scenarios, and Challenges* [Online]. Available at: https://arxiv.org/pdf/1612.03184.pdf

27 Embedded Intel Solutions (2015) *How Mobile Edge Computing is Helping Operators Face the Challenges of Today's Evolving Mobile Networks* [Online]. Available at: http://eecatalog.com/intel/2015/08/17/how-mobile-edge-computing-is-helping-operators-face-the-challenges-of-todays-evolving-mobile-networks/

28 Patel, M. *et al*. (2014) *Mobile-edge Computing Introductory Technical*. White Paper, Mobile-edge Computing (MEC) industry initiative.

29 Hart, J. (2016) What mobile Core Network Architecture Concepts will have an impact on 5G Evolution? *BT TSO – Research & Technology*. 5G NORMA Summer School, London KCL, June.

30 Lindstrom, P. *The Laws of Virtualization Security*. Baselinemag.com Driving Business Success with Technology [Online]. Available at: http://www.baselinemag.com/c/a/Security/The-Laws-of-Virtualization-Security

31 Puttonen, J., Afolaranmi, S.O., Moctezuma, L.G., Lobov, A. and Martinez Lastra, J.L. (2015) *Conference on Security in Cloud-Based Cyber-Physical Systems*, pp. 671–676. DOI:10.1109/3PGCIC.2015.30

32 Chonka, A. and Abawajy, J. (2012) Detecting and mitigating HX-DoS attacks against cloud web services. *Proceedings of the 15th International Conference on Network-Based Information Systems (NBiS)*, September, pp. 429–434.

33 Ficco, M. and Rak, M. (2015) Stealthy denial of service strategy in cloud computing. *IEEE Transactions on Cloud Computing*, 3(1), 80–94.

34 Hubbard, D. and Sutton, M. (2010) *Top Threats to Cloud Computing v1. 0*. Cloud Security Alliance.

35 Cox, P. *Intrusion Detection in a Cloud Computing Environment* [Online]. Available at: http://searchcloudcomputing.techtarget.com/tip/Intrusion-detection-in-a-cloud-computing-environment

36 Khan, A.R. (2012) Access control in cloud computing environment. *ARPN Journal of Engineering and Applied Sciences* 7(5), 613–615.

37 Younis, Y.A., Kashif, K. and Madjid, M. (2014) An access control model for cloud computing. *Journal of Information Security and Applications*, 19(1), 45–60.

38 Roman, R., Javier, L. and Masahiro, M. (2016) *Mobile Edge Computing, Fog – A Survey and Analysis of Security Threats and Challenges*. Future Generation Computer Systems.

39 Liang, B. (2016) *Mobile Edge Computing*. University of Toronto, Canada. [Online]. Available at: http://paswkshop.comm.utoronto.ca/~liang/publications/Chapter_MEC_2016.pdf

40 Stojmenovic, I. *et al*. (2015) An overview of fog computing and its security issues. *Concurrency and Computation: Practice and Experience*, 10, 2991–3005.

41 Zhang, L. *et al*. (2010) A man-in-the-middle attack on 3G-WLAN interworking, vol. 1. *Proceedings of the International Conference on Communications and Mobile Computing (CMC)*, IEEE.

42 Bahram, S. *et al*. (2010*)* DKSM: Subverting virtual machine introspection for fun and profit. *Proceedings of the 29th IEEE Symposium on Reliable Distributed Systems*, IEEE.

43 Ahmad, I., Namal, S., Ylianttila, M. and Gurtov, A. (2015) Security in software defined networks: a survey. *IEEE Communications Surveys & Tutorials*, 17(4), 2317–2346.

44 ONF, *SDN Security Considerations in the Data Center*. Open Networking Foundation, Palo Alto, CA [Online]. Available at: https://www.opennetworking.org/images/stories/downloads/sdn-resources/solution-briefs/sb-security-data-center.pdf

45 Shin, S. and Gu, G. (2012) CloudWatcher: Network security monitoring using OpenFlow in dynamic cloud networks (or: How to provide security monitoring as a service in clouds?), *Proceedings of the 20th IEEE ICNP*, October, pp. 1–6.

46 Xing, T., Huang, D., Xu, L., Chung, C.-J. and Khatkar, P. (2013) SnortFlow: A OpenFlow-based intrusion prevention system in cloud environment, *Proceedings of the 2nd GREE*, March, pp. 89–92.

47 ETSI (2014) *Mobile-Edge Computing Introductory Technical White Paper* [Online]. Available at: http://www.etsi.org/technologies-clusters/technologies/mobile-edge-computing (accessed 9 February 2017).

48 ETSI (2013) *Cloud Standards Coordination: Final Report* v 1.0 [Online]. Available at: http://www.etsi.org/images/files/Events/2013/2013_CSC_Delivery_WS/CSC-Final_report-013-CSC_Final_report_v1_0_PDF_format-.PDF

49 Hogan, M. *et al*. (2011) *NIST Cloud Computing Standards Roadmap*. NIST Special Publication 35.

50 Zhang, N. *et al*. (2015) Cloud assisted HetNets toward 5G wireless networks. *IEEE Communications Magazine*, 53(6), 59–65.