EUROPEAN UNION AGENCY
FOR CYBERSECURITY

FOG AND EDGE COMPUTING IN 5G

Security opportunities and challenges

MARCH 2023

ABBREVIATIONS

3GPP	3rd Generation Partnership Project
AES	Advanced Encryption Standard
AIOTI	Alliance for the Internet of Things Innovation
API	Application Programming Interface
CN	Core Network
EDN	Edge Data Network
EECC	European Edge Computing Consortium
EPC	Evolved Packet Core
ETSI	European Telecommunications Standards Institute
FPGAs	Field Programmable Gate Array
GTP	GPRS Tunnelling Protocol
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IIC	Industrial Internet Consortium
IIoT	Industrial Internet of Things
IMS	IP Multimedia Core Network Subsystem
IoT	Industrial Internet of Things
IP	Internet Protocol
ISO	International Organization for Standardisation
LADN	Local area data network
MEC	Multi-Access Edge Computing
MitM	Man in the middle
MMS	Multimedia Message Service
NEF	network exposure function
NFV	network function virtualisation
NIST	National Institute of Standards and Technology
NSC	network service chaining
OSS	Operations support systems
P2P	Peer-to-Peer
PCF	policy Control Function
PDU	protocol data unit
PGW	Packet Data Network Gateway
QoE	Quality of Experience
QoP	Quality of Protection
QoS	Quality of Service
RAN	Radio Access Network
SIP	Session Initiation Protocol
SLB	Security Level Basic

2.1.2. Attributes

One of the most important aspects of fog computing is the network management it provides [3]. Configuring and maintaining numerous heterogeneous devices and services is a demanding operation that is only becoming more complex as the number of devices and services grows. It is critical that management be accomplished in a more homogeneous manner. To address this management issue, NFV [5], SDN [6], and peer-to-peer (P2P) technologies are used [4].

NFV aims to transform the way network operators construct their digital infrastructure by leveraging the virtualisation technology that provides ease of deployment, management and maintenance with virtualised servers, switches and storage. Virtual devices such as servers and switches can be instantiated on demand with no requirement of possessing a physical device and installing it [7].

Similarly, SDN provides programmable interfaces for network operators that can dynamically change the configuration and architecture of network devices. Instead of making networking equipment more complex, as in the case of active networking [8], SDN provides simple programmable network devices. Furthermore, SDN advocates for the separation of control and data planes in network architecture. Any configuration performed on the control plane does not affect data flows. Consequently, the most notable benefits of SDN are the enhanced configuration, improved performance, and low latency.

Finally, the P2P architecture may interconnect fog endpoints to cooperate, act as decentralised storage and scale dynamically. Small quantities of data can be transmitted among endpoints by leveraging their proximity, thereby eliminating the need for a centralised storage point. As a result, small clusters of endpoints may be used as mini clouds using P2P to deliver functions that would normally require a centralised data server with centralised storage. Table 1 depicts the fog main attributes along with its advantages.

Table 1: Fog computing main attributes and their advantages

Main attributes	Advantages
Minimise latency	Analysis closer to the data source
Conserve network bandwidth	Eliminates the need to transport big amounts of data for analysis, freeing up bandwidth for other critical tasks
Reduce operating costs	Processes as much data as possible locally
Enhance security	Uses policies and procedures deployed across the entire IT environment to control heterogeneous devices
Improve reliability	By reducing the amount of data required to be transmitted, it automatically improves reliability in times of emergency or in difficult environmental conditions
Improved security of sensitive data	By analysing them locally without needing to transfer them to the cloud

2.1.3. Security aspects

One of the greatest security concerns in fog computing is data security and privacy [9]. Due to the shared communication nature of fog computing, it is quite challenging to ensure the privacy of the user's data. Early adaptions of fog computing relied on the cloud for data security; however, this solution was quickly disproven due to the centralised nature of cloud computing.

Other common security issues in fog computing include forensics, authentication issues and privacy concerns [10] [11]. It is quite a challenge for researchers to attempt to extract information with forensics due to the heterogeneous nature of fog computing. Additionally, the fact that fog computing acts as a medium between cloud and edge computing increases the level of difficulty in forensic analysis. This also creates complications in the authentication of users. A large number of heterogeneous devices require a standardised authentication protocol; however, different services and applications use their own protocols, rendering this solution incredibly complex.

Furthermore, the implementation of virtual machines (VMs) that can be found in cloud and fog computing settings (cloudlets) [12] can be considered a critical issue in terms of security. These VMs, which are often publicly available, contain critical applications and sensitive data. Therefore, it is often required to allow customers and users to have complete control over the management of their applications or data, while also ensuring the limitation of access to malicious users [13]. Trust is another significant factor. End users need to trust the platforms that are secure and well equipped to handle malicious activities [14]. Moreover, providers are often required to provide constant security checks and prompt updates to secure versions [15]; this, however, creates the need to consider a holistic approach that includes physical measures to properly secure the infrastructure. Therefore, besides a secure by design physical architecture that is required, one must deploy perimeter firewalls, demilitarised zones, intrusion detection and prevention systems, network segmentation and monitoring tools [16]. Physical segmentation and hardware-based protection, on the other hand, are ineffective against cyberattacks across VMs on the same server. Fog computing servers often run the same operating systems and web applications as physical and virtualised servers. Consequently, malicious users can exploit vulnerabilities on these machines remotely. In addition, the co-location of numerous VMs expands the attack surface and raises the potential for VM-to-VM penetration. In short, it is crucial to provide not only secure VMs but also secure environments in which the VMs can reside. To conclude, Table 2 details the major security threats of the adoption of fog computing.

Table 2: Fog computing main security threats

Security Threat	Description
Authentication and trust issues	Fog service providers can vary. This flexibility complicates the structure, wherein rogue fog nodes can thrive, leading end users to connect to it.
Privacy	The amount of fog nodes available for an end user to connect is a huge privacy concern since sensitive information is propagated to the fog nodes.
IP address spoofing	Any malicious actor can mask their IP to gain access to personal information that is stored in a particular fog node.

2.2. EDGE COMPUTING

Edge computing is the most recent addition to the computing paradigms covered in this report. It enables edge devices and servers to expand cloud capabilities at the edge in order to resolve

computational processes and store data in close proximity to the user. Edge computing is expected to be used to meet the communication needs of next-generation applications such as augmented reality [17]. Another gap that edge computing may bridge is that of vehicular ad hoc networks (VANETs) [18], wherein low latency is necessary, allowing cars to communicate with far less latency than interacting with a centralised cloud server requires.

2.2.1. Attributes

One of the main attributes of edge computing is the low latency and close proximity of devices [19], which enables edge computing to reduce overall round-trip time in comparison to traditional cloud communications. This allows crucial applications such as VANETs to exist [18]. The strategic location of edge servers reduces propagation delays and enables them to collect and process data based on the end user's usage instead of traditionally collecting data in another centralised location. This demonstrates another important attribute of edge computing that allows for the personalisation of services by using local data. Similarly, an edge server can use the localised network data to acquire network context information, use it to adapt the network accordingly, and handle the massive amounts of data that are transmitted.

Another attribute of edge computing is efficiency and sustainability. Thanks to the localised nature of edge computing, bandwidth requirements are low, thereby keeping the latency numbers and energy requirements at minimal levels too. Edge devices are mostly IoT devices, meaning that their energy capacities are constrained; therefore, energy efficiency is of high importance [20]. What is more, the collaboration of devices that edge computing provides is another attribute that enhances energy efficiency by distributing the task load to other nodes. Table 3 details the main attributes of edge computing, along with its advantages.

Table 3: Edge computing main attributes

Main attributes	Advantages
Low latency	Enables instantaneous communication
Close proximity	Reduces overall round-trip time
Location awareness	Collects and process data based on the end user's usage
On premises	Reduces propagation delays
Efficiency/sustainability	Bandwidth requirements are kept low

2.2.2. Security aspects

Creating an edge computing ecosystem poses a security challenge. There is a number of reasons for this. Firstly, edge computing is based on enabling various heterogeneous technologies. Despite the ability to guarantee security for each technology, it is a challenge to ensure the security of the whole system. Similarly, the core of edge computing – namely wireless networks, distributed and P2P systems, virtualised machines and network protocols – presents difficulties in securing these building blocks and orchestrating all the diverse security mechanisms. Lastly, the most significant security issue is the impact of a successful attack to a critical infrastructure such as edge. As mentioned before, the localised features of edge computing are important in deploying new technologies such as VANETs; however, a successful attack to VANETs might pose a threat to human life and society. The main security threats that exist in edge computing are listed in Table 4.

Table 4: Edge computing security threats

Security Threat	Description
Flooding attacks	(Distributed) denial-of-service attacks ((D)DoS) against edge nodes/devices
Zero-day attacks	With the introduction of heterogeneous devices and IoT applications, new vulnerabilities are common
Communication channel attacks	Information theft through packet capturing and wave signals
Power consumption attacks	Battery draining attacks against edge computing nodes/devices
Smartphone-based	Sensor-based and filesystem-based information theft
Server-side injection attacks	SQL injections, XSS, CSRF & SSRF, XML Sign, etc.
Authentication and authorisation attacks	MitM, rogue nodes

2.3. FOG AND EDGE COMPUTING IN 5G

5G networks are the next generation of wireless cellular networks. 5G is characterised by low latency and high throughput, high amounts of data that is transmitted and generated, and the requirement to support a heterogeneous environment to allow for the interoperability between various devices, network types and quality of service (QoS) ([4]) requirements. All these characteristics are unprecedented, never seen in previous generations' networks, and therefore require a new approach to fulfil the requirements, but also, a vast number of new technologies, architectures and innovations in mobile networks.

Fog and edge computing, which were briefly introduced in the previous section, can be used to extend the capabilities of 5G. For example, fog computing could be used as a network management and monitoring tool, thanks to its virtualised servers and monitoring sensors. Lastly, edge computing could be exploited to serve as a decentralised computational orchestrator to distribute tasks to multiple devices in order to reduce the overall workload and provide high QoS and QoE ([5]).

([4]) https://en.wikipedia.org/wiki/Quality_of_service
([5]) https://en.wikipedia.org/wiki/Quality_of_experience

various MEC apps and therefore must use fine-grained access control mechanisms to guarantee such isolations, i.e. let a given MEC app access only the services and information they have been authorised to access.

At the MEC system level, the MEC orchestrator is not only critical because it has privileged access to the MEC platform manager and VIM, but also because it is particularly exposed to end-user devices via the user app life cycle management proxy. Indeed, this proxy allows device applications to create and terminate (and possibly more) user applications in the MEC system, via the MEC orchestrator. When registration, discovery or deregistration is used without authorisation, a malicious EEC receives a list of the services and the topology structure of the edge data network from the edge enabler server discovery response message. The information received can reveal the edge data network's topology (e.g. URI, IP address, number of edge application servers, application server functionalities, API type, protocols). A malicious EEC may use this information to launch attacks on the edge data network or use this information for competitive reasons.

If GPSI is not authenticated, then an EEC that spoofs a victim UE's GPSI can learn some information about the location of the victim UE's location because the server list returned to the EEC is constructed considering the UE location learned from the 3GPP network.

Figure 7: Overview of standardisation efforts for fog and edge computing

3.4. JOINT 5G CORE THREAT LANDSCAPE FOR FOG AND EDGE APPLICATIONS

The common ground for 5G infrastructure for fog and edge applications is the 5G core domain, which provides the backbone for the connectivity of the different modules and which is becoming more and more softwarised as standards evolve. This transition has enabled agility in the development of different capabilities but has also created the space for different vulnerabilities and security gaps. A general outline of these 5G core security threats is outlined below.

- **Information leak.** Information on 5G core networks can be largely divided into information on EPC equipment to process the data and information on IMS equipment to provide various services. Because EPC equipment communicates using GTP protocol (GPRS tunnelling protocol) and IMS equipment communicates using session initiation protocol (SIP) protocol, the attacker can select a protocol suitable for the desired information. The GTP protocol is divided into GTP-C (control), used for core network equipment, and GTP-U (user), which delivers data traffic in the user terminal through a tunnel between the base station and PGW. In order to find out the IP information of the EPC equipment, the attacker can use a packet injection method that loads an echo request, 'that is to say (i.e.) a GTP-C message for health check between core network equipment, on the data payload to send. PGW checks this and

5. SECURITY ASPECTS

In this chapter, we will discuss the open security issues that exist in fog and edge computing in 5G networks. Despite the immense benefits that both fog and edge computing offer, they have their own disadvantages concerning privacy and security issues.

5.1. FOG COMPUTING IN 5G

Time-sensitive data analysis and local data storage are made easier by fog computing by reducing the volume and travelled distance of data that was previously sent to the cloud. Consequently, this addresses and minimises the impact that heterogeneous edge devices and IoT applications have in terms of security and privacy. An overview of the security aspects of fog computing in 5G along with the main issues that need addressing is provided in Table 5.

Table 5: Security aspects and main issues of fog computing

Security aspect	Fog computing issue
Threat landscape	A broken node asks a fog node for processing or storage, delaying a request from a reliable device [37]. Additionally, spoofing the addresses of numerous devices and sending phony requests leads to DoS attacks [38], while existing protection mechanisms are not tailored for fog architectures. Thus, a certification schema to verify authenticity [39] should be considered, even though this does not address a compromised node.
Virtualisation security	Dependencies in system elements such as the orchestrator, SDN controller, network controller and NFV security orchestrator expose numerous new vulnerabilities, widening the threat landscape [40], [41].
SDN security	Entry point created from a weakly protected fog node; privacy leakage containing location information [43].
Data security and privacy	Insufficient trust between devices and fog nodes due to technology being prone to errors and harmful attacks [44].
Trust	Resource limitation of 5G-connected devices renders conventional authentication methods such as PKI and authentication methods utilising certificates invalid.
Authentication	Lack of support, concerns about intellectual property, lack of proper documentation and graphical user interfaces, along with new security concerns that needs addressing [44].
Open-source security	Potential flaws regarding the flexibility of the built-in orchestration that could potentially allow an attacker to compromise a VNF.
Orchestration security	Entry point created from a weakly protected fog node; privacy leakage containing location information [43].

5.1.1. Threat landscape

Fog-computing environments are vulnerable to numerous harmful assaults, and if adequate security measures aren't put in place, they could seriously impair the 5G network's capabilities. A DoS attack is an example of a malicious assault that can be launched [45]. A DoS attack is easy to launch since the vast majority of devices connecting to networks are not mutually

5.1.8. Orchestration security

The complexity of allocating and optimising resources in 5G has led to a rise in the management and orchestration layer's use of artificial intelligence and machine-learning methods [63]. An orchestrator could provision VNFs in an SDN/NFV environment based on the health and intelligence of the network. For instance, in the event of a network overload or security attack, the orchestrator is alerted to the situation and, cooperating with the SDN controller, manages the firewalls and routers to lessen the impact of the attacks [64]. The orchestrator can simultaneously instantiate more VNFs as needed and scale them back when the attack weakens. Due to the flexibility of the built-in orchestration, there are potential flaws that could allow an attacker to compromise a VNF by using legitimate access to the orchestrator to change its configuration.

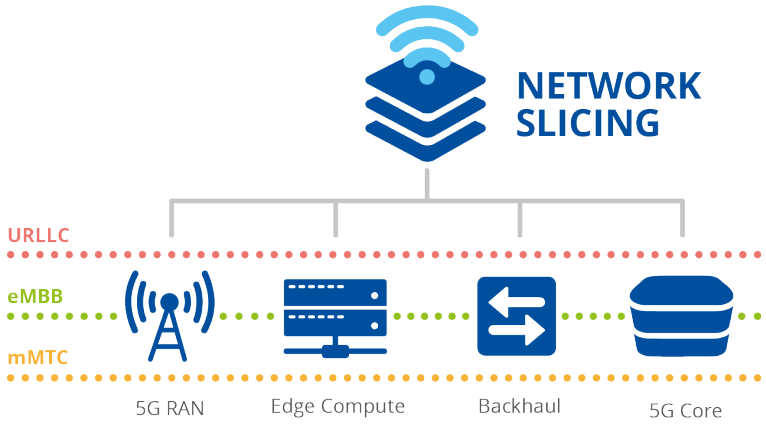
5.2. Edge computing in 5G

If the edge is compromised, there will be significant negative effects due to the edge's growing position in the 5G architecture and use cases [18], [65]. The edge becomes a desirable target for cyberattacks when this is coupled with the expanded threat surface as the edge moves closer to the end user. Security is enhanced by the fact that the edge hosts security controls for other 5G use cases, such as authentication, authorisation and real-time threat detection. For a low-latency application, security measures on the edge should also consider sophisticated and multi-step user handling scenarios, such as subscriber authentication with a visiting network. Authenticating will be impossible in this situation due to delay limits; hence an alternative approach should be looked into [66]. To ensure proper confidentiality and availability for the security functions, as along with any sensitive security contexts that may be held on the edge or communicated between the edge and the core, strong-layered security controls must be established [67]. Bi-lateral movements to the 5G control layer would be less risky if administration and network operations were properly separated from third-party applications. The attack surface from the user side could be reduced with the aid of computationally feasible trust systems [68]. Table 6 depicts the security aspects of edge computing along with its main issues.

Table 6: Security aspects and main issues of edge computing

Security aspect	Edge computing issue
Authentication	Lack of robust authentication measures.
Network slicing security	Security policies must be refined to enable trusted virtualised architectures and maintain effective slice isolation [69].
MEC security	The utilisation of mobile devices and deployment of edge cloud servers widens the threat landscape, while traditional mobile cloud computing security solutions cannot adapt to MEC and traditional data security methods cannot be applied to edge devices [70].
Supply chain security	Commodity modular hardware and software introduce numerous security vulnerabilities in the edge nodes such as backdoors, dormant harmful programs and falsified hardware certificates [71].
Networking protocol security	Distribution of credentials.
Intrusion detection	Traditional IDSs are unable to cope with the edge architecture, thus signature-based and behaviour-based detection should be implemented.
Privacy	To ensure privacy of end users' secure trust schemes and data encryption utilising asymmetric AES scheme.

Figure 10: 5G edge network slicing overview



5G network slicing can provide an efficient solution for resource isolation and data protection across different entities of the network – and edge in particular. The authors in [108] propose a 5G network slicing framework to address the security breaches and vulnerabilities of an edge-computing infrastructure. Network slices are end-to-end logical networks, so it is natural to aim for end-to-end security. The concept of end-to-end security is closely connected to the concepts of isolation and orchestration. Moreover, it is dependent on the business model and, consequently, on the trust model. In order to attain an adequate security level across the entire edge infrastructure, isolation of resources and targets needs to be ensured by a secure edge service orchestrator, in order not to degrade the service's performance, and last but not least, all involved parties at the edge infrastructure need to adopt a common trust model.

Table 7: 5G fog and edge application scenarios

5G fog application scenarios	5G edge application scenarios
Quality of privacy (QoP)	**Lightweight encryption schemes**
Blockchain for data encryption and device privacy	**Differential privacy**
SDN with VANETs	**MEC**
NSC	**Orchestration**
Network slicing	**Network slicing**

[106] C. Vallati, A. Virdis, E. Mingozzi, and G. Stea, 'Mobile-Edge Computing Come Home Connecting things in future smart homes using LTE device-to-device communications', *IEEE Consumer Electronics Magazine*, vol. 5, no. 4, pp. 77–83, Oct. 2016, doi: 10.1109/MCE.2016.2590100.

[107] R. Morabito, R. Petrolo, V. Loscri, and N. Mitton, 'Enabling a lightweight Edge Gateway-as-a-Service for the Internet of Things', in *2016 7th International Conference on the Network of the Future (NOF)*, Nov. 2016, pp. 1–5. doi: 10.1109/NOF.2016.7810110.

[108] R. F. Olimid and G. Nencioni, '5G Network Slicing: A Security Overview', *IEEE Access*, vol. 8, pp. 99999–100009, 2020, doi: 10.1109/ACCESS.2020.2997702.

[109] Jang, W.; Kim, S.K.; Oh, J.H.; Im, C.T. Session-based detection of signaling DoS on LTE mobile networks. *J. Adv. Comput. Netw.* **2014**, *2*, 159–162

[110] Park, S.; Kim, S.; Son, K.; Kim, H.; Park, J.; Yim, K. Real threats using GTP protocol and countermeasures on a 4G mobile grid computing environment. *Int. J. Web Grid Serv.* **2017**, *13*, 3–24.

[111] Park, S.; Kim, S.; Son, K.; Kim, H.; Park, J.; Yim, K. Real threats using GTP protocol and countermeasures on a 4G mobile grid computing environment. *Int. J. Web Grid Serv.* **2017**, *13*, 3–24

[112] Chlosta, M.; Rupprecht, D.; Holz, T.; Pöpper, C. LTE security disabled: Misconfiguration in commercial networks. In Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '19), Association for Computing Machinery, New York, NY, USA, 15–17 May 2019; pp. 261–266

[113] Park, S.; Kim, S.; Son, K.; Kim, H. Security threats and countermeasure frame using a session control mechanism on volte. In Proceedings of the 2015 10th International Conference on Broadband and Wireless Computing, Communication and Applications (BWCCA), Krakow, Poland, 4–6 November 2015; pp. 532–537