EUROPEAN UNION AGENCY
FOR CYBERSECURITY

FOG AND EDGE COMPUTING IN 5G

Security opportunities and challenges

MARCH 2023

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

CONTACT

For contacting the authors please use send an email to resilience@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu.

Editors

Evgenia Nikolouzou (ENISA)

CONTRIBUTORS

Evangelos K. Markakis (Hellenic Mediterranean University),
Michail Alexandros Kourtis (National Centre for Scientific Research, Demokritos)

ACKNOWLEDGEMENTS

We are grateful for the review and valuable input received from the experts from national authorities in the NIS Cooperation group, and particularly those experts contributing to the NIS CG work stream on 5G cybersecurity.

LEGAL NOTICE

COPYRIGHT NOTICE

PDF ISBN 978-92-9204-610-1 doi:10.2824/246475 TP-04-223-38-EN-N

CONTENTS

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

SLC	Security Level Critical
SLE	Security Level Enhanced
UPF	User plane function
VIM	Virtualized Infrastructure Manager

EXECUTIVE SUMMARY

The ambition of this report is to outline the various security aspects of fog and edge computing in the 5G domain. This includes the technical risks, and therefore trust and resilience, in the telco ecosystem. Fog and edge technologies are considered in this report as a multi-dimensional space encompassing not only technological and functional domains but also the related technology lifecycle processes, stakeholders, and applications. This report focuses on the fundamentals of fog and edge, an overview of their security aspects, the open challenges that these sectors face, the related standardisation efforts, the existing opportunities in this field, and different application scenarios. Fog and edge computing have become key enablers in the 5G ecosystem, creating new opportunities and novel applications, but also multi-modal security challenges, that the telco, cloud and industrial communities address them from different perspectives.

The need for this report stems from the work on the 5G EU toolbox. Specifically, the European Commission and the Member States, with the support of ENISA, developed a single EU coordinated risk assessment on cybersecurity in 5G networks, following the European Commission's recommendation on the cybersecurity of 5G networks. Subsequently, the NIS Cooperation Group published the EU toolbox of risk mitigating measures. The objectives of this toolbox are to identify a possible common set of measures that are capable of mitigating the main cybersecurity risks of 5G networks that were identified in the EU report on coordinated risk assessment and to provide guidance for the selection of measures that should be prioritised in mitigation plans at national and at EU level. The toolbox identifies two groups of measures Member States can take: strategic and technical measures. In addition, it identifies a number of supporting actions that can assist, enable or support the implementation of strategic and technical measures.

With this report, ENISA tries to provide support to the experts of the NIS Cooperation Group Work Stream on 5G Cybersecurity on current issues and challenges in the areas of fog and edge computing in 5G. This report aims to cover them from a technological and organisational point of view. Considerations of the effectiveness of specific standards and of the strategic aspects related to fog and edge security, although important, are outside the scope of this report and are covered merely from the technical analysis perspective.

Accordingly, this report:

- provides an overview of fog and edge technologies in terms of 5G, in relation to their architecture, attributes, and security aspects;
- covers the different architectural approaches that both paradigms have introduced in the telco domain, along with their relevant applications;
- addresses the various security challenges that have emerged from the fog and edge convergence with 5G, for example trustworthiness of edge nodes, multi-modality of fog devices, large number of access devices and technologies;
- outlines the standardisation efforts of fog and edge computing in regard to security.
- analyses the existing literature against an ideal situation of cybersecurity robustness and resilience, and address technical and organisational security aspects;
- analyses the current opportunities in terms of scalability, network management, reliability, sustainability, and federation for fog computing;
- detailing the current opportunities in terms of quality of experience (QoE), protocol standardisation, heterogeneity handling, and multi-access edge computing for edge computing;

- provides analysis on various application scenarios for fog and edge computing in 5G.

The report collects and analyses more than 100 documents and outlines the main security aspects in the fog and edge domains. The main observations that can be derived from the analysis are the following.

- Fog and edge computing specifications and guidelines cover to a greater extent the 'run' phase of a technology lifecycle, whereas other phases would need tailoring.
- Existing knowledge bases on cybersecurity threats and IT-security guidelines can be used for fog and edge native architectures and architectures relying on application programming interfaces (APIs). Although these families of software are well known to the IT industry, their use is quite recent and constitutes drivers of the 'cloudification' of the telecom sector.
- Fog and edge applications and services that have emerged from different sectors and have been integrated in the 5G domain are summarised. Both paradigms have enabled a horizontal cross-sector development of various innovative application scenarios.
- Presents the different novelties that have been developed under the scope of fog and edge computing and have had a disruptive impact in the networking technologies field overall. The report covers how novelties such as network service orchestration, federation, elasticity and scalability approach security challenges in the 5G domain.
- Analyses various mitigation measures that fog and edge computing have developed in response to various security challenges present and introduced in 5G and also the different sectors and layers that are affected.
- The available standards, specifications, and guidelines are general. They can be applied consistently to the fog and edge technical and functional domains and related lifecycle processes only after being tailored accordingly.
- Fog-specific standards, specifications, and guidelines are available to a greater extent to the stakeholders from the Industrie 4.0 and 'Internet of Things' (IoT) sectors. Whereas for edge computing, the European Telecommunications Standards Institute (ETSI) and the 3rd Generation Partnership Project (3GPP) have defined several standard activities of the telecommunication sector.

Finally, this report stresses that, while the technical and organisational standards and specifications analysed can contribute to the security of fog and edge computing for 5G, they should not be treated as an exhaustive list of measures guaranteeing security. There are risks that are not covered by standards, for example, residual risks whose cost is neither borne by nor attributable to a specific stakeholder, such as societal risks resulting from network malfunctions. This vision should be future-proof and not dependent on the variability of assets and configurations in the network.

1. INTRODUCTION

1.1. BACKGROUND AND POLICY CONTEXT

This report is an overview of the latest developments in the domains of fog and edge computing in relation to 5G networks. It encompasses the novelties introduced by the two paradigms in the telco ecosystem and the relevant security aspects involved. It summarises the information found in standardisation documents related to fog and edge. Moreover, the current opportunities of the technologies are presented, providing a scope of their impact and how it can be extended to the 5G field focusing on security.

Furthermore, different aspects of cloud computing and how these converge with the notions of fog and edge computing are presented in detail, namely how the evolution of cloud primitives has helped form different enablers for 5G at the edge and far edge of the network. The different elements involved cover a wide range of industries and domains ranging from the software-defined networking (SDN) and network function virtualisation (NFV) ecosystem to the supply chain industry. The wide coverage of different domains is also assessed in terms of security and trust for the services involved.

The report provides an analysis of the different elements of fog and edge computing paradigms, indicating how these layers have evolved to be incorporated into 5G. For each layer, a dedicated security aspect analysis is provided to examine security and risk as a whole for fog and edge. Regarding the security layer and the specifications that currently exist, the report consolidates information from various sources, including main 5G and Industrie 4.0 standardisation documents and telecommunication best practices (from 3GPP, ETSI, the Industrial Internet Consortium (IIC), the National Institute of Standards and Technology (NIST), and the International Electrotechnical Commission (IEC)). A consolidation of the security threats and vulnerabilities that these bodies identify for fog and edge devices and endpoints has also been performed. Taking into account the close connection between fog and industrial 'Internet of Things' (IIoT) technologies, the relevant standards have been investigated in terms of security requirements and solutions recommended. Regarding edge computing, the relevant 3GPP and ETSI standards have been analysed to provide a summary of the security architectures and requirements that are currently provided by the corresponding bodies.

The assessments provided in this report are based on the specifications of different standards for fog and edge computing that different industries have applied over the years, thus a potential 'mismatch' may be identified when looking at actual real-world system implementations. Moreover, security vulnerabilities and gaps have been extrapolated from technical system specifications provided by the standard specifications. The report aims to bridge the gap between functional specifications and implemented functions, but also concisely define the connections and gaps between fog, edge and 5G, as of today. As progress is continuously being made at the edge and far edge of the network, it is important to track and check compliance with each new feature that is being introduced in the telecommunications ecosystem.

For the time being, the material presented in this report aims to support various stakeholders in understanding the relevant vulnerabilities and cyberthreats resulting in the exposure of fog and edge in relation to 5G assets by exploiting the vulnerabilities.

1.2. POLICY CONTEXT

Working towards a technological revolution in the area of 5G, the European Commission and the Member States, with the support of ENISA, developed a single EU coordinated risk assessment on cybersecurity in 5G networks ([1]), following on the European Commission's recommendation on the cybersecurity of 5G networks ([2]) (published on 26 March 2019). This coordinated risk assessment is based on individual national risk assessments and identifies the main threats and threat actors, the most sensitive assets, the main vulnerabilities and the main risks. To complement this report, and in order to provide further input for the toolbox, ENISA carried out a dedicated threat landscape mapping, consisting of a detailed analysis of certain technical aspects, in particular the identification of network assets and of threats affecting these.

Subsequently, on 29 January 2020, the NIS Cooperation Group published the EU toolbox of risk-mitigating measures ([3]). The objectives of this toolbox are to identify a possible common set of measures that are capable of mitigating the main cybersecurity risks of 5G networks as have been identified in the EU coordinated risk assessment report and to provide guidance for the selection of measures, which should be prioritised in mitigation plans at the national and EU level. The toolbox identifies two groups of measures Member States can take: strategic and technical measures. In addition, it identifies a number of supporting actions that can assist, enable or support the implementation of strategic and technical measures.

The present report contributes to the identification of the present risks and security vulnerabilities that fog and edge ecosystems are currently susceptible to and provides a clear overview of the requirements and mitigation controls that need to be taken into account in order to minimise risk in the fog and edge systems and relevant sub-systems involved. While fog and edge computing, as paradigms, are included in various standard bodies, each body provides support for different business models, which may be at different maturity levels.

The most relevant standards activities to support edge cloud deployment in conjunction with mobile network operators (MNOs) are taking place at 3GPP and ETSI industry specification group on MEC. Other groups such as GSMA and 5GAA focus on setting requirements and implementation agreements leveraging those standards where applicable. Different standards activities cover different aspects and applicability statements and complement each other to a large extent. The standardisation section suggests different security architecture levels for IoT deployments and security interfaces for edge deployments that support different market-driven use cases and related requirements.

1.3. DOCUMENT PURPOSE AND OBJECTIVES

In recent years, fog and edge technologies have rapidly emerged in the telecommunications field with their fast integration in the 5G domain. Several national, European and international developments have led to a clearer picture of 5G infrastructure and its leverage on fog and edge developments at various levels. The fog and edge security specifications have been detailed from various standardisation bodies across different sectors and have found application to different verticals. Moreover, at the EU level, different heterogeneous vertical fog- and edge-driven pilots have been developed and different extension schemes for 5G are envisaged, in preparation for potential requests to ENISA issued by the European Commission Cybersecurity Certification Group in the future. This situation gives far better visibility on the details of fog and edge infrastructures and is a better starting point for updating the ENISA fog and edge computing in 5G. Having regard to these developments, the objectives, working methods and scope of this report are as follows.

([1]) https://ec.europa.eu/digital-single-market/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security
([2]) https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=58154
([3]) https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures

- The material collected and processed within this report consists of open-source resources. It covers mainly the state-of-the art of the fog and edge computing specification work, white papers and good practices. No concrete implementations of cloud, fog and edge service providers, vendors, etc. have been considered or analysed for the purposes of this report.
- The threat and vulnerability analysis performed is based on the extrapolation of existing threats and vulnerabilities found in collected material. In this respect, vulnerabilities referred to in various processed documents have been 'reverse-engineered' based on their relevance to various components/assets; subsequently, they have been grouped under the various zoom-ins and reflect the assessed technical and operational weaknesses, as mentioned in the various standards / good practices. It has to be noted that this is a pure desk-top exercise based on assumed vulnerabilities and threats and that it is not funded by real incidents. Also, actors that are presented as threats in this report are rather hypothetical, as no known attacks on such infrastructure exist as of yet.
- The comprehensive architectures of ETSI MEC and 3GPP developed in the corresponding reports have been included to present novelties of the ETSI and 3GPP specifications.
- A detailed technical and operational vulnerability analysis has been performed for the components of the fog and edge architectures. This analysis takes into account the threats exploiting those vulnerabilities and the controls reducing exposure to these threats, as defined by international organisations (3GPP, ETSI, GSMA, the International Organization for Standardisation (ISO), the International Telecommunication Union, NIST).
- Detailed information and security requirements for various functions and interfaces are included in this report, based on the IIC, ETSI and 3GPP specifications for fog and edge endpoints and interfaces.
- The development of this report followed a 'best-effort' approach. The collected information is not exhaustive, but is representative of the matters covered.
- The content of this report was restricted to components/matters found in relevant open-source material covering the entire specification, security requirements and research results related to fog and edge computing paradigms. The presented material has been put together by ENISA.

1.4. DOCUMENT SCOPE AND INTENDED AUDIENCE

The main purpose of this report is to provide knowledge and information on fog and edge cybersecurity issues in relation to 5G to the relevant community. This information may be useful to a variety of target groups, namely the following.

- **Non-technical stakeholders such as policymakers, regulators and law enforcement.** This target group may find this report useful to understand the current state of specification work, the overall architecture of fog and edge, the emerging vulnerabilities and threats, and respective mitigation practices and measures. For example, the threat landscape identified in this report may support policy actions in the areas of 5G networks, SDN, NFV and cybersecurity, where fog and edge have actively emerged in recent years.
- **Experts working in the telecommunication and cloud computing sectors, such as operators, vendors and service providers.** This target group may find this report useful to carry out detailed threat analyses and risk assessments in accordance with their particular needs and mandate (e.g. protect a specific number of components based on asset impact analysis, respond to specific vulnerabilities with customised mitigation measures).
- **Businesses, consultants and product developers.** This target group can draw valuable conclusions from the developed analysis and material for their products and

services. This can take the form of demonstrating how vulnerabilities have been eliminated by using developed defences, using the material for customer projects, and using the material as a benchmark for defining cybersecurity protection policies for such infrastructures (e.g. for the development of verticals). Moreover, the developed material can be used in developing security audits for fog and edge infrastructures.

- **Experts in research and innovation.** The presented material provides a detailed view of the security issues of fog and edge in terms of 5G. This target group may use this material as the basis for gap analysis, as material to evaluate the impact of research and as a source for innovation actions with regard to further development and implementation. Finally, this target group may use this material as a useful resource for numerous academic activities, such as teaching, research, support of scholars, etc.

Beyond these main target groups, some individual parts of the information provided in this report may be useful to a further number of target groups. For example, the assessed vulnerabilities –consolidated from various sources – may be a valuable resource for standardisation work in order to check the completeness of already performed assessments. Moreover, the provided material may be used for risk assessment within certification activities, providing information about threat exposure and threat actor motives and objectives. Finally, both the overview of fog and edge technologies and their respective standardisation and opportunities sections can be used as is or further developed by any stakeholders in performing their own vulnerability, threat and risk assessments.

1.5. DOCUMENT STRUCTURE

This report presents the results of the vulnerability and threat assessment work that was performed in the following manner.

- Chapter 2 presents an overview of the components of the fog and edge paradigms, with details on and an analysis of their corresponding architectures, attributes and security aspects. The presented features are detailed in relation to 5G, and the interaction impacts each domain and its related stakeholders.
- Chapter 3 presents the standardisation activities related to fog and edge computing for 5G in terms of security. A set of specifications from different standardisation bodies is presented in brief, as well as how these have impacted the security specification of the different fog and edge domains.
- Chapter 4 presents the current opportunities for fog and edge computing in the field of 5G, namely in terms of scalability, reliability, sustainability, heterogeneity and federation from different enablers across heterogeneous technology domains.
- Chapter 5 presents the security aspects from different technology domains and how these are leveraged and impact the fog and edge paradigms for 5G. This chapter covers a collection of different enablers in regard to security from the entire spectrum of cloud and telco technologies.
- Chapter 6 presents an overview of different security application scenarios for fog and edge computing in 5G and how these impact privacy and security aspects as a whole.
- Chapter 7 provides recommendations and conclusions drawn from the technology and security analysis.

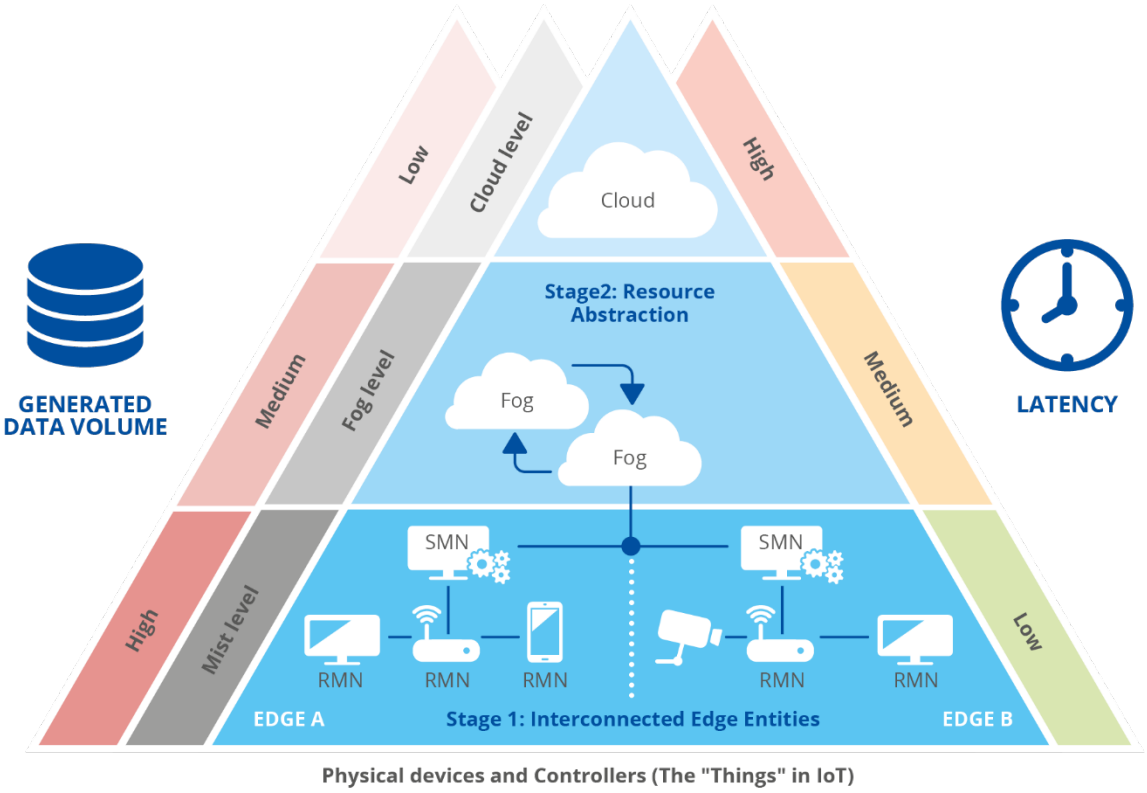
2. OVERVIEW OF FOG AND EDGE COMPUTING IN 5G

This chapter aims to introduce fog and edge computing and explain how they interweave with fifth generation (5G) networks. However, a small introduction to cloud computing is required, since it is interconnected with fog and edge computing. Cloud computing is a computing approach that is distinguished by dynamically scalable and virtualised resources delivered as services over the internet [1]. It has drastically transformed the digital landscape, with numerous applications moving to the cloud and major technology companies offering cloud services to the public. One of its most notable characteristics is the availability of a service without the requirement of considerable resources. This enables customers to access data storage remotely, take advantage of available resources and experiment in various digital settings, therefore lowering expenses. Considering this, the benefits of cloud computing include cost savings, ease of scaling and high availability.

2.1. FOG COMPUTING

Fog computing is an architecture that is a layer beneath cloud computing [2], as shown in Figure 1, where the main goal is to reduce the workload of edge and cloud devices by offering network and hardware resources to both parties [3]. It essentially extends cloud computing and services to the edge and provides computing, storage data and application services to end users while being hosted at the network's edge. It also reduces service latency and improves the overall end-user experience. It is a paradigm in which a large number of diverse, pervasive and decentralised devices connect with one another and with the network in order to fulfil storage and processing functions without the involvement of third parties [4]. Since it extends cloud computing, it enables end users to access data storage remotely and provides availability of services without needing extensive resources, hence lowering expenses. In more detail, fog computing consists of a control plane and a data plane. The control plane enables computing services to inhabit the edge of the networking environment as opposed to servers in a data centre, while fog computing (or 'fogging') enables short-term analytics at the edge. However, fog computing has its own disadvantages. Being tied to a physical location (often close to the edge) undermines the 'anytime/anywhere' potential offered by cloud computing. Moreover, fog computing introduces potential security issues such as internet protocol (IP) address spoofing or 'man in the middle' (MitM) attacks.

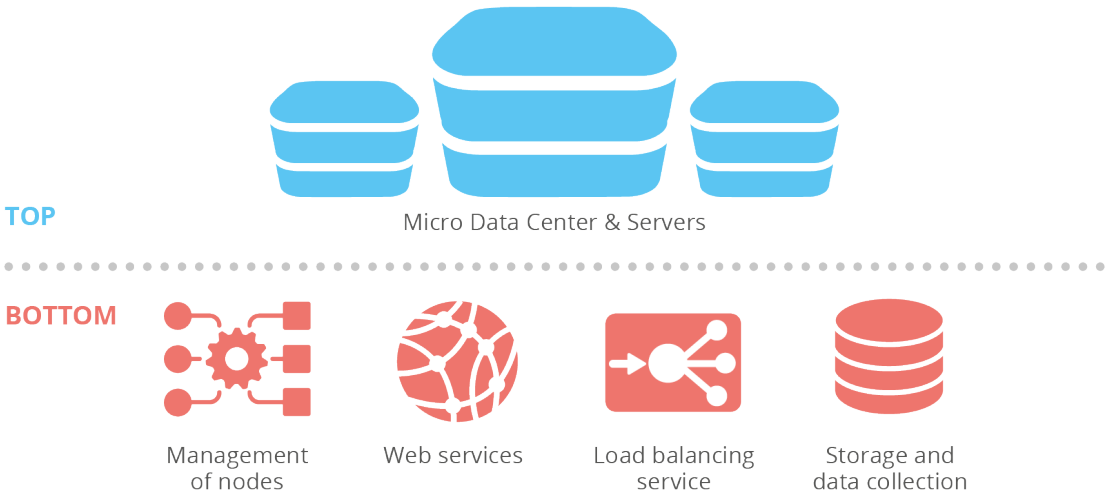
Figure 1: Cloud, fog and edge computing and how they are connected



2.1.1. Architecture

Fog computing architecture and cloud architecture are quite similar. Fog design is a pyramidal scheme that serves as a bridge between cloud and edge computing. In order to handle the data and communication of edge nodes, there are numerous devices at the bottom layer of fog computing. As shown in Figure 2, the bottom layer is also responsible for the connection to the edge nodes. The monitoring layer sits on top of it and is made up of servers and tiny data centres that keep an eye on the functioning of lower fog nodes and edge equipment.

Figure 2: Fog computing architecture



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

3. STANDARDISATION

3.1. FOG AND EDGE COMPUTING STANDARDISATION OVERVIEW

Due to the fog and edge computing paradigms, several national and international organisations and interested communities started to set up, among other things, initial terminologies, architecture models, reference technology stacks, recommendations and best practices. Currently the list of active groups is growing, and it is essential to provide an up-to-date overview over short periods. In the following section, a general overview of the standardisation activities within these groups is presented; a more extensive analysis is performed in separate sub-sections for dedicated groups and initiatives that have released security specifications. This section outlines the most prominent efforts in fog and edge computing standardisation in relation to security. It should be noted that edge computing has released a significantly higher amount of security specifications, whereas in fog computing the groups that are invested in the security aspect are Industrie 4.0' groups.

3.1.1. ISO/IEC

Edge computing is part of the work of the joint technical committee of ISO and IEC (ISO/IEC JTC 1). The organisations focus on the architectural foundation, relationships with IoT, cloud, smart infrastructures, etc. No dedicated specifications have been released in terms of security.

3.1.2. ETSI

At ETSI, the industry specification group (ISG) on MEC is creating a standardised, open environment allowing for the efficient and seamless integration of applications from vendors, service providers and third parties across multi-vendor MEC platforms. ETSI has released dedicated specifications regarding MEC security for edge computing, which is further analysed in Section 3.3.

3.1.3. GSMA

The *Groupe Spécial Mobile* Association (GSMA) Foundation is not a formal standards body but a global member-led organisation representing the mobile industry with impact on international standardisation work. It mainly focuses on a unified edge computing infrastructure for multiple operators. GSMA has released a list of security requirements in their NG.126 document, which references and is based on ETSI and NIST recommendations. More specifically, the GSMA Telco Cloud model ([6]) is a framework for deploying and managing cloud-based services in the telecommunications industry. The Telco Cloud model is designed to provide a common set of principles, guidelines and architecture for building and operating cloud-based services in the telecom sector.

One of the key aspects of the Telco Cloud model is its focus on security. The model includes a number of security features and best practices that are designed to protect telecom networks and services from potential threats and attacks. These features and practices may include the following.

- **Strong authentication and access controls.** The Telco Cloud model includes guidelines for implementing strong authentication and access controls for cloud-based services. This may include the use of multi-factor authentication, secure access

([6]) GSMA | Telco Edge Cloud Forum – Future Networks

mechanisms and other security measures to ensure that only authorised users can access the cloud-based services. No explicit mention of edge or fog computing.

- **Encryption.** The Telco Cloud model recommends the use of encryption for protecting sensitive data and communications in the cloud. This may include the use of encryption algorithms, such as AES or RSA, and the implementation of encryption at different layers of the network, such as the application, network and transport layers. The recommendation can be related in an abstract manner to fog and edge computing.
- **Network security.** The Telco Cloud model includes guidelines for securing the network infrastructure that supports cloud-based services. This may include the use of firewalls, intrusion detection and prevention systems, and other security measures to protect the network from potential threats and attacks.
- **Security monitoring and management.** The Telco Cloud model recommends the use of security monitoring and management tools to help identify and respond to potential security incidents. This may include the use of security information and event-management systems, network traffic analysis tools and other security tools to monitor the network for signs of security threats or attacks.

Overall, the GSMA Telco Cloud model provides a framework for deploying and managing cloud-based services in the telecom industry, with a strong emphasis on security. However, it does not specifically focus on either edge and fog computing, and the related security recommendations refer to cloud deployments in general. The model includes a number of security features and best practices that are designed to protect telecom networks and services from potential threats and attacks.

3.1.4. 3GPP

The 3GPP telecommunications standardisation body, from Release 17 of the 5G standard, aims to provide native support of edge computing in 3GPP networks. Paired to the edge computing specifications, a dedicated document on edge security accompanied by the secure edge architecture, and various security vulnerabilities and mitigation actions has been released. This is covered in Section 3.3.

3.1.5. IIC

The Industrial Internet Consortium (IIC), formerly known as OpenFog, builds the technical foundation for the IIoT and has released various specifications regarding overall IoT functionalities, requirements and operations. IIC has released a dedicated and extensive set of specifications regarding fog computing security, which is covered in Section 3.2.

3.1.6. Industrie 4.0

Industrie 4.0 is an I4.0 platform and specification group which promotes the development of I4.0 innovation in Germany. Industrie 4.0 has different working groups to tackle different challenges. In the context of fog computing, the specifications regarding the security aspects defined by the dedicated security group are covered in Section 3.2.

3.1.7. AIOTI

The aim of the Alliance for the Internet of Things Innovation (AIOTI) is to contribute to the creation of a dynamic European IoT ecosystem. AIOTI has released various specification documents regarding joint fog and edge computing activities. In the various specification documents, the security aspects that are referenced and used as a basis are mainly ETSI- and 3GPP-inherited.

3.1.8. EECC

The European Edge Computing Consortium (EECC) has released the specification Reference Architecture Model for Edge Computing, developed reference technology stacks (ECCE Edge Nodes), identified gaps and recommended best practices by evaluating approaches within

multiple scenarios ('Pathfinders'). However, no dedicated specifications regarding fog or edge security aspects have been introduced.

Figure 3: Overview of the standardisation bodies related to fog and edge computing

Below, the activities focused on the security standardisation aspects for fog and edge computing in relation to 5G are further analysed.

3.2. FOG COMPUTING SECURITY IN 5G

The term 'fog computing' commonly refers to the multi-layered computing infrastructure between end devices and cloud services. From the 5G perspective, it has been usually introduced in IoT-related specifications and standards supporting the cloud-to-thing continuum. Several standards-developing-organisation and industry forums have provided definition and specifications for fog computing in 5G from the security perspective.

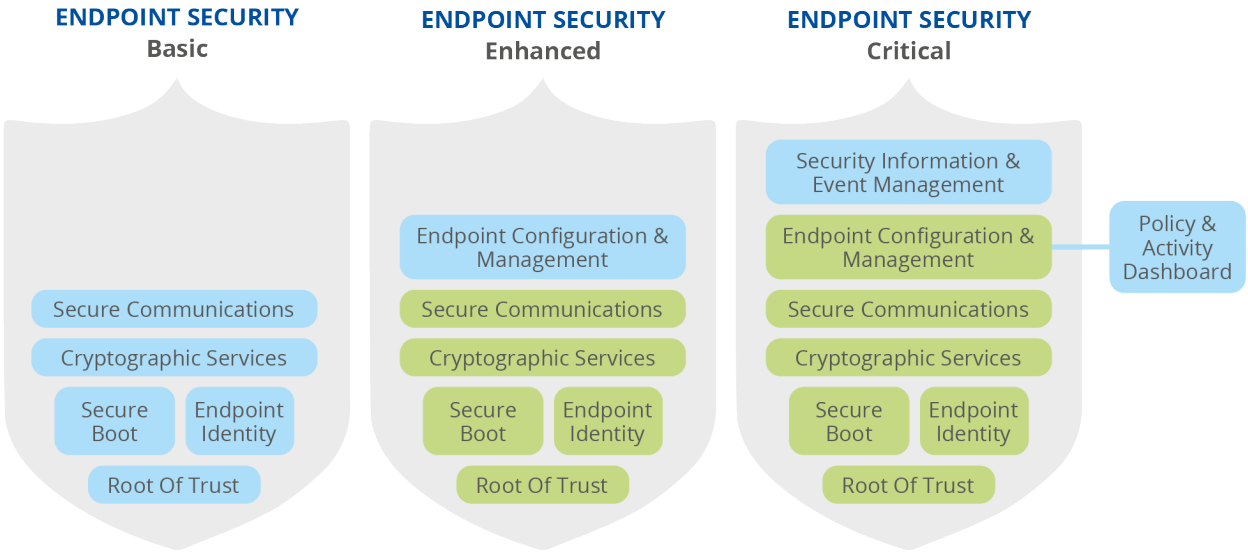
The IIC defines fog computing as 'a horizontal, system-level architecture that distributes computing, storage, control and networking functions closer to the users along a cloud-to-thing continuum' [21]. The automation industry defines the edge as the connection point between IT and operational technology (OT). Hence, edge computing sometimes refers to applying IT solutions to OT problems such as analytics, the need for more flexible user interfaces, or simply having more computing power than an automation controller does. The industrial internet is an internet of things, machines, computers and people. IIoT systems connect traditional OTs (e.g. industrial control systems) with people and traditional IT-based enterprise systems, forming larger end-to-end systems.

In its document entitled 'IIC endpoint security best practices', the IIC recommends suitable mechanisms for endpoint security in industrial applications under the broader scope of industrial internet security, by providing a concise description of the countermeasures needed to achieve a desired level of security for an endpoint while also achieving the appropriate safety, reliability, resilience and privacy. The document defines three levels of security: basic, enhanced and critical. These levels are defined based on the IEC document entitled 'System security requirements and security levels' (IEC 62443 3-3) [22]. Each security level is described as follows: 'Security Level Basic (SLB) provides protection against 'intentional violation using simple means with low resources', such as an ordinary virus. 'Security Level Enhanced (SLE) steps up to defend against 'sophisticated means with moderate resources', such as exploiting

known vulnerabilities in industrial control system software or systems. 'Security Level Critical (SLC) steps up further to defend against attackers with 'sophisticated means with extended resources', such as the ability to develop custom zero-day attacks. Each endpoint should have an appropriate level of security. The aforementioned security levels can be mapped to different security architectures that a fog system can be based upon. The different security architectures consist of different modules including but not limited to secure communications, cryptographic services, root of trust and others, which are further detailed below.

For each security level defined in IIC, a corresponding schema is also proposed, depicting the different security modules that comprise this level and the different layers between them. As security layers evolve new feature are introduced, which can be depicted in Figure 4 through the highlight of the new features. This narrated security evolution depicts the endpoint fortification and how it can be enhanced through its layer. The diagram in Figure 4 describe the different endpoint security architectures that IIC proposes for fog and IIoT endpoints.

Figure 4: IIC endpoint security architectures (newly introduced features are highlighted in green for each layer)



- **Root of trust (RoT)** forms the basis for the endpoint's security and determines the level of trust attainable by the device. This is related to the implemented software and hardware. For SLE and SLC, RoT should be implemented in the hardware. In order to attain this level of protection, physical hardware tampering, a discrete hardware security chip or an integrated security block with tamper resistance is generally required.
- **Endpoint identity** is an essential element in the security of fog ecosystems. Public key infrastructure (PKI) support is mandatory across all levels (basic, enhanced, critical); it also facilitates certificate chaining and the checking of the provenance of the different elements of the supply chain from an endpoint management system perspective.
- **Secure boot** attestation of firmware extends platform-level verification and assists in preventing unauthorised over-the-air and over-the-network execution of firmware and OS system loading.
- **Cryptographic services** support different implementations of cryptography across transport protocols (data in motion), storage (data at rest) and applications (data in use).
- **Endpoint configuration management** serves as the module to verify any remote or automated update to the firmware, OS, configuration and application, without relying on blacklists and whitelists for scalability across numerous endpoints.

- **Secure communications** enable a secure end-to-end communications protocol stack for all levels (SLB, SLE, SLC), in order to support:
    - extensible authentication protocols;
    - cryptographically protected endpoint-to-cloud connectivity;
    - cryptographically protected endpoint-to-endpoint connectivity;
    - trusted data transport based on secure public–private key pairs (PKI), and use of modern quantum-resistant cipher suites;
    - local endpoint firewall for network whitelisting and ingress/egress access controls;
    - interoperability across multi-vendor systems;
    - compatibility with security mechanisms used by core connectivity protocols defined in the industrial internet connectivity framework [23], regardless of whether these mechanisms are implemented with open-source stacks or closed-source stacks.
- Continuous monitoring for control configuration to detect and prevent unauthorised firmware changes and application-level controls to detect data confidentiality and integrity compromise.
- Policy and activity dashboard for visibility and remote control of the endpoints.
- System information and event management (SIEM) for incident response and audits to provision policy-based risk monitoring profiles, distribute rules using open interfaces, feed behavioural analysis and log the generated events into SIEM services.

Industrie 4.0 also provides a compliance framework in its 'IT Security in Industrie 4.0' document [24], where the IT and OT convergence is mainly covered, presenting the risks and challenges of the integration of IT assets in industrial environments. In order to achieve an appropriate level of security despite the increasing networking of production, zones with similar protective needs must be identified and separated from each other using technical means. This must happen in such a way that the separation of the individual system areas does not essentially restrict production processes. Communication between the zones can continue to take place if the transitions are clearly defined and secured accordingly. A careful zoning with corresponding identification and securing of information flows can therefore guarantee a high level of security, also in the highly networked system landscapes of Industrie 4.0. This can be achieved by carrying out the following.

- **Separation of system sub-networks.** System sub-networks can also be separated horizontally in the same way. This is necessary to counter any further compromising of upstream and downstream installations and systems following a successful attack on sub-systems of production. The necessity for horizontal separation becomes directly visible if the production system is considered in the context of Industrie 4.0. Actual production extends over a large number of systems and system groups, the components of which transfer not only data, but entire functions in some cases.
- **Zone transitions.** In order to segment the identified zones, special transitions should be established between them. The entire communication between two zones is then channelled through a zone transition of this type. Concentrating the communication channels makes filtering, monitoring and generally the securing of communication between zones considerably easier: the systematic implementation of zone transitions has the advantage of substantially reducing the complexity to be considered because instead of the communication channels between individual components, merely the zone transitions between zones of component groups need to be considered.
- **Radio technologies.** The described concept of zones and zone transitions should also be systematically transferred to radio technologies. This means in particular that all transmitters should at least be assigned one zone and that the defined zone transitions should be carried out via corresponding wireless gateways. The secure configuration of the radio technologies used plays a central role here. Low ranges should be achieved by shielding and adjusting the signal strength. The selected radio technology

should also guarantee a vulnerability to faults which is as low as possible (e.g. by means of frequency hopping).

- **Remote access connections.** For example, remote servicing by the integrator can also be incorporated in the defined zones and their transitions. Remote access should always be implemented through at least one zone transition, whereby this should be protected from failure by the use of redundant gateways.
- **Cryptography.** Many of the protective mechanisms already mentioned are based on cryptography. In order to guarantee secure communication, strong authentication or data confidentiality and data integrity, mathematical procedures are used which provide adequate protection in accordance with the current state of play.
- **5G operator's PKI.** Ideally, the system operator will already have a PKI for office IT use, with which they will also be able to generate certificates for their systems and modules and for the network equipment. In this case, it is important that new system components can be integrated into the existing PKI.

The specifications and guidelines are based on the detailed analysis in the various industrial guidance and compliance frameworks that already exist [25] and NIST SP 800-53[26].

3.3. EDGE COMPUTING SECURITY IN 5G

Edge computing refers to any computing or networking resource operating between end-devices' data sources and cloud-based data centres. In the context of 5G, the scope is extended to the radio access network (RAN) and core infrastructure domains, where edge computing acts as either as an enabler or extender or existing services. Several standards-developing-organisation and industry forums have provided definitions of edge computing.

ISO defines edge computing as a 'form of distributed computing in which significant processing and data storage takes place on nodes which are at the edge of the network' [27] [ISO_TR]. ETSI defines MEC as a 'system which provides an IT service environment and cloud-computing capabilities at the edge of an access network which contains one or more type of access technology and in close proximity to its users' [28]. Stakeholders from various industries approach edge computing using different terms and reference models, although in practice these approaches are not incompatible and may coexist.

- The telecommunication industry tends to use a model where edge computing services are deployed over NFV infrastructure, at aggregation points or in proximity to the user equipment (e.g. gNodeBs) [29].
- Enterprise and campus solutions often interpret edge computing as an 'edge cloud', i.e. a smaller data centre directly connected to the local network (often referred to as 'on-premise').

3.3.1. 3GPP

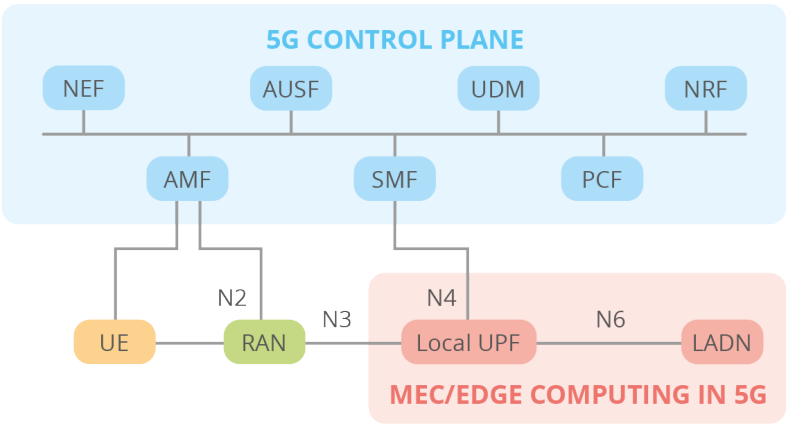
The 5G Core Network is a key enabler for edge computing. From the 3GPP Release 16, MEC was introduced with several capabilities supporting mobile edge computing, including the following.

- **User plane function (UPF) reselection.** The ability of an application function to influence UPF (re)selection and traffic routing directly via the policy control function (PCF) or indirectly via the network exposure function (NEF), depending on the operator's policies. NEF is a key feature for 5G network exposure in the edge and fog computing paradigms.
- **Local routing and traffic steering.** The 5G core network provides the means to select traffic to be routed to the applications in the local data network. A protocol data unit (PDU) session may have multiple N6 interfaces toward the data network. This is a key extension for enabling data processing in local edge and fog nodes.

- **Session and service continuity.** The session and service continuity is designed for different UE and application mobility scenarios, especially for complex edge scenarios involving multiple users.
- **Network capability exposure.** NEF helps to expose capability information and services of the 5G core network functions to external entities. Such entities could include application functions such as MEC-system functional entities. It also enables advanced monitoring for different edge and fog devices.
- **QoS and charging.** The integrated deployment of MEC in a 5G system relies on the UPF as the PDU session anchor and gateway to data networks where the MEC environment is deployed. The PCF can provide QoS and charging rules for PDU sessions associated with MEC. This ensures that the MEC-related user plane traffic receives the correct QoS treatment and is billed appropriately.
- **Local area data network (LADN).** Support of LADN by the 5G core network by providing support to connect to the LADN in a particular area where the applications are deployed.

These capabilities can be depicted in the overall architecture and inter-connections derived from the 3GPP standards regarding the integration of MEC interfaces in the 5G core plane.

Figure 5: 3GPP 5G core and MEC interfacing architecture

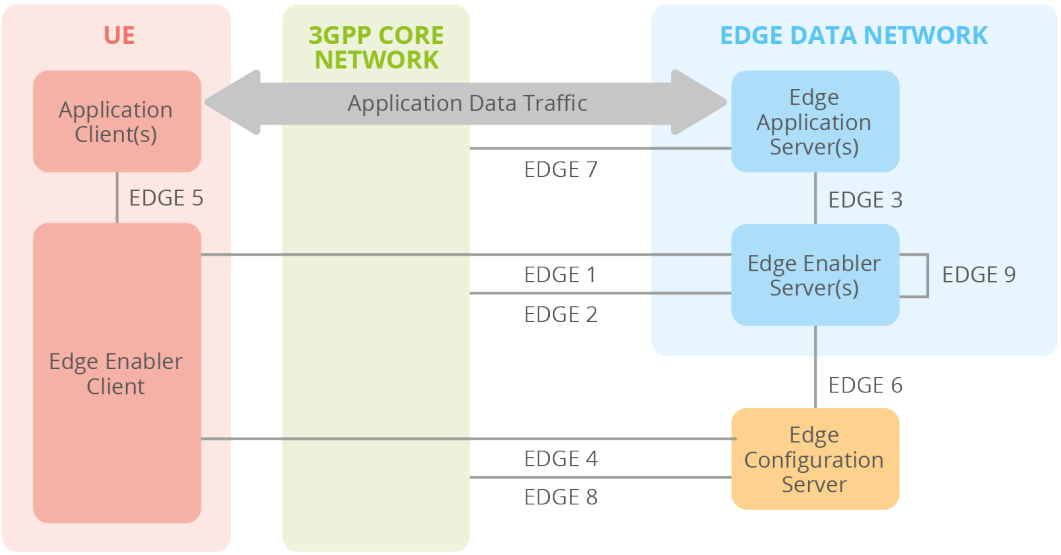


Local UPF support with local area data network (LADN)

This further extension of the edge functions and their corresponding softwarisation has led to an agile 5G system prototype, where different MEC/edge modules can be dynamically scaled in/out and integrated into the existing telco system. The MEC/edge modules mainly refer to the local UPFs and the LADN created by the associated applications of the system. Furthermore, 3GPP has included more security-specific details in the standards.

3GPP has defined its own set of specifications for security enhancements on the support for edge computing in 5G networks in TR 33.839[30]. 3GPP has defined edge applications and their relevant interfaces in TR 23.758 [31] and TS 23.558 [32]. The definition and study of security enhancements for the edge is based on the 3GPP-defined architecture for enabling edge applications, depicted in Figure 6.

Figure 6: 3GPP secure architecture for edge applications



Within this architecture, the edge-enabling client (EEC) deployed in the UE retrieves the edge configuration information from the edge configuration server (ECS). The edge configuration information includes the information that allows the EEC to connect to the EES (e.g. EDN service area); and the information for establishing a connection with EESs (such as URI). Based on the edge configuration information, the EEC could also acquire the required EAS information from the discovered EES. The ECS enables other authorised EESs to access their services. Meanwhile, the EES enables other authorised EASs to access their services.

On the basis on this workflow, a set of security threats has been identified, which cover potential security breaches between the different interfaces from the 5G core to the edge, as well as the corresponding security requirements. A representative list of the security threats and their counter-requirements is provided below.

- **Security threat #1.** When registration, discovery or deregistration is used without authorisation, a malicious EEC receives a list of the services and 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 an edge data network or use this information for competitive reasons.
  Security requirement #1. The edge enabler server needs to be able to determine whether the EEC is authorised to access the edge enabling server's services.

- **Security threat #2.** If access to provisioning and configuration information is granted without authentication and authorisation, a malicious EEC will be able to receive a list of configuration information from the edge enabling server, along with the topology structure of the edge data network, from the provisioning response message. The information received can reveal the edge data network's topology.
  Security requirement #2. The ECS needs to be able to determine whether edge-enabling the client is authorised to access provisioning services offered by the ECS.

- **Security threat #3.** Registration updates without any confidentiality or integrity can help a MitM actor impersonating the ECS to the edge-enabling server to expose and possibly alter the registration updates with a falsified edge-enabling server profile.

Security requirement #3. The ECS and the edge-enabling server need to perform mutual authentication to register and update the server profile information.

- **Security threat #4.** If user identifiers and credentials are not protected, a number of well-documented attacks can result in the loss of privacy, user data and other sensitive information for the users.

- **Security threat #5.** An unauthorised UE may be able to use the services provided by the target edge data network.
  Security requirement #5. Authentication of the UE and the target edge data network shall be supported during edge data network relocation with seamless change. Authorisation of UE for EAS service access during edge data network relocation with seamless change shall be supported.

Overall, 3GPP defines in detail different interfaces between the edge and the 5G core network that are vulnerable to attacks and security breaches, and lists a set of potential preventive requirements, as well as proposed solutions to further fortify the infrastructure of a 5G network.

3.3.2. ETSI multi-access edge computing

ETSI MEC focuses more on the orchestration of the MEC applications and defines a set of recommendations that a MEC platform manager should follow. As defined in the ETSI MEC 003 standard, the MEC reference architecture consists of different functional elements, the infrastructure of which should be secured at every level according to best practices for similar non-MEC-specific technologies.

The MEC platform manager has privileged access to all the managed MEC hosts where MEC applications are running, and therefore should be protected against unauthorised access using best practices of access control, for example least privilege principle, separation of duties, role-based access control / attribute-based access control policy enforcement, to name a few. In particular, the MEC platform manager should strongly authenticate requests (e.g. with X.509 certificate) on its management interfaces (Mm2/Mm3), to verify whether they originate from an authorised MEC orchestrator or OSS. Similarly, the underlying VIM, which manages the virtualisation infrastructure of the MEC hosts (where the data plane runs), should strongly authenticate requests on its management interfaces (Mm4/Mm6) as coming from an authorised MEC platform manager if not in the same trust domain (e.g. co-located), or an authorised MEC orchestrator.

The MEC hosts must be secured according to best practices of server security and virtualisation infrastructure security.

- **NFV recommendations.** For MEC systems based on the NFV architecture and running sensitive workloads, the ETSI NFV-SEC 003 specification defines specific security requirements for the isolation of such workloads (e.g. security functions) from non-sensitive ones and describes different technologies to enhance the security of the host system (e.g. MEC host) in this regard: system-hardening techniques, system-level authentication and access control, physical controls, communications security, software integrity protection, trusted execution environments, hardware security modules, etc.
- **MEC-specific recommendations.** MEC platform should strongly authenticate requests on its Mm5 interface as coming from an authorised MEC platform manager. Similarly, the virtualisation infrastructure should strongly authenticate requests on its Mm7 interface to make sure each one is a valid request from an authorised VIM. Furthermore, inside the MEC host, isolations of both resources and data must be guaranteed between the MEC apps, since they may belong to different tenants, users or network slices in the 5G context. In particular, the MEC platform is shared by the

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

sends an echo response, where the attacker can identify that the source IP of that message is PGW IP [108].

- **IP depletion.** The packet injection method described earlier to provoke an information leak threat is called GTP-in-GTP, and the attacker can deplete IP pools allocated to terminals in the core network through the same method. The attacker can increase the terminal number in the 'create session' request sequentially, so that the PGW allocates multiple IPs. If the PGW allocates all available IPs, 'create session' requests from normal terminals would be rejected and all of terminals accessing that core network would not be able to communicate [109].
- **DoS.** An attacker can continuously send an attach-request message to access the 5G core network by configuring multiple botnets and repeatedly turning the airplane mode on and off. This will result in excessive traffic load on a certain mobile carrier's core network, Since each attach request can generate approximately eight GTP-C messages, resulting in eight times the amount of traffic to the 5G core in the core network compared to one malicious action done by the attacker [110].
- **Non-access stratum manipulation**. The ciphering and integrity of non-access level protocol messages for signalling between terminals and the core network, such as attach-request messages used in the first attaching process, are not guarantee , attach-request messages used in the initial attaching step do not have their ciphering or integrity guaranteed. Therefore, an attacker can install a malicious base-station near the victim to steal and manipulate those messages. 3GPP's 33.401 technical specification defines the use of the integrity verification algorithm in terminals as essential, as opposed to the selective use of ciphering algorithm, analysed in detail in an extended evaluation scenario in [111].
- **Spoofing**. IP spoofing is a typical network attack. If an attacker changes the IP of data traffic transmitted from every 5G network to the victim's IP and sends the data traffic, its responses are all delivered to the victim, which can cause invalid charging and even DoS. Additionally, SIP or MMS spoofing can be abused for voice phishing. When the 'from' header that indicates the outgoing number in the SIP packet header is falsified, the incoming terminal displays that falsified number [112].

4. CURRENT OPPORTUNITIES

In this section, we will discuss the current opportunities that exist for fog and edge computing in 5G. Fog computing commonly refers to the cloud-to-IoT convergence, thus usually to a large number of devices with limited computing capabilities. Furthermore, a set of key attributes of fog computing are analysed in this section. These include scalability and elasticity in order to dynamically scale-in/out fog infrastructure according to a use case's needs; network management, as network provision for a large number of devices is always critical; reliability, given the fact that fog deals with limited capability devices and reliable connections must be ensured; sustainability, for the maintenance and life-cycle management of a heterogeneous group of devices; and federation, to be able to dynamically manage and orchestrate an upper-layer multi-modal entity.

Regarding edge computing, the convergence to the 5G domain has been more dynamic and is currently regarded as an extension to the telco infrastructure to provide additional computing capabilities. The main aspects that this section covers are QoE improvements and how edge nodes can further improve different multimedia services close to the user; protocol standardisation and how edge is currently positioned in the telco domain'; heterogeneity handling, to support different architectures and computing capabilities/requirements at the edge nodes; and MEC, which refers to the different connectivity options that edge can offer as an extension to a 5G infrastructure.

4.1. FOG-COMPUTING OPPORTUNITIES IN 5G

4.1.1. Scalability and elasticity

While fog computing does not have the scalability and elasticity offered in cloud computing (limitless processing resources on demand), it can be a viable solution as it offers at least two distinct advantages when compared to edge computing. Unexpected spikes in computational demand will not necessarily violate service-level agreements, and secondly, end users do not have to make sizable upfront investments in computing infrastructure; instead, they can grow naturally as their computing needs increase and only pay for what they use. The first advantage could be realised with the utilisation of scalable services, wherein the allocation of additional computational resources whenever needed has a direct and favourable impact on the performance and QoS of the hosted applications. Scalability research challenges might be divided into hardware, middleware and application levels. Fog providers must explore parallel computing with multi-core accelerators based on graphics-processing units to fulfil hardware needs, while hardware heterogeneity should allow for performance assurance, stability and isolation. Concerning the middleware level, it is important to implement programming abstractions and models that enable developers working on the 'platform as a service' model ([7]) in hybrid cloud/fog computing environments to focus on functional concerns rather than non-functional ones. Lastly, at the application level, there is a need for new algorithms to be introduced that do not inherit the deterministic nature of traditional algorithms to increase overall performance and scalability.

In regard to elasticity, the main research area concerns the ability to correctly predict the computational demands and performance of the applications. Closely related to middleware, elasticity is focused on workload management and performance management to scale up or

([7]) https://en.wikipedia.org/wiki/Platform_as_a_service.

down resources, including the management of cloudlets, such as garbage collection, dynamic creation and mobility.

In short, elasticity and scalability improve overall performance by providing appropriate operational capabilities in a cost-effective manner. Nonetheless, strategic resource management is essential to exploit these capabilities.

In conclusion, scalability and elasticity offer operational characteristics to boost the efficiency of fog computing applications in a way that is still being fully utilised. However, these capacities need to be strategically used through resource management and scheduling algorithms.

4.1.2. Network management

An important aspect of fog computing is the high amount of network usage and the number of users that interact with it [33]. Even though one of fog computing's promising aspects is to cut down on bandwidth utilisation in the internet's core, very few studies have taken this into account. More research is required to determine how much bandwidth may be saved with fog computing. These investigations may be measurement studies that record the real bandwidth consumption while fog computing is present.

Additionally, fog computing is not natively supported by SDN software [34]. Most economically feasible SDN environments are found in large data centres or campus networks. Therefore, improving and standardising SDN software for fog use cases would make it simpler to design fog-computing software. In addition, new SDN designs with various domains and hierarchies of SDN controllers will be necessary given the number of manufacturers and operators involved in fog systems.

Lastly, high-speed users, including users in vehicles and on trains, and vehicular computing, are not supported by the current communication protocols that are proposed for fog computing settings. One area of research is the development of fast or stateless authentication and handshake protocols for high-speed users and automobile communication. Furthermore, due to the frequent changes in mobile and high-speed IoT environments, fog service provisioning for IoT applications must be dynamic and proactive. Another potential option that needs further research is forecasting the behaviour and location of IoT devices and high-speed users using historical data or machine-learning techniques to provide dynamic and proactive fog service delivery.

4.1.3. Reliability

Fog services and networks present new issues for the current network and service-provisioning techniques in terms of dependability and availability. Fog and cloud computing must be factored into a coordinated service-provisioning system in order to ensure the availability and dependability of the fog services [4]. For instance, adding additional instances of functions that a fog service requires to analyse a stream of data can increase the service's availability. On the other hand, the allocation of the function instances to offer availability and dependability is not an easy choice due to the low computational power of the fog nodes in comparison to the cloud data centres. Future provisioning approaches for fog services may consider availability in addition to restrictions such as latency, throughput and security.

Additionally, the majority of studies in the field of fog computing do not use novel hardware or communication techniques, such as FPGAs, optical networks, FiWi (fiber-wireless) or non-volatile storage technologies. It would be wise to investigate modern hardware and communication technologies to construct fog networks, such as fog-to-cloud connections.

Moreover, to achieve a reliable infrastructure, you have to holistically monitor it. The literature has little research that provides monitoring plans for fog resources. When a fog node is used by

numerous operators or is situated in an area where many users frequent the node, monitoring is beneficial. Creating multi-operator access-supporting fog-resource monitoring methods is one such direction. Another solution that shows promise is the use of SDN-based monitoring software for fog-resource monitoring and fog-resource advertising.

4.1.4. Sustainability

The majority of energy studies focus on energy-aware offloading of computing, energy-aware mobility management, and the federation of IoT devices to reduce fog-system energy usage. However, there has been inadequate research into lowering fog's overall energy consumption. The energy used by a fog network is divided into three main categories: (1) energy used by IoT devices delivering data to the fog, (2) energy used by the network linking IoT devices and the fog nodes, and (3) energy used by the fog nodes themselves.

The use of energy harvesters and battery storage for IoT devices and sensors are promising research paths for lowering the energy consumption of IoT devices. Energy harvesters have the potential to reduce energy usage while presenting additional systemic difficulties, including uncertainty and unpredictability. One of the potential study paths is to determine where to place fog nodes and how close they should be to end users in order to reduce the energy consumption of the network-connecting IoT devices and the fog nodes. Another intriguing use case for energy usage is mobile fog nodes. Reducing the distance between fog servers and nearby renewable energy sources is one possible research direction for lowering the energy consumption of fog nodes. There are several approaches to solve this issue, including redirecting IoT device communication to a nearby fog node that uses renewable energy. The other option is for telecommunications firms to locate the fog nodes that require a lot of power to handle traffic and to persuade consumers to power their local fog nodes with local renewable energy from their microgrid.

4.1.5. Federation

There is currently no framework or program for controlling and federating fog resources across several operating domains, akin to hybrid cloud federation approaches. New federation systems for fog nodes are required, especially when they come from several operating domains. Models of resource-sharing for fog nodes from various vendors and operators should be taken into consideration by the federation system. For federated fog resources, new pricing models can be defined similarly. Finally, using the federation framework, policies for fresh fog resource sharing schemes (such as a P2P fog-computing, resource-sharing model) can be suggested.

4.2. EDGE COMPUTING OPPORTUNITIES IN 5G

4.2.1. Quality-of-experience improvements

QoE is a metric used to gauge how satisfied a consumer is with a service provider overall. QoS, which represents the idea that the hardware and software characteristics can be measured, improved and guaranteed, is linked to QoE but is different from it. It is difficult to strike a balance between an application's higher availability or seamless connectivity, which the cloud can offer when an end-user device is not close to the edge server, and its higher QoE, which the edge cloud can offer when UEs are close to the edge server, in order to reduce jitter and delay. Therefore, collaborative computational methods such as hybrid computing are applicable. Edge computing provides proxying capabilities on behalf of user equipment and can be used to manage network or service states for developing applications. The trade-off between availability and QoE performance can be accomplished with less signalling overhead experienced by network activities by retaining the network states. To reduce signalling overhead, the signalling messages can also be combined. This results in less network congestion, which boosts network performance and scalability. QoS could be enhanced by addressing this unresolved problem.

4.2.2. Protocol standardisation

A set of widely recognised guidelines for edge computing in the 5G ecosystem must be provided by standardising bodies or organisations in order for protocols to be standardised. There are primarily two difficulties. First off, because the edge cloud is flexible and may be customised in a variety of ways by various vendors, it is challenging to come to an agreement on a standard (such as the location and capabilities of the edge cloud). Second, several heterogeneous end-user devices communicate with the edge cloud using various interfaces. In order for different layers and computing paradigms to cooperate with one another in a multi-vendor environment, standardisation efforts have been put in place, such as the initiative set up by ETSI [35].

4.2.3. Heterogeneity handling

With regard to edge computing for 5G, the heterogeneity of communication and computing technologies has made it challenging to provide a solution that is adaptable to many environments. For edge nodes, software-based or programming-based techniques may create a programming model to make it easier to run workloads concurrently at various hardware levels. However, a thorough distributed computing system must enable cooperative operation between the various systems. Workload is divided into separate, more manageable tasks using data and task-level parallelism, which can then be carried out concurrently across many pieces of hardware and cloud edge layers. The suggested methods make it possible for edge servers and other end-user devices to communicate.

4.2.4. Multi-access edge computing

The need to have cloud computing capabilities at the network's edge led to the fast adoption of MEC. While there are two main categories for MEC – dedicated MEC and distributed MEC – the focus should be on distributed MEC since dedicated MEC is designed to be tailored for specific solutions/businesses. Moving cloud-computing capabilities to the edge provides scalability to the infrastructure with ultra-low latency and high bandwidth. Moreover, distributed MEC is fit to be deployed in public 5G networks, while retaining the edge-computing applications to protect against cybersecurity threats, moving the security perimeter closer to the source. However, several issues need further research for a MEC-ready environment. While through MEC deployment we can minimise latencies through optimal bandwidth utilisation, the optimisation of spectrum usage regarding complex system components is lacking [36].

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

verified [45]. When IoT network-connected devices ask for endless processing/storage services, the attack may be initiated. In other words, a compromised or broken node could repeatedly ask a fog node for processing or storage, delaying requests from reliable devices [37]. When several nodes fire this attack at the same time, its intensity doubles. Spoofing the addresses of numerous devices and sending phony requests is an additional method of launching this attack [46]. Due to the openness of the network, existing protection mechanisms for other types of networks are ill-suited for fog computing. The scale of the network is the first significant obstacle. Potentially hundreds of thousands of nodes in a 5G network use fog to get around computational and storage constraints and improve performance. Since none of these devices can be verified as authentic by fog nodes, they may rely on a reliable third party, such as a certification body that grants credentials, to verify authenticity [47]. However, the processing fog node can only verify the presence of such credentials to confirm that the request was sent by an authorised node. As a valid member of the network, a compromised node would accommodate all such requests. On the other hand, limiting network connectivity or filtering queries made by devices renders the purpose of fog nodes useless. Additionally, the address space is rather vast and without boundaries, therefore spoofing addresses is more straightforward.

5.1.2. Virtualisation security

Hybrid cloud/fog environments can use virtualisation to flexibly provision security resources and features, including firewall functionalities, DDoS protection, intrusion detection systems (IDS) and intrusion detection systems (IPS) [48]. However, other system elements such as the orchestrator, SDN controller, network controller and NFV security orchestrator are necessary for dynamic deployment to be successful. Because of these dependencies, the security functions themselves are exposed to the risks and weaknesses of the underlying components [49]. Additional dangers in security-function virtualisation are caused by pertinent integrated automation methods [50].

5.1.3. Software-defined networking security

SDN controllers consist of two APIs: north-bound APIs and south-bound APIs. North-bound ones are responsible for getting information about the network activity, whereas south-bound ones are responsible for the management of the network [51]. Given the information acquired by north-bound APIs and the management of the routers and switches through south-bound APIs, an SDN controller can enable dynamic safeguards. It thus strengthens the capacity to promptly counteract cyberattacks and increases network resilience. Nevertheless, an SDN controller's north-bound and south-bound interfaces are vulnerable to intrusions. Threats such as spoofing, REST API parameter exploitation, MiTM attacks and DoS attacks, protocol fuzzing, API flood assaults, and impersonation of SDN controllers can all be directed at SDN controllers [42]. To guarantee that the SDN controller runs reliably, effective mitigation procedures must be established to identify these attacks and implement the necessary countermeasures.

5.1.4. Data security and privacy

5G networks are heterogeneous and therefore the data that is retrieved from the various devices are of various types that are used to 1) enable essential functions and use cases and 2) enable the automation of decision-making in applications and system management and orchestration [52]. Data is an integral aspect of 5G. Several scenarios, including classification and appropriate protection for at-rest and in-transit data, should be considered from a security standpoint in this situation. When developing or setting up the system, privacy should be taken into consideration to make sure that only relevant data is gathered and stored [53]. A systematic framework with clear objectives, monitoring and controls should govern data sharing among 5G subsystems, use cases and slices [54].

To lessen the overall strain on the data centre, fog computing relies on the computational capability of remote nodes [55]. In fog computing, privacy protection is more difficult because, in contrast to faraway cloud servers that are located in the main network, fog nodes that are close

to end users may acquire sensitive information about the identity, utility usage (such as smart grid) or location of end users. Furthermore, since fog nodes are dispersed across such a broad area, centralised control has become more challenging [33]. An entry point for a network thief could be a compromised, weakly protected fog node. Once inside the network, the intrusive party has the ability to harvest and steal entities' exchanged user privacy data. Privacy leakage may also result from increased communication between the three layers that make up the fog architecture. Since the location of equipment can be used to identify its owners, location privacy is one of the most crucial models for privacy. Since fog clients delegate their work to the closest fog nodes, an adversary can learn about your location, trajectory and mobility patterns. By examining how a user uses fog services, such as the smart grid, user habits can also be discovered by the adversary. The measurements from smart meters can reveal more personal information, along with information about when the residence is empty [56].

5.1.5. Trust

The end users can expect to receive dependable and secure services from 5G networks. This necessitates a certain degree of mutual trust between all of the fog network's devices. In order to establish the initial set of connections between devices and fog nodes in the network, authentication is crucial. However, this is insufficient because technology is prone to errors and harmful attacks [57]. In this situation, trust is crucial to developing relationships based on prior contacts. A fog network should have a two-way relationship with trust. In other words, the fog nodes that provide services to devices should be able to verify the legitimacy of the devices making service requests. On the other side, devices should be able to confirm whether the targeted fog nodes are actually safe before sending data or other valuable processing requests. Maintaining dependability and security in the fog network necessitates the establishment of a strong trust model. The issue of trust in the cloud-computing environment has been addressed by several studies [58], [59]. However, it is necessary to reconsider this issue given the particular difficulties offered by the fog computing environment. In contrast to a cloud computing environment, a fog node is required to account for past interactions with devices in the form of trust and reputation.

5.1.6. Authentication

One of the most important requirements in a fog network is the authentication of networked devices that have subscribed to fog services [60]. A device must first join the network by authenticating itself to the fog network in order to use the services of the network. This is necessary to stop illegal nodes from entering. But as the network's participating devices are limited in terms of power, processing and storage, this turns into a daunting problem. Due to the resource limitations of 5G-connected devices, conventional authentication methods utilising certificates and PKI are not suitable. As an alternative, multicast authentication employing PKI has been proposed in [61] for secure communications. In essence, authentication services must be provided as a service alongside storage and processing capabilities, requiring a device to obtain authentication from the fog node through an intermediary, such as the certifying authority. This operational paradigm would stop illegal nodes from joining the fog network. Additionally, this would give the fog nodes the ability to limit service requests coming from rogue or compromised nodes [6].

5.1.7. Open-source security

Various open-source initiatives are currently accelerating the rollout of 5G and SDN/NFV. In order to create open-source technologies that can be deployed to 5G networks, the operator and vendor communities are working together [62]. Although open source has a variety of benefits, such as better data security, lesser vendor lock-in and higher and speedier adaptability to the market', it also confronts a number of challenges, such as a lack of support, concerns about intellectual property, a lack of documentation and graphical user interfaces, and the level of customisation necessary for certain use cases. Additionally, each of them brings up security concerns that the open-source community must address [51].

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.

5.2.1. Authentication

The development of inter-cloud identity management systems is pursued in a variety of ways [72][73]. Such methods allow for single-sign-on authentication between clouds by utilising a number of standards, including SAML ([8]) and OpenID ([9]). There are a number of technologies that allow for reciprocal authentication for P2P computing without requiring a connection to a central authentication server [73]. All of these approaches may be modified to handle the authentication of edge data centres that are a part of various trust domains because their design is consistent with the underlying infrastructures of edge paradigms.

5.2.2. Network slicing security

A security aspect in terms of network slicing can be put in place to better shield the edge nodes. The current use of network slicing, however, also raises security issues [74]. To enable trusted virtualised architecture and maintain effective slice isolation, the right security policies must be put in place. Slice categorisation and sufficient resource provisioning are examples of such security mechanisms. To further restrict and secure information transfers between slices, strict security rules must be put in place. Numerous dangers, including side-channel attacks across slices and DoS attacks using the exhaustion of virtual resources, would be prevented and mitigated as a result [75].

5.2.3. Multi-access edge computing security

While the adoption of MEC brings significant improvements in terms of security and privacy, it also exposes new threats in the ecosystem. The use of mobile devices and the deployment of edge cloud servers widens the threat landscape. Several security solutions tailored to mobile cloud computing cannot adapt to MEC, while at the same time traditional data security methods cannot be applied to edge devices since they are resource constrained [76].

Additionally, MEC being a technology integrated into 5G increases the chances for successful attacks such as DoS/DDoS, VNF manipulation, VNF location shift and other softwarised attacks [77] [78]. Using auto-configurable security mechanisms to securely authenticate and communicate between VNFs could prevent several of these attacks [79].

5.2.4. Supply chain security

Numerous security vulnerabilities are being introduced in the edge nodes because of the trend of using commodity modular hardware and software more frequently. Backdoors, dormant harmful programs and falsified hardware certificates are a few examples of such dangers [80]. Promising solutions will need to handle this on various levels. For example, implementing certain security restrictions across integrated software and common hardware will be possible thanks to trust platforms that are computationally feasible, such as blockchain. To enable attacks or the detection/prediction of malicious occurrences, the 5G NFV would need to increase its capabilities in security monitoring and anomaly detection [81].

5.2.5. Networking protocol security

Edge paradigms use a variety of communication technologies, all of which are either established standards or the subject of in-depth research by both business and academics. They establish their own security procedures and controls that can guarantee data integrity and privacy between two authenticated organisations. The distribution of the credentials that will be used to negotiate the session keys is one of the difficulties in this area [82]. Even so, there are remedies, even though further research is required. A designated certification authority, for

([8]) https://en.wikipedia.org/wiki/Security_Assertion_Markup_Language
([9]) https://en.wikipedia.org/wiki/OpenID

instance, that is under the jurisdiction of a single infrastructure provider, has the ability to distribute credentials to all the elements that are part of their trust domain [83], [84].

Additionally, the edge paradigm is using virtualised networking, an important aspect one must consider [85]. The security of the virtualised network infrastructure, or the network infrastructure used by the VMs deployed at edge data centres, is another factor that must be taken into consideration. SDN and NFV can both be very helpful when discussing edge paradigm. These methods can be applied in a variety of ways, such as isolating certain types of traffic even in the presence of adversaries, isolating insecure network devices, routing traffic towards security devices, real-time system reconfiguration, etc. Contemplating that NFV and SDN's primary objectives are to streamline network management by virtualising router functions and integrating programmable network control and operation logic. These services are advantageous for edge paradigms as well because managing the network infrastructure is one of the problems that need to be resolved [60], [86], [87]. Summarising, both SDN and NFV have unique security issues that need to be resolved [51], [88].

5.2.6. Intrusion detection

With a few notable exceptions, such as the active honeypot system created in [89], the majority of research on intrusion detection and prevention systems has concentrated on mobile cloud computing [47]. This system's primary goal was to identify local adversaries in mobile edge computing deployments. However, some of these MCC-focused research papers could also be applied to other paradigms. In [90] the design called for mobile devices employing 5G networks to hand off their intrusion detection duties to centralised cloud-based services. Although the focus of this research was on centralised cloud services, it may be possible to modify this framework for a more dispersed strategy in which the IDS services are placed at nearby edge data centres. The state of their surroundings will then be completely visible to such services. A distributed IDS is demonstrated in [91], which was set up in a cloudlet mesh topology. With this design, the cloudlet's members can work together and with other parties to identify malware, malicious assaults, and other threats. A federation of edge data centres may also employ this kind of collaborative IDS to keep an eye on traffic in a specific area [92].

It is entirely viable to reuse different IDS techniques and solutions created for cloud computing [72] and other relevant paradigms, even though there is still work to be done. The primary function of edge data centres is to offer consumers access to cloud computing services. Therefore, IDS that keep an eye on VM activity, internal network activity and their surroundings can be useful for edge data centres [93]. Dealing with the infrastructure's distributed nature, where several trust domains coexist, presents the main issue in this situation. However, many IDS solutions are self-monitoring and do not require centralised infrastructures.

In addition, there are numerous IDS frameworks whose objective is to join and watch over multiple trust domains. These frameworks' components may be reused or modified for our situation. For instance, in [94] the authors presented a security architecture for federated cloud environments that enables the deployment of early warning systems such as honeypots and the early detection of cyberattacks. This design must be implemented in every trust domain's central command and control centre, hence further research is required to determine whether it can be applied to an N-tiered hierarchy. However, the architecture also includes a number of mechanisms that let numerous trust domains coordinate cross-cloud and in-cloud defence operations.

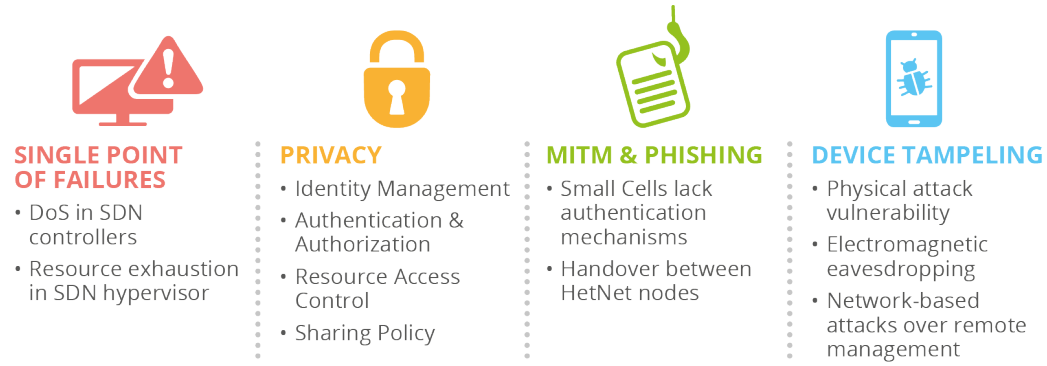
5.2.7. Privacy

In the last few years, privacy has seen a lot of activity in the realm of edge concepts [95]. In reality, many of the security protocols discussed in the earlier sections enable anonymous user interaction with edge data centres and other entities [96]. Additionally, there are numerous data privacy methods created especially for the mobile cloud-computing paradigm. These approaches address a number of issues, such as enforcing privacy standards when transferring

code and data between cooperating mobile devices [97] and hiding the location of a group of clients that are spread across a certain region by building a P2P network [98]. These technologies require that all devices be linked to the internet and be aware of their current position. They are intended for a collaborative cloud of local devices. They might therefore offer some suggestions for the creation of future privacy methods for collaborative edge data centres. There are additional techniques that take full advantage of the idea of interconnected local cloudlets, such as the software-defined pseudonym system for VANETs created in [56].

Let us consider the use scenarios in which there is a trust connection between the users and the nearby edge data centres (such as personal cloudlets and corporate settings). In such circumstances, privacy assistance entities may be set up in the edge data centres. These organisations will serve as the users' interface and may use different data privacy procedures. These controls can be used to manage the accuracy and detail of the personal data that service providers and other distant entities receive [99], [100]. The privacy helpers can also implement other privacy services, such as hiding users' addresses or assuming pseudonyms to shield their identities from other remote services [72].

Figure 8: Overview of security challenges in fog and edge computing for 5G



6. APPLICATION SCENARIOS

6.1. FOG COMPUTING IN 5G

Fog computing is a network computing and services paradigm that provides data, computation and storage services to end users that can be housed at network edge or end devices. It can decrease service latency while also enhancing QoS/QoE and reducing cloud infrastructure workload. It is considered a heterogeneous ubiquitous scenario that combines mobile communication, micro-clouds, distributed systems and big data, in which devices frequently cooperate through the network to provide prompt task processing or storage without the need for third-party interaction, or simply put, a middleman between cloud and edge computing. Therefore, it is crucial to secure data transmission between the devices and prevent any attacks that might occur from unsuspected actors, such as mobile devices, sensors or micro controllers, all of which are prone to botnet attacks.

However, before discussing security, one has to understand the architecture of fog computing to be able to advance further. Fog computing is halfway between cloud and edge – it is the linking component between these two paradigms. Edge devices such as end-user devices, sensors and networked vehicles are using fog computing to interconnect but also communicate through the cloud. Considering that, it is important to secure transmission between devices, promptly mitigate any attack that might be observed and ensure seamless connectivity between the paradigms.

Researchers have looked into many different aspects of fog computing and how to secure it; however, due to the nature of fog computing as a mediator, solutions are focused on data transmission and its privacy.

6.1.1. Fog computing privacy solutions for 5G

Transmitting data between different services, components or stakeholders is a delicate matter, and recent guidelines about data privacy have forced technical companies and organisations to enforce an enhanced privacy system. The term quality of protection (QoP) is often applied as a metric regarding the level of data security to be enforced. In regard to QoP, authors in [36] present a paradigm that enables end users to adjust QoP according to the desired security and privacy. Additionally, data pre-processing is done in parallel; this is based on predicate encryption, a novel cryptographic system which enables end users to choose specifically who can access the encrypted data.

Blockchain is also a technology that could be leveraged due to its decentralised nature and ability to encrypt data and preserve privacy. In [101], authors propose a blockchain-empowered security framework to secure data privacy and analysis which is carried out by a deep learning component in parallel. It is shown that smart contracts can enhance data privacy, preserve anonymity and avoid any leaks to the public. In a similar manner, authors in [6], analyse the effect of combining blockchain and SDN in a VANET environment. Decentralised network management is achieved, while reducing workload and enhancing trust in the network by introducing a trust model that counters any malicious activities and eliminates the need for a central controller, thus eliminating single points of failure.

6.1.2. Fog computing networking solutions for 5G

As mentioned above, by acting as a mediator between cloud and edge, fog computing is also susceptible to network attacks, therefore, studies have focused on how to enhance security at network levels. In [5], authors explain the reasoning behind using fog computing for tasks that

require immediate action and enhance its security by using a network service chaining (NSC) model along with SDNs. NSC is a service model that integrates SDN and NFV to perform fast computation in a 5G environment with the help of various communication protocols, consequently increasing security and the dynamicity of available protocols.

Thanks to the NFV's ability to separate different devices in separate networks, namely network slicing, authors in [102] propose a framework that enables secure service-oriented network slices, allowing for secure data transmission and isolation. These network slices are selected by a privacy-preserving mechanism, allowing for the selection of a proper secure network slice for data forwarding, but also taking away access from malicious users. On a similar note, authors in [56] propose a scalable and efficient scheme for vehicular fog computing. This scheme is based on the Chinese Remainder Theory and has an effect on communication restraints between vehicles and fog computing nodes to ensure mutual trust. Based on this trust, secure network slices are implemented to provide service-oriented slices, thereby avoiding interceptive malicious acts.

6.2. EDGE COMPUTING IN 5G

Edge computing can be defined as a computational paradigm, where edge-processing units, i.e. servers, can form mini clouds (edge clouds) to enhance and extend cloud capabilities at the edge of the network. With the emergence of 5G and the decoupling of different layers of the network, edge computing has been established as a key enabler in the realisation of the full 5G potential. Whether this is to accelerate different services at the edge, cloud-enabled RAN or support for different 5G slicing mechanisms, edge computing offers a wide variety of options to facilitate different scenarios and use cases. The decoupling of resources and computing capabilities allows edge infrastructure to be scalable and agile.

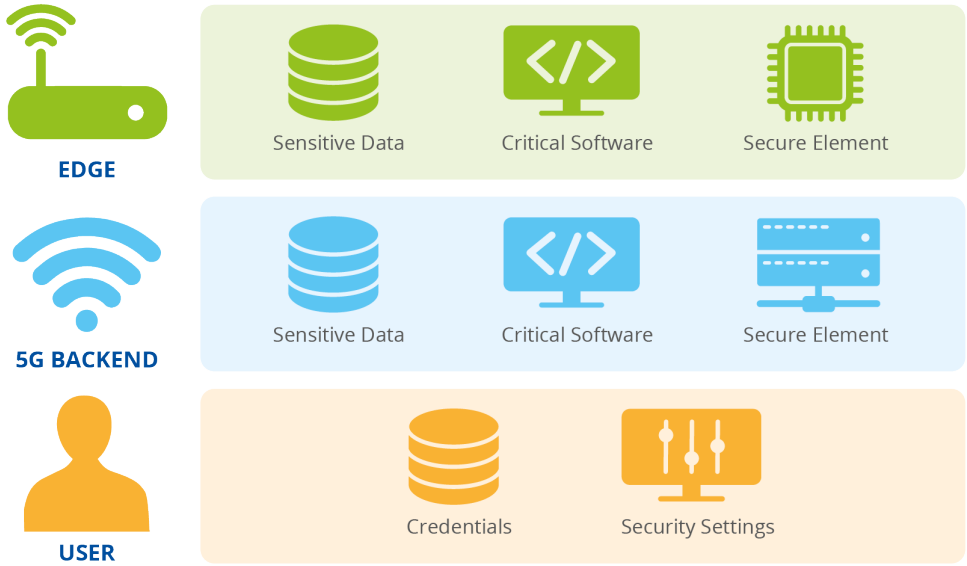
Furthermore, the decentralised perspective that edge computing enables in 5G networks is also susceptible to various threats and security breaches, given its decoupled architecture and operation. Edge servers operate at the last mile of the network, thus they can be inter-located from the rest of the environment, rendering their provision challenging in certain cases. This can lead edge computing resources to be vulnerable to targeted attacks and to security breaches due to deprecated software and hardware updates during their lifetime. Additionally, their user-driven topology and proximity also makes them susceptible to privacy-related attacks, as more than often sensitive user data can be stored at the edge to reduce access speed and latency.

The research community has extensively focused on documenting and covering the security aspects of edge networking in regard to 5G, and has mainly focused on the privacy concerns regarding user data security and the various network-based attack vectors and vulnerabilities that edge servers are susceptible to.

6.2.1. Edge computing privacy solutions for 5G

In edge computing, privacy may refer to many aspects, including geographical location, user identity, trust management and data privacy. It also arises in various procedures, including when the data are collected, transmitted and/or processed. The complexity of 5G networks, together with the multiple involved edge computing techniques, brings many privacy threats to the current 5G systems. Thus, protecting the privacy in 5G networks is not only an important topic, but also a difficult task.

Figure 9: Edge privacy solution overview for 5G

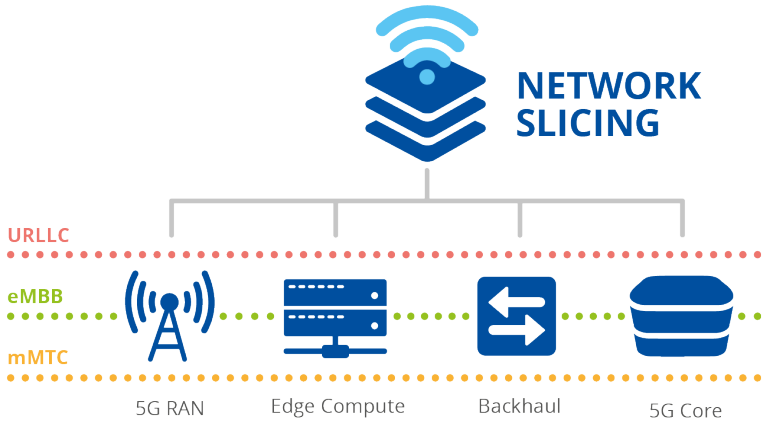


To ensure privacy in edge intelligence in 5G networks [103], several cryptographic techniques can be combined to enhance the privacy protection level. Encryption is the first level of data privacy. In the context of edge intelligence, lightweight encryption schemes are required. Differential privacy can be leveraged to make it possible to collect and share aggregated data while hiding the information of a specific person. For identity hiding, blockchain can be utilised with pseudonyms. In such systems, several privacy-enhancing signatures should also be considered, such as group signatures and ring signatures, where a group of users are chosen to hide the real participant.

6.2.2. Edge computing networking solutions for 5G

As mentioned above, by acting as an enabler close to the user, edge computing is also susceptible to network attacks; therefore, studies have focused on how to enhance security at network level. In [104], [105], authors explain in detail the different attack vectors and vulnerabilities of edge computing for tasks that require immediate action and enhance its security by using specialised and reliable local services for processing and storage capabilities for large data streams. In addition, in [105], the authors consider dependability, security and performance aspects in 5G MEC. These aspects are usually addressed individually, but they are not independent, and they can be conflicting (i.e. a solution for improving one aspect may impact the others – for instance, the usage of encryption to gain security causes a delay and therefore a decrease in performance). All potential conflicts described in [105] will need to be further investigated in the context of future 5G-MEC systems. Conventional gateways which allow IoT applications to run on the centralised cloud can be empowered with MEC-server functionalities [106], [107].

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

7. CONCLUSIONS

Having reached a good degree of cohesion and detail in this version of the report on fog and edge in 5G security, the next stage is to put these learnings/this research into practice at EU, Member State and fog and edge service provider level. By means of the identified recommendations, this objective can be achieved. It is important to use this material in various stakeholder activities, identify current and future developments and try to accommodate those in future versions of the present report. The report has covered a wide variety of application and service areas where fog and edge have emerged and has identified different security challenges in each one. The aim of the report was to summarise the broad field of telco communications in conjunction with the fog and edge paradigms, whose main attributes – i.e. heterogeneity and decentralisation – may offer innovative paths for application development in 5G, but also have generated various security challenges at the last-mile network infrastructure.

The report collects and analyses more than a hundred documents and outlines the main security aspects in the fog and edge domains. The main observations that can be derived from the analysis are the following.

- Fog and edge computing have room for improvement in terms of data security and privacy, and authentication mechanisms tailored to each one.
- Utilising existing and upcoming technologies can make an impact in terms of addressing the security challenges imposed by the paradigms.
- Fog and edge computing offer ample space for innovation, not only in the application field, but also from the security perspective, where different enablers can be leveraged to build trustworthy and robust telco environments.
- Heterogeneity is a key element in both paradigms, which by definition aim to combine cloud enablers with telco network infrastructure, with the goal to build an agile, robust and dynamic network environment for 5G communication providers.
- Existing knowledge bases on cybersecurity threats and IT security guidelines can be used for fog and edge native architectures and architectures relying on APIs. Although these families of software are well known to the IT industry, their use is quite recent and constitutes a driver of the ‘cloudification’ of the telecom sector.
- Fog and edge computing specifications and guidelines cover to a greater extent the ‘run’ phase of a technology lifecycle, whereas other phases would need tailoring.
- The available standards, specifications and guidelines are general. While they are not the primary focus of this report, they can be applied consistently to the fog and edge technical and functional domains and related lifecycle processes if they are tailored accordingly.
- Fog-specific standards, specifications and guidelines are available to a greater extent to the stakeholders from the Industrie 4.0 and IoT sectors. Whereas for edge computing, ETSI and 3GPP have defined several standard activities of the telecommunications sector.

Finally, this report stresses that, while significant progress has been made in both paradigms (fog and edge computing) there are several security-related issues and challenges that need addressing. Different sectors have provided different enablers to both paradigms, and innovation as a whole has benefited the overall network communications field significantly, mainly thanks to the integration of disruptive network management solutions, such as service orchestration, federation and elasticity, which have been applied to different security domains in the telco world. In addition, while the technical and organisational standards and specifications

analysed in the report can contribute to improving the security of fog and edge computing for 5G, they should not be treated as an exhaustive list of measures guaranteeing security. With the introduction of fog and edge computing for 5G, which widened the cybersecurity threat landscape, several risks have been introduced that are not covered by the solutions nor the existing standards. This vision should be future proof and should not depend on the variability of assets and configurations in the network.

8. REFERENCES

[1] L. Wang *et al.*, 'Cloud computing: A perspective study', *New Gener Comput*, vol. 28, no. 2, pp. 137–146, Apr. 2010, doi: 10.1007/S00354-008-0081-5.

[2] S. Kitanov, E. Monteiro, and T. Janevski, '5G and the Fog – Survey of related technologies and research directions', *Proceedings of the 18th Mediterranean Electrotechnical Conference: Intelligent and Efficient Technologies and Services for the Citizen, MELECON 2016*, Jun. 2016, doi: 10.1109/MELCON.2016.7495388.

[3] C. H. Hong and B. Varghese, 'Resource Management in Fog/Edge Computing', *ACM Computing Surveys (CSUR)*, vol. 52, no. 5, Sep. 2019, doi: 10.1145/3326066.

[4] H. F. Atlam, R. J. Walters, and G. B. Wills, 'Fog Computing and the Internet of Things: A Review', *Big Data and Cognitive Computing 2018, Vol. 2, Page 10*, vol. 2, no. 2, p. 10, Apr. 2018, doi: 10.3390/BDCC2020010.

[5] R. Chaudhary, N. Kumar, and S. Zeadally, 'Network Service Chaining in Fog and Cloud Computing for the 5G Environment: Data Management and Security Challenges', *IEEE Communications Magazine*, vol. 55, no. 11, pp. 114–122, Nov. 2017, doi: 10.1109/MCOM.2017.1700102.

[6] J. Gao *et al.*, 'A Blockchain-SDN-Enabled Internet of Vehicles Environment for Fog Computing and 5G Networks', *IEEE Internet Things J*, vol. 7, no. 5, pp. 4278–4291, May 2020, doi: 10.1109/JIOT.2019.2956241.

[7] H. Hawilo, A. Shami, M. Mirahmadi, and R. Asal, 'NFV: State of the art, challenges, and implementation in next generation mobile networks (vEPC)', *IEEE Netw*, vol. 28, no. 6, pp. 18–26, Nov. 2014, doi: 10.1109/MNET.2014.6963800.

[8] D. Kreutz *et al.*, 'Software-Defined Networking: A Comprehensive Survey'.

[9] P. Y. Zhang, M. C. Zhou, and G. Fortino, 'Security and trust issues in Fog computing: A survey', *Future Generation Computer Systems*, vol. 88, pp. 16–27, Nov. 2018, doi: 10.1016/J.FUTURE.2018.05.008.

[10] S. Rathore, J. H. Park, and H. Chang, 'Deep Learning and Blockchain-Empowered Security Framework for Intelligent 5G-Enabled IoT', *IEEE Access*, vol. 9, pp. 90075–90083, 2021, doi: 10.1109/ACCESS.2021.3077069.

[11] J. Mathew and R. J. Priyadarsini, 'Enhancing security in IoT healthcare services using fog computing', *International Journal of Advanced Science and Technology*, vol. 28, no. 17, pp. 444–450, 2019.

[12] L. F. Bittencourt, M. M. Lopes, I. Petri, and O. F. Rana, 'Towards Virtual Machine Migration in Fog Computing', in *2015 10th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC)*, Nov. 2015, pp. 1–8. doi: 10.1109/3PGCIC.2015.85.

[13] Z. Zhou, S. Yang, L. Pu, and S. Yu, 'CEFL: Online Admission Control, Data Scheduling, and Accuracy Tuning for Cost-Efficient Federated Learning across Edge Nodes', *IEEE*

Internet Things J, vol. 7, no. 10, pp. 9341–9356, Oct. 2020, doi: 10.1109/JIOT.2020.2984332.

[14] M. D. Ryan, 'Cloud computing security: The scientific challenge, and a survey of solutions', *Journal of Systems and Software*, vol. 86, no. 9, pp. 2263–2268, Sep. 2013, doi: 10.1016/j.jss.2012.12.025.

[15] S. Subashini and V. Kavitha, 'A survey on security issues in service delivery models of cloud computing', *Journal of Network and Computer Applications*, vol. 34, no. 1, pp. 1–11, Jan. 2011, doi: 10.1016/j.jnca.2010.07.006.

[16] A. Abbas and S. U. Khan, 'A review on the state-of-the-art privacy-preserving approaches in the e-Health clouds', *IEEE J Biomed Health Inform*, vol. 18, no. 4, pp. 1431–1441, 2014, doi: 10.1109/JBHI.2014.2300846.

[17] P. Ranaweera and A. Jurcut, 'MEC-enabled 5G Use Cases: A Survey on Security Vulnerabilities and Countermeasures', *ACM Comput. Surv*, vol. 54, no. 186, 2021, doi: 10.1145/3474552.

[18] S. Garg *et al.*, 'Edge Computing-Based Security Framework for Big Data Analytics in VANETs', *IEEE Netw*, vol. 33, no. 2, pp. 72–81, Mar. 2019, doi: 10.1109/MNET.2019.1800239.

[19] F. Zhou and R. Q. Hu, 'Computation Efficiency Maximization in Wireless-Powered Mobile Edge Computing Networks', *IEEE Trans Wirel Commun*, vol. 19, no. 5, pp. 3170–3184, May 2020, doi: 10.1109/TWC.2020.2970920.

[20] J. Pan and J. McElhannon, 'Future Edge Cloud and Edge Computing for Internet of Things Applications', *IEEE Internet Things J*, vol. 5, no. 1, pp. 439–449, Feb. 2018, doi: 10.1109/JIOT.2017.2767608.

[21] 'OpenFog Reference Architecture for Fog Computing', 2017. [Online]. Available: www.OpenFogConsortium.org

[22] 'International Electrotechnical Commission: IEC 62443-3-3:2013, Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels, 2013', Sep. 2016.

[23] R. Joshi, 'The Industrial Internet of Things Volume G5: Connectivity Framework', 2017.

[24] P. Industrie, 'IT Security in Industrie 4.0 Action fields for operators.' [Online]. Available: www.bmwi.de

[25] Internationale Elektrotechnische Kommission, *Industrial communication networks : network and system security. Pt. 1,1 Terminology, concepts and models*. IEC Central Office, 2009.

[26] 'Security and Privacy Controls for Information Systems and Organizations', Gaithersburg, MD, Sep. 2020. doi: 10.6028/NIST.SP.800-53r5.

[27] Iec, *Internet of things (IoT)-Edge computing INTERNATIONAL ELECTROTECHNICAL COMMISSION*.

[28] Mec, 'GS MEC 001 – V2.1.1 – Multi-access Edge Computing (MEC); Terminology', 2019. [Online]. Available: https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

[29] Mec, 'ETSI GS MEC 003 – V2.1.1 – Multi-access Edge Computing (MEC); Framework and Reference Architecture', 2019.

[30] '3GPP TR 33.839 Study on security aspects of enhancement of support for edge computing in the 5G Core (5GC).'

[31] '3GPP TR 23.758: 'Study on application architecture for enabling Edge Applications.'

[32] '3GPP TS 23.558: 'Architecture for enabling Edge Applications'.'

[33] A. Mijuskovic, A. Chiumento, R. Bemthuis, A. Aldea, and P. Havinga, 'Resource Management Techniques for Cloud/Fog and Edge Computing: An Evaluation Framework and Classification', *Sensors 2021, Vol. 21, Page 1832*, vol. 21, no. 5, p. 1832, Mar. 2021, doi: 10.3390/S21051832.

[34] R. Mahmud, R. Kotagiri, and R. Buyya, 'Fog Computing: A taxonomy, survey and future directions', *Internet of Things*, vol. 0, no. 9789811058608, pp. 103–130, 2018, doi: 10.1007/978-981-10-5861-5_5.

[35] F. Raviglione *et al.*, 'From collaborative awareness to collaborative information enhancement in vehicular networks ☆', *Vehicular Communications*, vol. 36, p. 100497, 2022, doi: 10.1016/j.vehcom.2022.100497.

[36] S. Shahzadi, M. Iqbal, T. Dagiuklas, and Z. U. Qayyum, 'Multi-access edge computing: open issues, challenges and future perspectives', *Journal of Cloud Computing*, vol. 6, no. 1, p. 30, Dec. 2017, doi: 10.1186/s13677-017-0097-9.

[37] A. MacDermott, P. Kendrick, I. Idowu, M. Ashall, and Q. Shi, 'Securing Things in the Healthcare Internet of Things', in *2019 Global IoT Summit (GIoTS)*, Jun. 2019, pp. 1–6. doi: 10.1109/GIOTS.2019.8766383.

[38] H. Rahimi, A. Zibaeenejad, P. Rajabzadeh, and A. A. Safavi, 'On the Security of the 5G-IoT Architecture', in *Proceedings of the international conference on smart cities and internet of things – SCIOT '18*, 2018, pp. 1–8. doi: 10.1145/3269961.3269968.

[39] S. Xu, Y. Qian, and R. Q. Hu, 'Privacy-Preserving Data Preprocessing for Fog Computing in 5G Network Security', in *2018 IEEE Global Communications Conference (GLOBECOM)*, Dec. 2018, pp. 1–6. doi: 10.1109/GLOCOM.2018.8647912.

[40] A. Dutta and E. Hammad, '5G Security Challenges and Opportunities: A System Approach', in *2020 IEEE 3rd 5G World Forum (5GWF)*, Sep. 2020, pp. 109–114. doi: 10.1109/5GWF49715.2020.9221122.

[41] F. Zhang and H. Chen, 'Security-Preserving Live Migration of Virtual Machines in the Cloud', *Journal of Network and Systems Management*, vol. 21, no. 4, pp. 562–587, Dec. 2013, doi: 10.1007/s10922-012-9253-1.

[42] P. Nowakowski, P. Żórawski, K. Cabaj, M. Gregorczyk, M. Purski, and W. Mazurczyk, 'Distributed Packet Inspection for Network Security Purposes in Software-Defined Networking Environments Network Function Virtualization, Software Defined Networks, Net-work Security, 5G System Architecture, Integrated Security Frame-work.'

[43] J. Huang, Y. Qian, and R. Q. Hu, 'Security Provision for Vehicular Fog Computing', in *2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring)*, May 2020, pp. 1–5. doi: 10.1109/VTC2020-Spring48590.2020.9129424.

[44] H. Sami, A. Mourad, H. Otrok, and J. Bentahar, 'FScaler: Automatic Resource Scaling of Containers in Fog Clusters Using Reinforcement Learning', in *2020 International Wireless Communications and Mobile Computing (IWCMC)*, Jun. 2020, pp. 1824–1829. doi: 10.1109/IWCMC48107.2020.9148401.

[45] H. Rahimi, A. Zibaeenejad, P. Rajabzadeh, and A. A. Safavi, 'On the security of the 5G-IoT architecture', *ACM International Conference Proceeding Series*, Sep. 2018, doi: 10.1145/3269961.3269968.

[46] S. Xu, Y. Qian, and R. Q. Hu, 'Privacy-Preserving Data Preprocessing for Fog Computing in 5G Network Security', *2018 IEEE Global Communications Conference, GLOBECOM 2018 – Proceedings*, 2018, doi: 10.1109/GLOCOM.2018.8647912.

[47] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, 'A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures', *IEEE Access*, vol. 7, pp. 82721–82743, 2019, doi: 10.1109/ACCESS.2019.2924045.

[48] R. Mahmud, R. Kotagiri, and R. Buyya, 'Fog Computing: A Taxonomy, Survey and Future Directions', 2018, pp. 103–130. doi: 10.1007/978-981-10-5861-5_5.

[49] A. Dutta and E. Hammad, '5G Security Challenges and Opportunities: A System Approach', *2020 IEEE 3rd 5G World Forum, 5GWF 2020 – Conference Proceedings*, pp. 109–114, Sep. 2020, doi: 10.1109/5GWF49715.2020.9221122.

[50] F. Zhang and H. Chen, 'Security-preserving live migration of virtual machines in the cloud', *Journal of Network and Systems Management*, vol. 21, no. 4, pp. 562–587, Dec. 2013, doi: 10.1007/S10922-012-9253-1.

[51] M. Liyanage *et al.*, 'Enhancing Security of Software Defined Mobile Networks', *IEEE Access*, vol. 5, pp. 9422–9438, 2017, doi: 10.1109/ACCESS.2017.2701416.

[52] F. Rossi, M. Nardelli, and V. Cardellini, 'Horizontal and vertical scaling of container-based applications using reinforcement learning', *IEEE International Conference on Cloud Computing, CLOUD*, vol. 2019-July, pp. 329–338, Jul. 2019, doi: 10.1109/CLOUD.2019.00061.

[53] M. C. Parker *et al.*, 'CHARISMA: Converged heterogeneous advanced 5G cloud-RAN architecture for intelligent and secure media access', *EUCNC 2016 – European Conference on Networks and Communications*, pp. 240–244, Sep. 2016, doi: 10.1109/EUCNC.2016.7561040.

[54] L. Xiao, X. Wan, C. Dai, X. Du, X. Chen, and M. Guizani, 'Security in Mobile Edge Caching with Reinforcement Learning', *IEEE Wirel Commun*, vol. 25, no. 3, pp. 116–122, Jun. 2018, doi: 10.1109/MWC.2018.1700291.

[55] Z. Mohammad, T. A. Qattam, and K. Saleh, 'Security weaknesses and attacks on the internet of things applications', *2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology, JEEIT 2019 – Proceedings*, pp. 431–436, 2019, doi: 10.1109/JEEIT.2019.8717411.

[56] J. Huang, Y. Qian, and R. Q. Hu, 'Security Provision for Vehicular Fog Computing', *IEEE Vehicular Technology Conference*, vol. 2020-May, May 2020, doi: 10.1109/VTC2020-SPRING48590.2020.9129424.

[57] H. Sami, A. Mourad, H. Otrok, and J. Bentahar, 'FScaler: Automatic Resource Scaling of Containers in Fog Clusters Using Reinforcement Learning', *2020 International Wireless Communications and Mobile Computing, IWCMC 2020*, pp. 1824–1829, Jun. 2020, doi: 10.1109/IWCMC48107.2020.9148401.

[58] A. A. A. EL-Latif, B. Abd-El-Atty, S. E. Venegas-Andraca, and W. Mazurczyk, 'Efficient quantum-based security protocols for information sharing and data protection in 5G networks', *Future Generation Computer Systems*, vol. 100, pp. 893–906, Nov. 2019, doi: 10.1016/J.FUTURE.2019.05.053.

[59] M. Ali *et al.*, 'SeDaSC: Secure Data Sharing in Clouds', *IEEE Syst J*, vol. 11, no. 2, pp. 395–404, Jun. 2017, doi: 10.1109/JSYST.2014.2379646.

[60] E. Markakis, Y. Nikoloudakis, E. Pallis, and M. Manso, 'Security Assessment as a Service Cross-Layered System for the Adoption of Digital, Personalised and Trusted Healthcare', *IEEE 5th World Forum on Internet of Things, WF-IoT 2019 – Conference Proceedings*, pp. 91–94, 2019, doi: 10.1109/WF-IoT.2019.8767249.

[61] P. Kamble and A. Gawade, 'Digitalization of Healthcare with IoT and Cryptographic Encryption against DOS Attacks', *Proceedings of the 4th International Conference on Contemporary Computing and Informatics, IC3I 2019*, pp. 69–73, 2019, doi: 10.1109/IC3I46837.2019.9055531.

[62] J. Ortiz *et al.*, 'INSPIRE-5Gplus: Intelligent security and pervasive trust for 5G and beyond networks', *ACM International Conference Proceeding Series*, Aug. 2020, doi: 10.1145/3407023.3409219.

[63] F. Pan, Y. Jiang, H. Wen, R. Liao, and A. Xu, 'Physical layer security assisted 5G network security', *IEEE Vehicular Technology Conference*, vol. 2017-September, pp. 1–5, Feb. 2018, doi: 10.1109/VTCFALL.2017.8288343.

[64] S. Nowaczewski and W. Mazurczyk, 'Securing Future Internet and 5G using Customer Edge Switching using DNSCrypt and DNSSEC', doi: 10.22667/JOWUA.2020.09.30.087.

[65] R. Pepito and A. Dutta, 'Open Source 5G Security Testbed for Edge Computing', *Proceedings – 2021 IEEE 4th 5G World Forum, 5GWF 2021*, pp. 388–393, 2021, doi: 10.1109/5GWF52925.2021.00075.

[66] Y. He, F. R. Yu, N. Zhao, and H. Yin, 'Secure Social Networks in 5G Systems with Mobile Edge Computing, Caching, and Device-to-Device Communications', *IEEE Wirel Commun*, vol. 25, no. 3, pp. 103–109, Jun. 2018, doi: 10.1109/MWC.2018.1700274.

[67] J. Zhang, H. Zhong, J. Cui, M. Tian, Y. Xu, and L. Liu, 'Edge Computing-Based Privacy-Preserving Authentication Framework and Protocol for 5G-Enabled Vehicular Networks', *IEEE Trans Veh Technol*, vol. 69, no. 7, pp. 7940–7954, Jul. 2020, doi: 10.1109/TVT.2020.2994144.

[68] X. Nie, L. T. Yang, J. Feng, and S. Zhang, 'Differentially Private Tensor Train Decomposition in Edge-Cloud Computing for SDN-Based Internet of Things', *IEEE Internet Things J*, vol. 7, no. 7, pp. 5695–5705, Jul. 2020, doi: 10.1109/JIOT.2019.2960293.

[69] B. Niu, W. You, H. Tang, and X. Wang, '5G network slice security trust degree calculation model', in *2017 3rd IEEE International Conference on Computer and Communications (ICCC)*, Dec. 2017, pp. 1150–1157. doi: 10.1109/CompComm.2017.8322724.

[70] Y. Liu, M. Peng, G. Shou, Y. Chen, and S. Chen, 'Toward Edge Intelligence: Multiaccess Edge Computing for 5G and Internet of Things', *IEEE Internet Things J*, vol. 7, no. 8, pp. 6722–6747, Aug. 2020, doi: 10.1109/JIOT.2020.3004500.

[71] F. Casino, T. K. Dasaklis, and C. Patsakis, 'A systematic literature review of blockchain-based applications: Current status, classification and open issues', *Telematics and Informatics*, vol. 36, pp. 55–81, Mar. 2019, doi: 10.1016/j.tele.2018.11.006.

[72] J. Pan and Z. Yang, 'Cybersecurity Challenges and Opportunities in the New 'Edge Computing + IoT' World', in *Proceedings of the 2018 ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization – SDN-NFV Sec'18*, 2018, vol. 2018-Janua, pp. 29–32. doi: 10.1145/3180465.3180470.

[73] A. Braeken, M. Liyanage, P. Kumar, and J. Murphy, 'Novel 5G Authentication Protocol to Improve the Resistance Against Active Attacks and Malicious Serving Networks', *IEEE Access*, vol. 7, pp. 64040–64052, 2019, doi: 10.1109/ACCESS.2019.2914941.

[74] B. Niu, W. You, H. Tang, and X. Wang, '5G network slice security trust degree calculation model', *2017 3rd IEEE International Conference on Computer and Communications, ICCC 2017*, vol. 2018-January, pp. 1150–1157, Mar. 2018, doi: 10.1109/COMPCOMM.2017.8322724.

[75] A. Mathew, 'Network Slicing in 5G and the Security Concerns', *Proceedings of the 4th International Conference on Computing Methodologies and Communication, ICCMC 2020*, pp. 75–78, Mar. 2020, doi: 10.1109/ICCMC48092.2020.ICCMC-00014.

[76] Y. Liu, M. Peng, G. Shou, Y. Chen, and S. Chen, 'Toward Edge Intelligence: Multiaccess Edge Computing for 5G and Internet of Things', *IEEE Internet Things J*, vol. 7, no. 8, pp. 6722–6747, Aug. 2020, doi: 10.1109/JIOT.2020.3004500.

[77] S. Lal, T. Taleb, and A. Dutta, 'NFV: Security Threats and Best Practices', *IEEE Communications Magazine*, vol. 55, no. 8, pp. 211–217, Aug. 2017, doi: 10.1109/MCOM.2017.1600899.

[78] T. Alharbi and M. Portmann, 'The (In)Security of Virtualization in Software Defined Networks', *IEEE Access*, vol. 7, pp. 66584–66594, 2019, doi: 10.1109/ACCESS.2019.2918101.

[79] H. Kim, P. Park, and J. Ryou, 'Auto-configurable Security Mechanism for NFV', *KSII Transactions on Internet and Information Systems*, vol. 12, p. 786+, 2018, [Online]. Available: https://link.gale.com/apps/doc/A533104111/AONE?u=anon~fe71aabb&sid=googleScholar&xid=7461146b

[80] F. Casino, T. K. Dasaklis, and C. Patsakis, 'A systematic literature review of blockchain-based applications: Current status, classification and open issues', *Telematics and Informatics*, vol. 36. Elsevier Ltd, pp. 55–81, Mar. 01, 2019. doi: 10.1016/j.tele.2018.11.006.

[81] I. H. Abdulqadder, D. Zou, I. T. Aziz, B. Yuan, and W. Dai, 'Deployment of robust security scheme in SDN based 5G network over NFV enabled cloud environment', *IEEE Trans*

Emerg Top Comput, vol. 9, no. 2, pp. 866–877, Apr. 2021, doi: 10.1109/TETC.2018.2879714.

[82] B. Chen *et al.*, 'A Security Awareness and Protection System for 5G Smart Healthcare Based on Zero-Trust Architecture', *IEEE Internet Things J*, vol. 8, no. 13, pp. 10248–10263, Jul. 2021, doi: 10.1109/JIOT.2020.3041042.

[83] G. H. S. Carvalho, I. Woungang, A. Anpalagan, and I. Traore, 'Optimal Security Risk Management Mechanism for the 5G Cloudified Infrastructure', *IEEE Transactions on Network and Service Management*, vol. 18, no. 2, pp. 1260–1274, Jun. 2021, doi: 10.1109/TNSM.2021.3057761.

[84] N. Gonzalez *et al.*, 'A quantitative analysis of current security concerns and solutions for cloud computing', *Journal of Cloud Computing*, vol. 1, no. 1, pp. 1–18, 2012, doi: 10.1186/2192-113X-1-11.

[85] R. Khan, P. Kumar, D. N. K. Jayakody, and M. Liyanage, 'A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements, and Future Directions', *IEEE Communications Surveys and Tutorials*, vol. 22, no. 1, pp. 196–248, Jan. 2020, doi: 10.1109/COMST.2019.2933899.

[86] Y. Nikoloudakis *et al.*, 'Towards a Machine Learning Based Situational Awareness Framework for Cybersecurity: An SDN Implementation', *Sensors 2021, Vol. 21, Page 4939*, vol. 21, no. 14, p. 4939, Jul. 2021, doi: 10.3390/S21144939.

[87] K. Karras *et al.*, 'A Hardware Acceleration Platform for AI-Based Inference at the Edge', *Circuits Syst Signal Process*, vol. 39, no. 2, pp. 1059–1070, Feb. 2020, doi: 10.1007/S00034-019-01226-7.

[88] Y. E. Gebremariam, D. G. Duguma, H. Y. Park, Y. N. Kim, B. Kim, and I. You, '5G and beyond telco cloud: Architecture and cybersecurity challenges', *World Automation Congress Proceedings*, vol. 2021-August, pp. 1–6, Aug. 2021, doi: 10.23919/WAC50355.2021.9559450.

[89] R. Vishwakarma and A. K. Jain, 'A honeypot with machine learning based detection framework for defending IoT based botnet DDoS attacks', in *Proceedings of the International Conference on Trends in Electronics and Informatics, ICOEI 2019*, Apr. 2019, pp. 1019–1024. doi: 10.1109/ICOEI.2019.8862720.

[90] D. Li, W. Peng, W. Deng, and F. Gai, 'A Blockchain-Based Authentication and Security Mechanism for IoT', in *2018 27th International Conference on Computer Communication and Networks (ICCCN)*, Feb. 2018, vol. 2018-July, pp. 1–6. doi: 10.1109/ICCCN.2018.8487449.

[91] H. Si, C. Sun, Y. Li, H. Qiao, and L. Shi, 'IoT information sharing security mechanism based on blockchain technology', *Future Generation Computer Systems*, vol. 101, pp. 1028–1040, Feb. 2019, doi: 10.1016/j.future.2019.07.036.

[92] O. Salman, I. H. Elhajj, A. Chehab, and A. Kayssi, 'A machine learning based framework for IoT device identification and abnormal traffic detection', *Transactions on Emerging Telecommunications Technologies*, Sep. 2019, doi: 10.1002/ett.3743.

[93] P. Krishnan, K. Jain, P. G. Jose, K. Achuthan, and R. Buyya, 'SDN Enabled QoE and Security Framework for Multimedia Applications in 5G Networks', *ACM Transactions on*

Multimedia Computing, Communications, and Applications (TOMM), vol. 17, no. 2, Apr. 2021, doi: 10.1145/3377390.

[94] B. Wen, Z. Luo, and Y. Wen, 'Evidence and Trust: IoT Collaborative Security Mechanism', in *2018 Eighth International Conference on Information Science and Technology (ICIST)*, Feb. 2018, pp. 98–99. doi: 10.1109/ICIST.2018.8426148.

[95] S. Rathore, J. H. Park, and H. Chang, 'Deep Learning and Blockchain-Empowered Security Framework for Intelligent 5G-Enabled IoT', *IEEE Access*, vol. 9, pp. 90075–90083, 2021, doi: 10.1109/ACCESS.2021.3077069.

[96] R. Khan, P. Kumar, D. N. K. Jayakody, and M. Liyanage, 'A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements, and Future Directions', *IEEE Communications Surveys and Tutorials*, vol. 22, no. 1, pp. 196–248, Jan. 2020, doi: 10.1109/COMST.2019.2933899.

[97] J. Xu, K. Ota, and M. Dong, 'Saving Energy on the Edge: In-Memory Caching for Multi-Tier Heterogeneous Networks', *IEEE Communications Magazine*, vol. 56, no. 5, pp. 102–107, May 2018, doi: 10.1109/MCOM.2018.1700909.

[98] M. Qin, L. Chen, N. Zhao, Y. Chen, F. R. Yu, and G. Wei, 'Computing and relaying: Utilizing mobile edge computing for P2P communications', *IEEE Trans Veh Technol*, vol. 69, no. 2, pp. 1582–1594, Feb. 2020, doi: 10.1109/TVT.2019.2956996.

[99] T. Tantidham and Y. N. Aung, 'Emergency Service for Smart Home System Using Ethereum Blockchain: System and Architecture', in *2019 IEEE International Conference on Pervasive Computing and Communications Workshops, PerCom Workshops 2019*, Mar. 2019, pp. 888–893. doi: 10.1109/PERCOMW.2019.8730816.

[100] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, 'Overview of 5G Security Challenges and Solutions', *IEEE Communications Standards Magazine*, vol. 2, no. 1, pp. 36–43, Mar. 2018, doi: 10.1109/MCOMSTD.2018.1700063.

[101] S. Rathore, J. H. Park, and H. Chang, 'Deep Learning and Blockchain-Empowered Security Framework for Intelligent 5G-Enabled IoT', *IEEE Access*, vol. 9, pp. 90075–90083, 2021, doi: 10.1109/ACCESS.2021.3077069.

[102] J. Ni, X. Lin, and X. S. Shen, 'Efficient and Secure Service-Oriented Authentication Supporting Network Slicing for 5G-Enabled IoT', *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 3, pp. 644–657, Mar. 2018, doi: 10.1109/JSAC.2018.2815418.

[103] Y. Li, Y. Yu, W. Susilo, Z. Hong, and M. Guizani, 'Security and Privacy for Edge Intelligence in 5G and Beyond Networks: Challenges and Solutions', *IEEE Wirel Commun*, vol. 28, no. 2, pp. 63–69, Apr. 2021, doi: 10.1109/MWC.001.2000318.

[104] P. Porambage, J. Okwuibe, M. Liyanage, M. Ylianttila, and T. Taleb, 'Survey on Multi-Access Edge Computing for Internet of Things Realization', *IEEE Communications Surveys and Tutorials*, vol. 20, no. 4. Institute of Electrical and Electronics Engineers Inc., pp. 2961–2991, Oct. 01, 2018. doi: 10.1109/COMST.2018.2849509.

[105] G. Nencioni, R. G. Garroppo, and R. F. Olimid, '5G Multi-access Edge Computing: Security, Dependability, and Performance', Jul. 2021.

[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

TP-04-22-338-EN-N

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14, Chalandri 15231, Attiki, Greece

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN 978-92-9204-610-15
doi:10.2824/24647