PRIVATEER

Privacy-first Security Enablers for 6G Networks

Deliverable 2.1

6G threat landscape and gap analysis

DRAFT – Pending approval by the Smart Networks and Services Joint Undertaking (SNS JU)

Co-funded by the European Union

6G SNS

PRIVATEER has received funding from the Smart Networks and Services Joint Undertaking (SNS JU) under the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101096110

Space Hellas SA, NCSR "Demokritos, Telefónica I&D, RHEA System SA, INESC TEC, Infili Technologies PC, Ubitech Ltd, Universidad Complutense de Madrid, Institute of Communication and Computer Systems, Forsvarets Forksninginstitutt, Iquadrat Informatica SL, Instituto Politecnico do Porto, ERTICO ITS Europe

PRIVATEER

Deliverable 2.1

6G threat landscape and gap analysis

Deliverable Type
Report

Month and Date of Delivery
March 31st 2023

Work Package
2

Leader
RHEA

Dissemination Level
Public

Authors
Fabrizio Scaglione (RHEA)
Cristian Petrollini (RHEA)
Francesco Manti (RHEA)

Programme	Contract Number	Duration	Starting Date
Horizon Europe	101096110	36 months	January 2023

Contact Us
privateer-contact@spacemaillist.eu

PRIVATEER has received funding from the Smart Networks and Services Joint Undertaking (SNS JU) under the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101096110

Contributors

Name	*Organization*
Lampros Argyriou, Dimitrios Giagkos, Antonia Karamatskou, Antonis Litke, Nikos Papadakis	INFILI
Antonio Pastor, Hugo Ramón	TID
Fábio Silva, Ricardo Santos	IPP
Georgios Gardikis	SPH
António Pinto, João Vilela	INESC TEC
Anastasios Bikos	IQU
Markus Leira Asprusten, Martin Strand, Gudmund Grov, Åvald Åslaugson Sommervoll	FFI
Manolis Katsaragakis, Dimosthenis Masouros , Dimitrios Soudris	ICCS
Ioannis Koufos, Maria Christopoulou, Stella Dimopoulou, George Xilouris	NCSRD
Anna Angelogianni, Thanassis Giannetsos	UBITECH
Jesús Alonso López, Antonio López Vivar, Elmira Saeedi Taleghani	UCM

Reviewers

Name	*Organization*
António Pinto, João Vilela	INESC TEC
Dimitris Santorinaios	NCSRD

Copyright and Disclaimer

Version History

Version	Date	Modifications
1	31/03/2023	First Version

List of Acronyms

Acronym	*Description*
3GPP	Third Generation Partnership Project
5GC	5G Core
5G-PPP	5G Public Private Partnership
ABAC	Attribute Based Access Control
ABE	Attribute Based Encryption
ACME	Automated Certificate Management Environment
AI	Artificial Intelligence
AMF	Access Management Function
AMF-UPF	Access Management Function (AMF) – User Plane Function (UPF)
API	Application Programming Interface
ASIC	Application Specific Integrated Circuits
AUC	Area Under Curve
AUSF	Authentication Server Function
BBU	Base Band Unit
BFT	Byzantine Fault Tolerant
B5G	Beyond 5G
CA	Certificate Authority
CapEx	Capital Expenditures
CAV	Connected Autonomous Vehicles
CFT	Crash Fault Tolerant protocol
CIV	Configuration Integrity Verification
CMPv2	Certificate Management Protocol version 2
CPU	Central Processing Unit
CSP	Cloud Service Provider
CTI	Cyber Threat Intelligence
CU	Central Unit
DAA	Direct Anonymous Attestation
DAM	Damage
DC	Data Center
DDoS	Distributed Denial-of-Service
DID	Decentralized Identifier
DIS	Disaster
DL	Distributed Ledger
DLT	Distributed Ledger Technology
DP	Differential Privacy
DP3T	Decentralized Privacy-Preserving Proximity Tracing
DRAM	Dynamic Random-Access Memory
DT	Decision Trees
DU	Distributed Unit

DWDM	Dense Wavelength Division Multiplexing
E2E	End-to-End
EC	European Commission
ECC	Error Correction Code
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
eIDAS	electronic IDentification Authentication and Signature
EIH	Eavesdropping/Interception/ Hijacking
EM	Electro-Magnetic
eMBB	Enhanced Mobile Broadband
ETSI	European Telecommunications Standards Institute
EU	European Union
FM	Failures or Malfunctions
FPGA	Field-Programmable Gate Array
GA	Grant Agreement
GAN	Generative Adversarial Neural Network
GDPR	General Data Protection Regulation
GMPLS	Generalized MPLS
gNB	gNodeB
GNNs	Graph Neural Networks
GPU	Graphics Processing Unit
HBO	Heap-based Optimizer
HPoHO	Hybrid Political optimizer together with a Heap-based Optimizer
HyDNT	Hybrid Neural Decision Tree
HW	Hardware
ICT	Information Comunication Technology
IMSI	International Mobile Subscriber Identity
IoE	Internet of Everything
IoT	Internet of Things
IRS	Intelligent Reflecting Surface
ISG ZSM	Industry Specification Group - Zero-touch network and Service Management
IT	Information Technology
KO	Kick Off (realted the tohe start of the PRIVATEER Project)
KPI	Key Performance Indicators
KVI	Key Value Item
LCM	Lifecycle Management
LDPC	Low-Density Parity-Check (LDPC)
LEG	Legal
LIME	Local Interpretable Model-agnostic Explanations
LIS	Large Intelligence Surface
LoA	Level of Assurance
M2M	Machine-to-machine

MAC	Medium Access Control
MANO	MANagement and Orchestration
MEC	Multi-access Edge Computing
MIMO	Multiple-Input Multiple-Output
MISP	Malware Information Sharing Platform
mMIMO	Massive Multiple-Input Multiple-Output
mMTC	Massive Machine-type Communication
ML	Machine Learning
MNO	Mobile Network Operators (MNO)
MPC	MultiParty Computation
MPLS	Multiprotocol Label Switching
MSP	Managed Services Providers
NAA	Nefarious Activity/Abuse
NATO	North Atlantic Treaty Organization,
NetApps	Network Applications
NG-eNBs	Next Generation Evolved NodeB
NG-RAN	Next Generation Radio Access Network
NIST	National Institute for Standards and Technology (USA)
NSA	National Security Agency (USA)
NSC	Network Slice Component
NSM	Network Slice Manager
NFV	Network Function Virtualization
NFVi	Network Functions Virtualization infrastructure
NMS	Network Management System
NOMA	Non-Orthogonal Multiple Access
NS	Network Services
NSMF	Network Slice Management Function
NTN	Non-Terrestrial Networks
NWDAF	Network Data Analytics Function
OFDMA	Orthogonal Frequency Division Multiple Access
OPoT	Ordered Proof of Transit
OS	Operating System
OUT	Outages
PA	Physical Attacks
PAaS	Privacy-As-a-Service
PET	Privacy Enhancing Technologies
PI	Privacy Index
PHY	Physical Layer
PKI	Public Key Infrastructure
PoC	Proof of Concept
PoT	Proofs-of-Transit
PTL	PRIVATEER Threat Landascape

PUF	Physical Unclonable Functions
QKD	Quantum Key Distribution
QoS	Quality of Service
RA	Remote Attestation
RAN	Radio Access Network
RASM	Remote Attestation Security Model
RAT	Radio access technology
R&D	Reasearch and Development
RLC	Radio Link Control RLC
RO	Ring Oscillator
RSA	Rivest-Shamir-Adleman cryptosystem
RU	Remote Unit
SBA	Service Based Architecture
SDN	Software-Defined Networking
SD-WAN	Software-Defined Wide Area Network
SHAP	SHapley Additive exPlanations
SLA	Service Level Agreement
SLO	Service Level Objective
SME	Small-Medium Enterprise
SOA	Service Oriented Architecture
SP	Service Providers
SSI	Self-sovereign identity
SW	Software
Tbps	Terabit per second
TEEs	Trusted Execution Environments
THz	Tera Hertz
TL	Threat Landscape
TLS	Transport Layer Security
TTP	Tactics, Techniques and Procedures
UAV	Unmanned Aerial Vehicle
UD	Unintentional Damage
UC	Use Case
UE	User Equipment
UICC	Universal Integrated Circuit Card
VC	Verifiable Credential
VIM	Virtualization Infrastructure Manager
VLC	Visible Light Communication
VM	Virtual Machine
VNF	Virtualize Network Function
VPN	Virtual Private Network
vRAN	Virtualized Radio Access Networks
WAN	Wide Area Network

WDM	Wavelength Divison Multiplexing
WIM	WAN Infrastructure Manager
XaaS	Everything as a Service
XAI	eXplainable Artificial Intelligence
ZTM	Zero Touch Management

Executive Summary

This is the first deliverable of Work Package 2 (WP2), “PRIVATEER framework design, integration and evaluation”, denoted D2.1 “6G threat landscape and gap analysis”.
The main objective of the WP2 includes all the system engineering activities for the PRIVATEER framework, namely requirements management, design and specification, integration and verification via use case scenarios.
More specifically, the main objectives addressed in this document include a comprehensive identification of the threat landscape in 6G, with a specific focus on new/evolved threats through an extensive literature review with a drill down on the identifiable risk factors that contribute to privacy leakage of end users, service providers and infrastructure providers. Furthermore, identifying gaps related to 6G candidate technologies and also proposing specific security and privacy related 6G Key Performance Indicators (KPIs) and Key Value Indicators (KVIs).
In 2030, society is expected to have evolved around increasingly advanced technologies, where networks act as the communication and information backbone, allowing communication to take place anywhere and at any time.
New radio, access and transport technologies will give a 3D connection to everyone and everything with an incredible bandwidth and low latency, a cloud-continuum or a “service everywhere” will bring the services so close to the consumer to have a new “human-and-machine-centric” paradigm where the 6G network will be the fundamental enabler.

These technologies are expected to give the opportunity for a completely new set and families of use cases like E-health, immersive smart city, Interconnected vehicles, Unmanned Aerial Vehicles (UAVs), cooperating mobile robots, etc., just to name a few, and so, billions of things, humans, and connected vehicles, robots and drones will generate Zettabytes of digital information.
From the current researches and studies all agree unanimously the Artificial Intelligence (AI) and Machine Learning (ML) will be used pervasively across 6G security architecture, process and technology domains to automate and support the 6G network for a flexible, dynamic configuration and orchestration, as well as the real business enabler
AI/ML is a multifaced actor in this 6G playground because it is expected to be exploited in many different ways: (i) in the physical, network and service layers for the management and to enhance the security of the 6G network to bear the new envisioned use case scenarios; (ii) as a new attack “surface” for cyber threats; (iii) as a technology used as an attack vector to implement new kind of attacks.
AI is envisaged to assume the governance of the network, automating its design, orchestration and operation with the goal of achieving a "Zero Touch" infrastructure.
In addition, the capacity of 6G networks to handle computationally intensive applications like ML will promote the implementation of programmable hardware platforms such as Field Programmable Gate Arrays (FPGAs) and Graphics Processing Units (GPUs).

Blockchain with its concept of decentralised transactions will be also a core building block for 6G networks, enabling intelligent resource management, spectrum sharing, as well as scalability and availability. Blockchain is considered a promising technology for advanced protection in terms of security and privacy, nevertheless there is a trade-off between security and efficiency in terms of reliability and coverage and many research are conducted to discover the effects between security, privacy, performance and sustainability.
The new 6G technological dimension will be deployed according to the "Ubiquitous Computing" paradigm, which extends the concept of Edge Computing by distributing network functions, processing capabilities, content and applications to the edge of the network. Moreover, it is expected to have a further improvement of the network slicing techniques already used in 5G networks, by deploying emerging technologies such as Virtualized Radio Access Networks (vRAN) and Open RAN to reach more precise security attestation running on commodity servers.
Network Function Virtualization (NFV) has been deployed in 5G networks, and it is expected to be implemented in 6G by virtualizing network functions that were previously run on dedicated hardware. On the other hand, Software-Defined Wide Area Network (SD-WAN) is a cloud native approach to WAN connectivity with the objective to simplify network management and operations.
Another important evolution regards the spectrum management. Along with the reuse of the bands already currently adopted for mobile services, the massive exploitation of high frequencies bands in the THz ranges will also be the core of 6G communications. For what concerns transmission technologies, 6G is expected to be a shift toward ultra-massive MIMO antenna systems and capable of exploiting Intelligent Reflecting Surfaces (IRS) and Large Intelligent Surfaces (LIS).
The development of quantum communication and computing has been a topic of extensive research over the past few decades and has led to the creation of various quantum technologies such as quantum key distribution, quantum teleportation, and quantum error correction. These technologies have the potential to revolutionize communication and information processing and could significantly impact fields such as cryptography as well as communication. However, the implementation of quantum technologies within the 6G scope is expected to be more complex, but cannot be ignored.
Moreover, one of the other challenges of a 6G network will be also to address at least some of the currently know security threats from the 5G and the older networks that still coexists and will continue to coexist for years to come.

With the respect to the security and privacy aspects of this enormous amount of data and technology shift, it is inevitable to foresee an increased attack surface and a higher attacker appetite compared to 5G network, so it is paramount to design all the technology enablers with a “security-by-design” and “privacy-first” approach.

Due to the central role of 6G network in the future society its classification as critical infrastructure will become much more “critical”, for this reason and also considering the new geo-political situation after the start of the Ukraine-Russia conflict, much

more attention and consideration take the State-sponsored, Cybercriminals, Hacktivists actors in the playground.
It is also expected that the attacks will also evolve exploiting the AI/ML technologies giving to the attacker, amongst many, the capability to analyse huge amount of data to infer information.

From this 6G TL analysis, it is clear that privacy preservation deserves dedicated attention to assure that society realizes the full value of 6G technologies.
Many privacy concerns related to the physical, connection and service layers of the 6G networks have been identified and need to be adequately addressed. For the physical layer point-of-view the main concern is related to location exposure and position tracking. Regarding the connection and service layers the main highlighted privacy concerns are related to the balance between the needs of user data sharing and processing for: a) the purpose of the flexible and dynamical 6G network configuration and orchestration to be able to provide the best experience to the user, b) for the business case itself, c) for security and auditing reasons (e.g. security data analytics, CTI sharing), and the utmost need of avoiding to make these private data directly available to non-authorized actors either to be inferenced by any means. Overcoming these challenges requires that new approaches and technologies have to be put in place. Privacy Enhancing Technologies (PETs) is the recently coined term to group the novel techniques for addressing the privacy concerns that cannot be successfully or comprehensively managed by the classical privacy techniques; just to name some of main foreseen in the 6G ecosystem: differential privacy, homomorphic encryption, secure multi-party computation and Confidential Computing.

At the current stage of the 6G definition, analysing many sources to prepare this TL, different privacy concerns have been identified and described. Many different studies, analysis and proposed solutions are still in progress with the aim to find the best approach to solve/mitigate the threat.
One of the challenges related to the Privacy aspects faced during the production of this document, was made up in the complexity to establish KVIs and KPIs as a new approach to adopt a 6G network “privacy-first” design paradigm based on performance- and value-oriented objectively measurable indicators.
Some relevant Privacy and Security KVI and KPIs proposed in this paper, can be used as reference for the design phase, measured during their initial development phases along with all the development lifecycles and can serve as the base for the overall 6G network healthiness operation.

Table of Contents

Index of Figures

Index of Tables

1 Introduction

This deliverable represents the outcome of a first analysis to identify the main foreseeable Security and Privacy threats related to the envisioned 6G Network and candidate 6G enabling technologies, as current studies and researches forecast to be fully/partially operational by 2030.

The biggest challenge regarding the 6G PRIVATEER TL is the fact that architecture and related key technologies are not yet defined. Moreover there are neither historical data about security weaknesses nor incidents and threat actors for 6G. Due to the forementioned, the 6G Threat Landscape analysis follows a structured methodology which is described in chapter 2, and examines existing materials (Studies from academies, EU projects, vendors, Communication consortiums, experts, white papers, threat analysis on previous xG networks, etc.) to have a solid initial starting point, delving deeper and eventually formulating some assumptions.

At the time of writing this document all the threats exposure of the 5G network are far from being completely known and some references used to prepare this report are considered as 'work in progress' by the authors (from different entities, organizations, institutions, regulators, etc.). It is worth noting that this initial TL has the aim to give a high-level understanding of the potential relevant cyberthreats within the 6G ecosystem but it needs to be extended and updated to be more detailed while the envisioned 6G network architecture and core components are being developed.

The analysis begins by defining the possible main stakeholders and end-users of the 6G ecosystem in Section 3.1, as well as the new use cases by which the 6G will be fully exploited. From this point of view, the analysis is focused on defining the main threats and threat actors interested in exploiting possible vulnerabilities for different types of attacks, respectively chapter 3.2 and 3.3. Then, after a decomposition in domains (chapter 3.4), the deliverable focuses on the envisioned key technologies that could be the building blocks of a new candidate 6G network and for each of them an analysis is presented that showcases the technological benefits, as well as possible security and privacy related concerns, thoroughly presented in chapter 4. Notably, a specific chapter has been created on the privacy topic, for the further analysis of concerns and possible technological approaches that could be implemented in the 6G definition and design stage for preserving the stakeholders' privacy. Chapter 6 has been thoroughly analysed to bridge the gap between the currently envisioned 6G Network and the 5G Network in terms of existing or future countermeasures to mitigate potential threats. Chapter 7 outlines the Use Case Scenarios that will be employed as part of the PRIVATEER project to evaluate the

privacy framework which will be developed as fundamental components for a "privacy-by-design" architecture.

Towards the end of this document, specifically in Chapter 8, potential KPIs and KVIs are suggested as a foundational measure of security and privacy for 6G.

2 Methodology

The methodology adopted for this PRIVATEER Threat Landscape (PTL) deliverable is a tailored process derived from the "ENISA CYBERSECURITY THREAT LANDSCAPE METHODOLOGY" [1]. It comprises 5 steps, namely direction, collection, processing, analysis & production, and consuming, as following described:

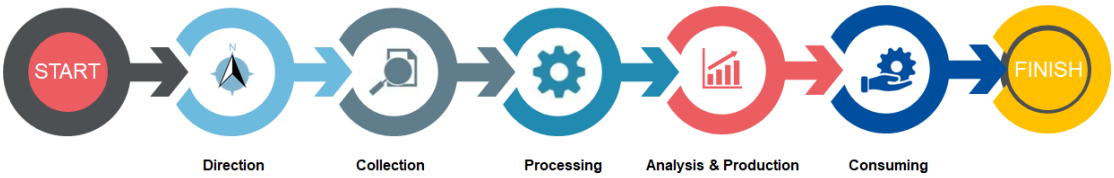

Figure 1 TL Methodology flow

2.1 Direction

One of the first steps to implement a Threat Landscape (TL) is to define:

- the purpose
- the TL "consumers"
- the requirements

A key purpose of this report is to identify the most critical components (assets) in a candidate 6G Network Architecture, and identify assets which may become a target to various new or not yet mitigated cybersecurity threats, with a special focus to the ones that address the privacy related aspects.

PRIVATEER TL main goal is to answer the following questions:

- Which 6g technologies are in scope and affected?
- Which are the main stakeholders?
- Who is the threat actor and what is its main motivation?
    - (possibly) What are the used Tactics, Techniques and Procedures (TTP)?
- What are the main threats?
    - What is the impact of the incidents?
    - What are the privacy-related specific threats?
        - What countermeasures can be applied?

in order to deliver actionable intelligence to the next phases of the PRIVATEER project.

2.2 Collection

The collection step has the main objective of information gathering. The information is selected and organized in the next steps, later transformed into actionable intelligence. Information is collected from different data sources (publicly available reports, subscription services, information shared by many different vendors, public feeds, etc.).

A collection requirement has been established as following described:

Table 1. TL Methodology: Collection requirements

Intelligence Requirement	Collection Requirement
What are the foreseeable threats in 6G ecosystem?	• Consult papers about the current and future trends for cybersecurity threats • Consult papers about current (5G) and future 6G ecosystem in terms of - Stakeholders - Users and use cases - Key enabling technologies
Timeframe for collecting data	Kick Off (KO) + 1 month
Type of data	• Publicly available Academic Research • Publicly available Research Studies • White Papers • Public studies from technology vendors • Public deliverables from projects • Public studies and TL about cybersecurity • EU regulations

During the Collection phase, all the documents are stored in a shared repository and classified to be properly used in the Processing step. The main attributes defined are:

- Original name of the document
- File name in the shared storage
- Publication date
- Collection date
- Type of document
    - White paper
    - Academic research paper
    - Institutional paper (Regulation, Trend Analysis, Threat Landscape, Taxonomy, etc.)
    - Vendor technical analysis
    - Project deliverable

- Topic of interest:
  - 5G/6G Technology related
  - Cybersecurity threats
  - Privacy aspects
  - Multiple aspects

At the end of the collection and classification steps, it is then possible to proceed with the Processing step.

2.3 Processing

The data processing aims at converting acquired raw data of different types, format, trust level and granularity, in a format that the experts can better utilize for their analysis and for the output of intelligence in the next step.

The two main activities performed in this phase are as follows. The first activity is to understand the credibility and trustworthiness of the information collected, through a process of cross-checking the extracted information with other papers/information from other sources. The second activity is to validate this information in terms of meaningfulness for the scope of the TL, which means that if a source of information is considered useful and in scope to build the TL, it is marked accordingly for further fruition in the next step, otherwise, it is marked as discarded in the classification document.

At the end of the data processing step, all the useful insights which will be further analysed for the purpose of the TL production, are identified and highlighted.

2.4 Analysis & Production

During this step, the team aims to answer all the questions that have been raised in the collection phase. Additionally, the team shall identify gaps that could potentially be used for creating recommendations, based on past knowledge (if any) and other sources. In this step, the team conducts expert analysis to provide meaningful conclusions based on the collected information. Based on these conclusions, considering the entire threat landscape, including cybersecurity policies, market standardisation and certification efforts, capacity building exercises and trainings and operational cooperation, actionable recommendations as well as cybersecurity measures will be produced.

2.5 Consuming

The Consuming step is the one where the actionable intelligence, output of the GAP analysis on the depicted 6G TL, will feed the subsequent process of Use Case Scenario elicitation in order to address the privacy-related threats.

3 Threat Landscape Overview

In order to be able to draw a contextualized Threat Landscape, the first activity is to appropriately define the boundaries in terms of:

- **Stakeholders**: customers, but also the ones with roles in the deployment, operation and supervision of the 5G infrastructure, because they constitute an essential part of the 6G ecosystem and are also the ones responsible for mitigating the identified threats, by introducing specific countermeasures that reduce risk.
- **Threat Actors**: providing information on threat agents assessing the potential motives emerging from the abuse/misuse of 6G assets/technologies.
- **Main Threats**: using a taxonomy-based approach to the main threats to which the 6G ecosystem could be exposed to.
- **Specific Domain**: 6G ecosystem represented by its logical domains.

In Chapter 4, having in mind both the TL boundaries and the taxonomy described in Section 3.3, for each of the main key enabling technologies, foreseen in the 6G ecosystem, will be analysed in regard to its technical features, as well as, to the envisioned threats and possible countermeasures.

3.1 Stakeholders

3.1.1 End Users/Service Customers

This group includes not only the individuals who will be using 6G devices and services for private use, but also the enterprise users/vertical industries who take benefit of 6G advances to fulfil their operational requirements. Various industries, including healthcare, transportation, and entertainment, are expected to be transformed by 6G technology, making them stakeholders in its development and deployment. In principle, in the end users' domain, the PRIVATEER developments are primarily addressed to enterprise customers, since they address more specific needs - and their application requires some technical background on the user's side. Users and Service consumers absolutely require the security and privacy of their personal -or corporate- data. They also expect secure access to 6G services and protection against malware and other security threats. Nonetheless, not all users have the same needs; different industries have unique security requirements for their use of 6G networks, such as secure connectivity for industrial control systems in the energy sector, or privacy and security for sensitive medical data in healthcare.

3.1.2 Infrastructure Providers/Neutral hosts

5G and, even more, 6G, departs from the traditional service delivery model where the Mobile Network Operators (MNO)/Service Providers (SP) own the full end-to-end infrastructure and promote the model of infrastructure leasing and sharing. This also embraces the 5G/6G neutral host business model, which enables shared access to 5G/6G infrastructure for multiple SPs/MNOs. Under this model, a neutral host operator, such as a datacenter provider, a tower company, or a real estate developer, builds and operates 6G infrastructure, such as small cells and other network components. Multiple SPs/MNOs can then use this infrastructure to provide 6G services to their customers, eliminating the need for each SP to build its own infrastructure for the same coverage area. The main benefits of the 6G neutral host model include reduced costs for SPs, increased network coverage and capacity, and faster deployment of 6G networks. Additionally, it enables more efficient use of spectrum and other resources, and can facilitate innovation and competition in the 6G market. However, the neutral host model also presents challenges, such as the need to ensure network interoperability, security, and reliability, as well as the need to resolve any disputes between SPs over access to the shared infrastructure. Neutral host privacy is an important factor in the sense that operational data that is exposed to tenant MNOs must be controlled. PRIVATEER will allow infrastructure providers / neutral hosts to securely share their infrastructure with multiple tenant SPs, while their privacy is preserved.

3.1.3 Service Providers

This group includes the MNOs, which provide the 6G service (connectivity & NetApps, as a network slice) to customers. As part of their regulatory compliance and contractual obligations, service providers must ensure the confidentiality, integrity, and availability of services, as well as the protection of customer data and privacy. They must also implement measures to prevent unauthorized access to their networks and secure the supply chain of network components and services. At the same time, they cater for the privacy of their own corporate data, on the grounds of commercial confidence and safeguarding their market reputation. PRIVATEER provides a solution which addresses "360-degree privacy", i.e. enabling SPs to secure their services respecting their (enterprise) customers' privacy, as well as their own.

3.1.4 Other stakeholders

In addition to the three groups mentioned above, which deserve particular attention in this document since they are directly engaged in the operations of the PRIVATEER security framework, security and privacy aspects in 6G concerns also other stakeholders, such as:

Vendors: Companies that manufacture 6G-compatible devices, such as smartphones, tablets, and other mobile devices. Vendors must ensure the security and privacy of the 6G components and systems they produce, as well as secure the supply chain of these products. For vendors, PRIVATEER offers an affordable and efficient open-source additional layer of security for their 6G equipment.

NetApp developers: They develop network applications (NetApps) to be deployed as part of a customer service/slice within the 6G compute continuum. The security of NetApps is an essential element of the security of the overall 6G service. Before deployment, proper certification and security auditing processes are essential. After deployment, the security enablers offered by PRIVATEER can be engaged to verify integrity and proper operation.

Governmental/regulatory agencies and standardisation organisations: They are responsible for developing and enforcing 6G standards and regulations, which need to embrace security controls. Additionally, government agencies have a responsibility to ensure that 6G networks are secure and comply with national security and privacy laws. They may also have specific security requirements for critical infrastructure and emergency services that use 6G networks. Mechanisms such the ones proposed by PRIVATEER can be mandated as part of the service delivery chain to mitigate security and privacy issues.

3.2 Threat Actors

Threat Landscape motivation. To better illuminate the effect of cyberthreats against 6G networks, it is crucial to assess the most critical assets that may be compromised by malicious threat actors, as well as the security threat exposure of these assets.

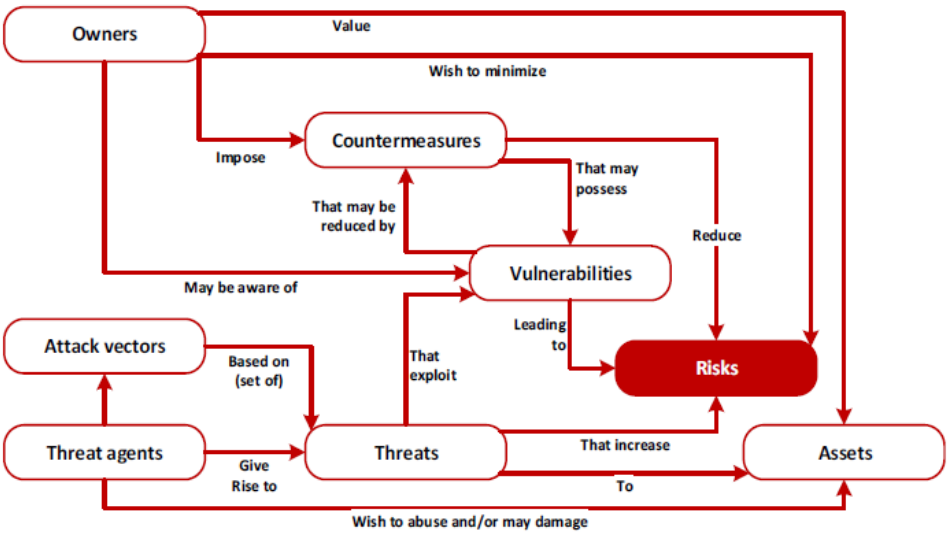

Figure 2 Methodology based on ISO 27005 [106]

Threats play an essential role in risk assessment, especially when considering the versatile components of risks. The object target category of such risk vectors are the vital security assets that belong to companies, corporations, and individuals, whereas the subjects or risk-threat initiators are technically (human) *threat agents.*

For as long as the next generation of Cellular Networks (5G/6G & beyond) keeps evolving, it is highly expected that current threat actors' profiles will incorporate novel and more dangerously sophisticated attack profiles. This is mainly due to the vastly interconnectivity nature of the upcoming 6G network deployments, where the Internet-of-Everything (IoE) and massive Machine-2-Machine (M2M) types of communications are going to become of paramount importance and presence. Due, also, to the business-driven type of 6G applications deployment, added-valued critical services, functions and slices will inevitably become an easier target for security threat compromising different parties.

To more efficiently brainstorm the security threat landscape for the next generation mobile networks, it is needed to dive deep into the attacker's motivations, goals, and psychology (i.e., how they think). Given such challenges, the following facts should be taken into consideration:

- The security attack and corresponding surface are expected to grow bigger, more intelligent, and highly scalable as per the amount of critical infrastructure.
- New advanced tools and exploitable techniques will be developed (e.g., Artificial Intelligence driven security attacks).
- The more interconnected verticals and industries, and/or business models become, the larger will the targeted and observed threat landscape grow.
- Persistent threat groups will be expanded or combined with other ones to initiate more aggregated and massive attacks.

Due to the degree of severity from the advancement of attack actors' intelligence, the cybersecurity theoretical comprehension, mitigations and solutions need to be extrapolated.

ENISA ELT2018 [2] groups threat agents as follows:

- Cyber criminals
- Insider (own, third parties)
- Nation states
- Hacktivists
- Cyber-fighters
- Cyber-terrorists
- Corporations

- Script kiddies

Another more dangerous trait of malicious actors occurs when the threat agent has legitimate access to the business network. By acknowledging such intruders as legitimate internal or external authorities into the corporate networks, their attacking capabilities become even more facilitated.

Table 2, extracted from ENISA Threat Landscape for 5G [4] maps the involvement of threat actors to specific threats.

Table 2. ENISA TL 5G Threat Actors vs Threats

	Cyber-criminals	Insiders	Nation states	Cyber-warriors	Hacktivists	Corporations	Cyber-terrorists	Script-kiddies
Nefarious activity/ Abuse	✓	✓	✓	✓	✓	✓	✓	✓
Eavesdropping/ Interception/Hijacking	✓	✓	✓	✓	✓	✓	✓	✓
Disasters			✓	✓			✓	
Unintentional Damage	✓	✓	✓	✓				✓
Outages	✓	✓	✓	✓	✓			
Failures/Malfunctions	✓	✓	✓	✓	✓	✓	✓	✓
Legal	✓	✓	✓	✓	✓	✓	✓	
Physical attacks	✓	✓	✓	✓	✓	✓	✓	

Legend:

Primary group for threat: ✓

Secondary group for threat: ✓

During the ENISA Threat Landscape 2022 Report [3] (ETL2022), the identified preliminary 5G/6G threats include:

- Ransomware
- Malware
- Social Engineering threats
- Threats against data
- Threats against availability: Denial of Service
- Threats against availability: Internet threats
- Disinformation – misinformation
- Supply-chain attacks

We need to amplify the fact that based also on the presence of the previous threat actors, there has been a serious impact of geopolitics on the cybersecurity threat

landscape. For instance, the conflict between Russia-Ukraine reshaped the threat landscape in terms of increased hacktivist activity. *Geopolitics* have a strong impact on cyber operations, as well as *misinformation* (i.e., fake news and deep-faking which pose a serious privacy threat - AI-enabled disinformation and deepfakes). Furthermore, threat actors tend to be increasing their capabilities. For example, more resourceful threat actors have utilised *0-day exploits* to achieve their strategic cybersecurity aims. Continuous 'retirements' and the *rebranding*, or re-enabling of ransomware groups is being used to deceive law enforcement and avoid sanctions. A new upcoming trend of *hacker-as-a-service* business model, especially since 2021, has gained relevancy. Criminal hacker groups have a special tendency to target supply chain and attack Managed Services Providers (MSPs).

Finally, data compromises are rising every year with huge data privacy breaches. Also, ML models are at the core of modern distributed systems and are becoming the target of attacks. Person proliferation and *identity theft* create new cybersecurity havocs in terms of privacy.

Conclusively, as per the purposes of the ETL2022, the following four categories of cybersecurity threat actors are considered again as moderate to critical:

- State-sponsored actors
- Cybercrime actors
- Hacker-for-hire actors
- Hacktivists

3.3 Threats

At the date of this analysis for the 6G PRIVATEER TL, all the advantages from 5G innovations are far to be fully exploited and even less all the risks and threats are not thoroughly identified and depicted. The following sections summarize the main IT and 5G specific threats identified in the ENISA TL for 5G.

3.3.1 Taxonomy of Threats

The following list presents a high-level categorization of threats, based on the ENISA threat taxonomy [5]:

- Nefarious Activity/Abuse (NAA) - This threat category is defined as “intended actions that target ICT systems, infrastructure, and networks by means of malicious acts with the aim to either steal, alter, or destroy a specified target”;

- Eavesdropping/Interception/Hijacking (EIH) - This threat category is defined as “actions aiming to listen, interrupt, or seize control of a third-party communication without consent”;

- Physical Attacks (PA) - This threat category is defined as “actions which aim to destroy, expose, alter, disable, steal or gain unauthorized access to physical assets such as infrastructure, hardware, or interconnection”;

- Damage (DAM) - This threat category is defined as intentional actions aimed at causing “destruction, harm, or injury of property or persons and results in a failure or reduction in usefulness”;

- Unintentional Damage (UD) - This threat category is defined as unintentional actions aimed at causing “destruction, harm, or injury of property or persons and results in a failure or reduction in usefulness”;

- Failures or Malfunctions (FM) - This threat category is defined as “Partial or full insufficient functioning of an asset (hardware or software)”;

- Outages (OUT) - This threat category is defined as “unexpected disruptions of service or decrease in quality falling below a required level";

- Disaster (DIS) - This threat category is defined as “a sudden accident or a natural catastrophe that causes great damage or loss of life”;

- Legal (LEG) - This threat category is defined as “legal actions of third parties (contracting or otherwise), in order to prohibit actions or compensate for loss based on applicable law”.

3.3.2 Threats from 5G Threat Landscape

In order to better depict what is the foreseeable TL for the 6G technology, it is important to understand, at least, which are the remaining risks of the 5G networks. 5G networks are the ones supposed to be in place at the date the new 6G will start its deployment.

For this reason, in ANNEX A has been attached the ENISA 5G TL table where the above listed main threat types are granularly decomposed in more specific threats and mapped to the affected IT and 5G assets, complemented with their potential impact.

3.4 6G Domains

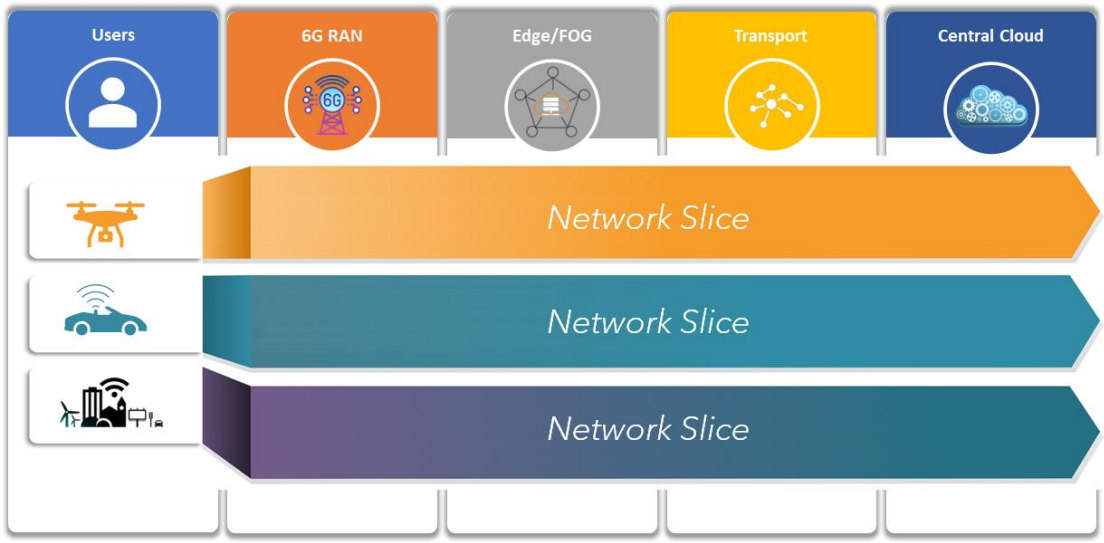

Figure 3. 6G Domains

In this section, we describe the 6G ecosystem, as organized by its logical domains, so as to assess the security and privacy requirements and implications in the respective domains.

3.4.1 User

The development of 6G technology is expected to revolutionise the world as we know it today. The envisaged capabilities of 6G could enable a myriad of possible novel applications and use cases on which the different users and stakeholders will be involved at different levels, as well as, will also be exposed to new threats to their privacy. The possible use cases that can involve all the users and stakeholders are, among many others, UAV-based mobility, extended reality, Connected Autonomous Vehicles (CAV), and digital twins.

The implementation of the 6G technologies requires the collaboration of several stakeholders, including state governments, international organisations, infrastructure providers, service providers, and end-users. Each stakeholder plays a critical role in making 6G a reality, and their collective efforts will determine the success of this ground-breaking technology.

State governments are seen as major drivers in the implementation of 6G R&D, as they have the financial and political power to support the necessary infrastructure and provide the necessary legislation to ensure the ethical use of this technology. Additionally, state governments can view 6G technology as a strategic resource from a geopolitical perspective. International organisations such as the United Nations can also use 6G to achieve sustainable development goals, while the European Union coordinates efforts to ensure independent production of all necessary 6G

components in Europe, increasing resilience to commercial crises with external actors.

Infrastructure providers such as Ministries, Local Authorities, and public-private partnerships play an essential role in the deployment of 6G as they are responsible for building and maintaining the infrastructure, including data centres and highways, which are essential components of the 6G ecosystem. In this context, smart cities will play a crucial role in ensuring the effective deployment of 6G technology.

Service providers, including large tech companies, SMEs, and start-ups, will be responsible for developing and deploying new applications and services built on 6G. It's important to note that the unpredictability of future developments in 6G technology is high, and new business models may emerge that cannot yet be anticipated.

Vertical markets are commercial niches where providers cater to a particular target group, and 6G will be instrumental in providing tailored services for these markets. Lastly, consumers are also essential stakeholders in the 6G ecosystem and their opinion might affect the adoption of the 6G technology, as they become increasingly conscious of the sustainability and energy consumption aspects, a challenge that is vital to be addressed.

3.4.2 6G RAN

The RAN (Radio Access Network) domain is a crucial component of modern cellular networks, including 5G, B5G and upcoming 6G networks. It is responsible for the wireless transmission and reception of data between user devices and the core network. The RAN domain in 6G will play an even more important role due to the higher bandwidth and lower latency requirements of 6G applications such as virtual and augmented reality, holographic communications, and tactile Internet. The 6G RAN will need to support massive connectivity, ultra-reliable and low-latency communications, and provide ubiquitous coverage in both indoor and outdoor environments. As a result, 6G RAN will need to incorporate advanced technologies such as terahertz and visible light communications, massive MIMO (Multiple-Input Multiple-Output), AI-driven dynamic spectrum management, and network slicing to meet the demanding requirements of future 6G applications.

RAN components are divided into two different units: (I) Base Band Unit (BBU) which runs as a software and (ii) Remote Radio Head which is deployed in the field [163]. In 5G and B5G networks the functionality of the BBU can be implemented as a set of VNFs in order to provide a more flexible deployment. In detail, the VNF decomposition of the BBU enables the usage of the Central Unit (CU) which is responsible for handling host time-tolerant functions of the RAN domain and the Distributed Unit (DU) which handles host time-sensitive instead. The authors in [163] highlight the challenges that arise in RAN slicing. Precisely, there are heterogeneous

Quality of Service (QoS) requirements of diverse services, significant interference in wireless network environments, signalling overhear cost by RAN slicing control and the RAN slicing control is a task with high complexity.

The Third Generation Partnership Project (3GPP) specified the latest RAN architecture called Next-Generation RAN (NG-RAN) introducing new interfaces, functional components, split options and technologies [165]. NG-RAN consists of next-generation Node Bs (gNBs) and next generation evolved Node Bs (ng-eNBs) and both are connected with the AMF-UPF functions of the 5G core over NG interfaces. Furthermore, gNBs and ng-eNBS are interconnected with each other using Xn interfaces [165]. Major differences with the previous RAN infrastructures are present only in the functionalities of the structural components, as the network architecture mostly remains the same. The authors in [166] state that NG-RAN should be slice-aware in order to provide differentiated QoS requirements to enhanced mobile broadband (eMBB), ultra-reliable low latency communication (URLLC) and massive machine-type communication (mMTC) service types UEs. Functions and components of NG-RAN can be virtualized in four different levels: application, cloud, spectrum and cooperation which means that in the aforementioned levels, slicing can be done.

To overcome the limitations of joint optimization and control of RAN components, the limited options for deployment of RAN equipment from multiple vendors and the overall limited reconfigurability, standardizations efforts created a new paradigm called Open RAN. Open RAN offers a solution for disaggregated, virtualised and software-based component deployments [168]. Those deployments are connected through open interfaces that are interoperable between multiple vendors at the same time. It is also highlighted that open and interoperable interfaces allow operators to use different equipment.

A specific implementation of the Open RAN architecture has been developed by the O-RAN Alliance [169] which has set detailed guidelines and specifications. They are focusing on extending RAN to be an open and intelligence domain, on developing open software in cooperation with the Linux Foundation and on supporting O-RAN member companies regarding testing and integrating their O-RAN implementations.

3.4.3 Edge/FOG

Multi-access Edge Computing (MEC) is a technology that aims to offload the computations and data storage capabilities closer to the end users and that is achieved by deploying computational resources to the edges of the network. Edge computing provides many advantages to 6G Networks such as low latency, improved QoS, increased speeds while allowing privacy and security issues to be addressed as well [174]. In detail, by bringing computing resources closer to the end-users, edge computing can significantly reduce network latency. This is particularly important for real-time applications, such as virtual reality and augmented reality, where even

small delays can cause significant performance issues. Furthermore, Edge computing enables the delivery of higher-quality services to end-users, by allowing for more granular control over network resources, such as bandwidth, processing power, and storage. By offloading computation and storage tasks from the core network to the edge, edge computing can reduce network congestion and improve overall network performance. Moreover, edge computing can improve privacy and security by keeping sensitive data closer to the end-user and reducing the amount of data that needs to be transmitted over the network.

An Edge is practically a semi-autonomous system that communicates and updates itself, when needed, through the central cloud and is separated into two levels; the MEC system level and the MEC host level [170, 172, 173]:

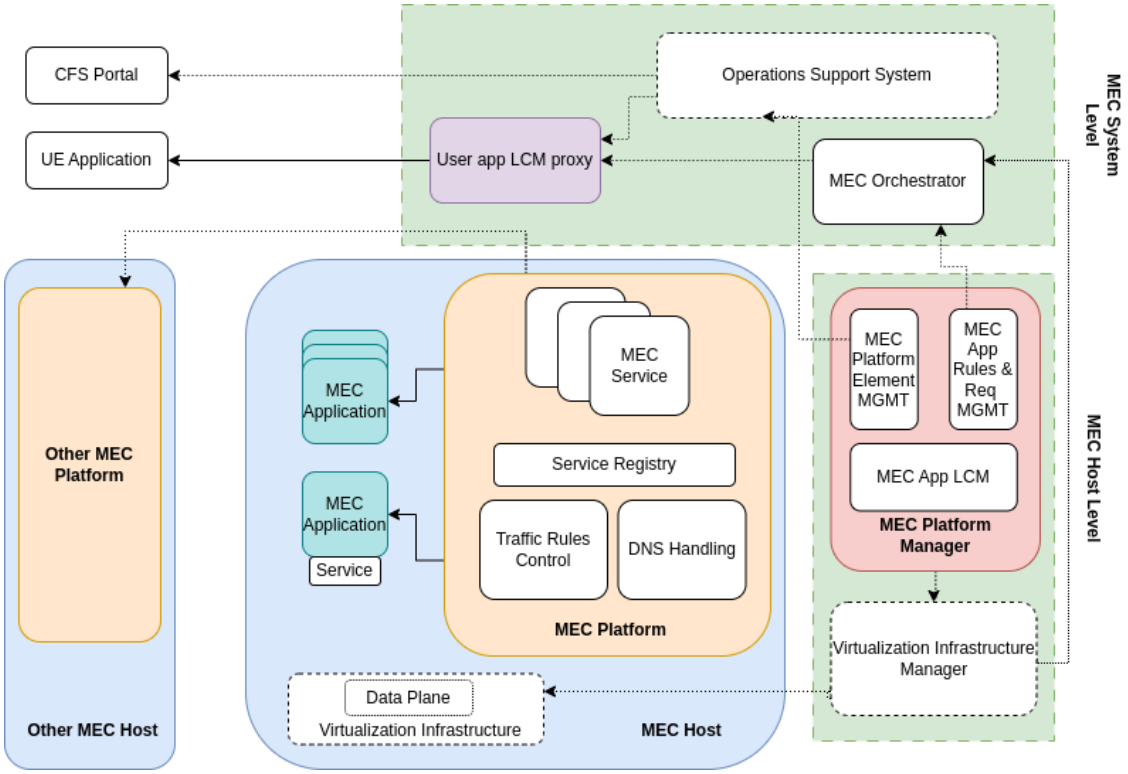

Figure 4 MEC Levels

3.4.3.1 MEC Host Level

- MEC host – The MEC host is a logical construct which embraces the MEC platform and the virtualization infrastructure that provides compute, storage and network resources to the MEC applications. A MEC host provides the resources for storing data near to the end users and the computational resources for the services and applications that run on that system. It contains the MEC platform and the virtualization infrastructure which provides computational, network and data storage resources in order to run MEC applications. Finally, it is connected with the core network of the MNO.

- MEC Applications - Applications that run as virtual machines on top of the Virtualization infrastructure and are created upon validated requests from the MEC management and based on pre-set configurations. When a MEC application is instantiated in the system, the system level management initiates a validating process for the service and the resources required as indicated by the MEC application. The host is selected according to the specified requirements as well.
- MEC Virtualization Infrastructure Manager (VIM) – It is responsible for the management of the virtualized resources that MEC applications require. Management actions can be the allocation of the application and the releasing of virtualized compute and storage nodes. Examples of VIMs that are often met in edges are Openstack and Kubernetes.
- MEC Virtualisation Infrastructure – It is deployed as a Network Function Virtualization Infrastructure (NFVI) and is managed by a VIM. It further includes a data plane that is responsible for the execution of traffic rules that route the traffic generated from/to applications/services/DNS servers/3GPP network/other networks. Traffic rules are received from the MEC platform.
- MEC Platform – MEC platform is a collection of all processes that are required by MEC applications, so that they can be fully functional on a particular virtualization infrastructure. It also provides access to persistent storage and time of day information. MEC services are provided and consumed by MEC applications and can sometimes be provided by the MEC platform itself.
- MEC Platform Manager - It consists of the MEC platform element management, the MEC Application Lifecycle Management (LCM) and MEC application policy management functions. The application LCM is responsible for instantiating, terminating and relocating a MEC application, further providing indications to the MEC orchestrator regarding application related events. The policy management includes authorizations, traffic rules, DNS configurations and resolving issues when conflicts are present in different set of policies.

3.4.3.2 MEC System Level

- MEC Orchestrator – A core component of MEC which supervises the complete MEC system. The authors in [170] state that this component is similar in many ways to the ETSI Network Functions Virtualization Orchestrator showing similar responsibilities such as coordination, instance control, resource conflict solving and many more. The orchestrator is typically located in the Edge Domain but can be often met in the Central Cloud. There is direct communication with the MEC controller and the MEC platform manager so that it is ensured that the MEC infrastructure is efficiently used and that the applications and services are delivered with the optimal performance and QoS. In detail, the orchestrator is also responsible for the

management of MEC applications and all related procedures, such as integrity and authenticity checks, policy validation, maintenance of an application availability catalogue, etc.

- Operations Support System – This entity is responsible for the instantiation and the termination of applications after a request is received from the CFS portal and UE applications. Processed request are forwarded to the MEC Orchestrator [172].

3.4.4 Transport

Transport networks are commonly identified as communication services provided by telecommunications operators to subscribers over large geographical areas. Transport architectures are complex networks that connect various access nodes (subscribers' point of presence) and data centers. The transport network can be summarized as an architecture that aggregates traffic from different areas towards a core network, or backbone, that carries large amounts of data to interconnect those areas between them, with data centers and with external to networks, such as roaming interconnections or the Internet. One relevant example are the 5G networks, where transport provides the connectivity between the Radio access, MEC, the 5G Core, Internet and the IPX roaming network. The transport network uses various technologies, such as DWDM, MPLS, and microwave, to increase the network's capacity and efficiency.

One of the key challenges in the development of 6G networks is the need for greater network flexibility to meet the demands of new topologies such as mesh networks, Non-Terrestrial Networks (NTN), and other emerging network configurations. These new topologies require greater performance, scalability, and QoS, which requires the development of new technologies and approaches to ensure that 6G networks can meet their demands.

The heterogeneity of 6G environments demands higher adoption of programmable networks and associated management technologies. The reference technology is Software-Defined Networking (SDN), an emerging network architecture (see Figure 5) that allows network administrators to manage and control the network infrastructure dynamically through software, rather than manually configuring each individual device [30]. The programmable nature of SDN also allows for flexibility and scalability, as new network functions and applications can be added or modified without significant changes to the underlying hardware.

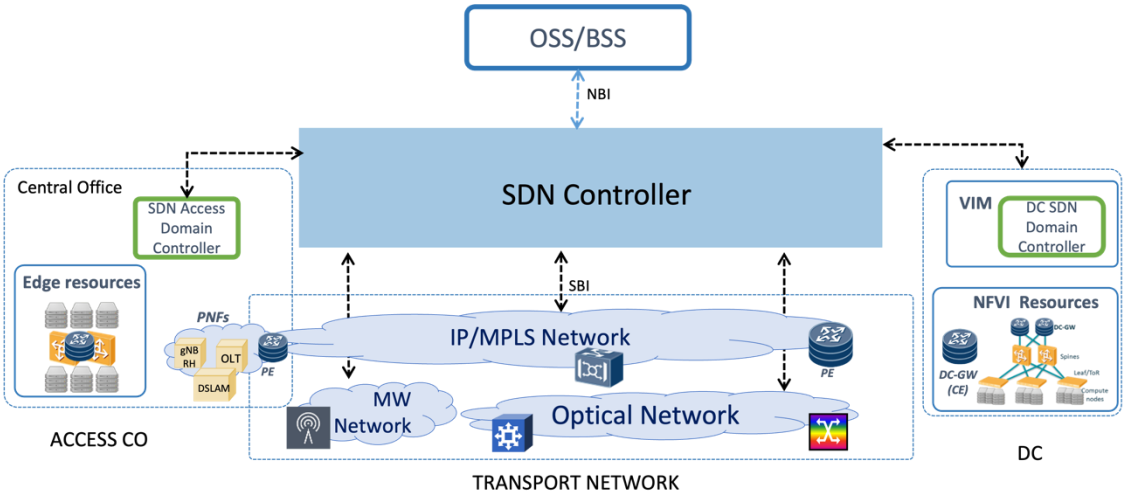

Figure 5 Network operator SDN architecture. SDN Controller and network domains interactions

Despite those advantages for 6G, there are also challenges such as security and privacy that need to be addressed as SDN continues to evolve [31]. One of the primary concerns is the centralization of control, which makes the network more vulnerable to attacks if the SDN controller is compromised, such as unauthorized access to the network, modification of traffic flows, or Distributed Denial-of-Service (DDoS) attacks. Additionally, the programmability of SDN also opens up new attack vectors, as attackers can use SDN APIs to inject malicious code and manipulate network traffic, including the traffic redirection for illegal inspection, with a clear impact on privacy.

3.4.5 Central Cloud

Many studies on 6G architectures indicate the convergence of mobile communications and cloud computing as one of the major drivers for network evolution.

4G started the path of network function virtualization and the 5G technologies, adopting a service-based architecture, accelerated the enablement of network cloudification, edge computing, and network as a service. In 6G, a further evolution of distributed cloud and communications systems is expected, where 6G systems will provide a wide-area cloud with ubiquitous computing across and among devices, network nodes and datacenters. Mechanisms for workload distribution among the computing nodes in the 6G wide-area cloud will enable a continuum of services and satisfy related QoS needs. A cloud-native philosophy will be a fundamental part of the design and deployment of 6G functions.

Cloud native refers to a system that has cloud designed for or built into it from the beginning. It describes the patterns of organizations, architectures, and technologies that consistently, reliably, and at scale take full advantage of the possibilities of the cloud (to support cloud-oriented business models).

The development of 6G technology is still in its early stage and there are many active 6G discussions and technology development efforts around the globe. If we try to summarize these discussions, a fundamental difference from previous generations can be observed and the majority of them are focusing on new dimensions of capabilities and services. The expectations are that 6G will be the first generation to shift from a communication-centric system to a communication computing-data centric system. The 6G system can become a wide-area cloud [83], a **cloud continuum**, with ubiquitous computing and intelligence across mobile device computing, network computing, and edge/centre datacentre computing. The 6G distributed cloud and communications system is expected to provide communication, computing, and data services. This contrasts with prior generations, which primarily provide communication services. The communication, computing, and data services can be provided in forms of infrastructure service (e.g., containerized communication-computing-data infrastructure), platform service (e.g., platform services for scaling out computing across mobile devices and network compute), and software services (e.g., data analytics services). The 6G system needs to be designed with the capability of providing those various forms of services (e.g., Everything as a Service (XaaS)). A computing service plane and a data service plane are expected to be introduced in 6G systems in addition to the communication service plane.

The scale of the mobile network will be leveraged to scale out computing, from regional/national datacentre computing to ubiquitous computing. This goes beyond the 5G network function virtualization and cloudification and will lead to a paradigm shift in communication and cloud computing. The shift towards a communication-computing-data centric system and the expectation of making 6G a **cloud continuum** is driven by multiple factors and perspectives:

- Business - there is a strong business need to introduce new dimensions of capabilities to foster the next trillion-dollar applications to sustain growth. Computing, communication and data are fundamental capabilities that the 6G system needs to enable. On top, various applications and use cases can be enabled, such as immersive reality, digital twin, connected automation, and applications powered by massive sensing and AI, etc.
- Technology - the current design of cloud and edges is not flexible because they were designed separately in a too rigid way which is a kind of limitation on the concept of a flexible a dynamical cloud. Mobile systems and cloud computing systems have been conventionally designed separately from mobile systems, focusing on providing better communication services and cloud computing systems operating over the top. This separate design approach works well for centralized computing. However, as computing becomes more distributed and moves to far edges, close coordination between communication and computing is needed to realize the benefits of distributed computing. The separate design approach adds barriers to the coordination between communication and computing and causes complexity

and scalability issues. This problem is becoming evident in 5G edge computing. To prepare for further computing scaling out from edge computing to ubiquitous computing in 6G, the system bottleneck and complexity has to be addressed. The transport network also needs to be upgraded from current service-unaware data pipe to a fully programmable and service-aware traffic path so that data can be flexibly steered to intermediate processing endpoints along a service chain.

- Application - emerging applications are raising the bar of higher demands on data and computing and more has to come. Many applications rely on AI technologies which need to be powered by massive amounts of data and high-end computing. Ultra-low response time are often required to meet mission-critical requirements or improve user experiences. The increasing use of sensors will lead to an exponential growth in data, which puts high pressure on communication, computing, and storage infrastructure. It is projected to generate 1 million zettabytes of data generated per year by 2032 [73]. The growth of data would far outpace the growth of communication capacity. We would not be able to transport all the data to datacentres for processing and even if there will be sufficient communication capacity, the cost of transporting data will still remain high. With an estimated 10 nJ/bit energy consumption for transporting data over 500 km, 22 trillion kWh of energy will be needed to transport 1 million zettabytes of data. Computing close to data sources is a way to cater to the exponential growth of data and reduce the energy cost of data transport. Moreover, increasing awareness of privacy and security often demands that data be processed at locations close to data sources.

Designing 6G cloud continuum means touch every aspect of the system, including system architecture, air interface design, service enablement and management, operation and management, software and hardware platforms, and an high-performance programmable transport network. A major structural change is expected to enable mobile systems to transition from a communication-centric system to a communication-computing-data system and still a lot of fundamental technical decisions need to be made.

This new paradigm of cloud continuum computing means that network and user data will be shared for compute purposes. Classes of data sensitivity and privacy-preserving methods should be researched to identify which data can be shared at which protection level. Security mechanisms and methods that preserve data integrity also must be soundly put in place.

4 6G Candidate Architecture and Technologies

The main objective of this chapter is to summarise the main innovative technical enablers which are required for the envisioned 6G architecture and, for each of them, present an analysis on the possible cybersecurity threats to which it can be exposed.

Table 3. 6G Key Enabling Technology per Layer

Layer		6G Key Enabling Technology	6G "Edge" Technology
Physical Layer	Spectrum & Communication	-mmWave communications -Terahertz (THz) Communications -Visible Light Communication (VLC)	-Molecular communications
	Antenna Modulation	-Ultra-massive MIMO, Cell-free MIMO -NOMA -Holographic radio -Large intelligent surfaces (LIS)	
	Coding	-Multiuser LDPC, space-time coding	
Connection layer (Network layer)	Networking & features	-SD-WAN -NFV -Slicing (Deep) -Blockchain, distributed ledgers -Post-Quantum Cryptography -Specialized FGAs	-Quantum communications
Service layer	Edge/Cloud features	-Container-based virtualization -Zero-touch service orchestration -Distributed/autonomous computing	-Quantum computing
AI	AI model & capability	-Trustable AI -Explainable AI -Machine Learning / Federated Learning -Specialized FGAs	

4.1 Physical Layer Technologies

The main 6G technologies foreseen for the physical layer will be described in this section. For each of them, the main security and privacy threats to which the technology could be exposed to will also be analysed.

4.1.1 MIMO Beamforming

MIMO indicates the use of a multiple antenna system, both on the emitting and receiving side, to improve the performance of the communication channel. Instead, beamforming, or spatial filtering, refers to a signal processing technique used in antenna and sensor arrays for the directional transmission or reception of signals.

In this document, two types of MIMO techniques are considered as the most promising:

- Massive MIMO: where massive refers to the large number of antennas employed in the base station antenna array. Those systems have the advantage of considerably enlarging the network capacity by supporting a large number of spatially separated users, and to simplify the signal processing required.
- mmWave MIMO: those systems can achieve high data rates by leveraging the broad spectrum of the mmWave band. This small wavelength regime makes possible the employment of large antenna arrays to extensively increase the throughput via spatial multiplexing.

4.1.2 Large Intelligent Surface

A Large Intelligence Surface (LIS), also known as Intelligent Reflecting Surface (IRS), is a planar antenna array whose entire surface area is available for radio signal transmission and reception. LIS-based communication is considered to play a crucial role in B5G and 6G technology thanks to the significant improvement of the spectral efficiency, the signal-to-noise ratio, and the reduction of the energy consumption during the transmission.

4.1.3 Non-Orthogonal Multiple Access (NOMA)

NOMA is a radio access technique for next-generation wireless communications allowing multiple users to be granted access to the desired channel. NOMA is expected to enhance performance gains by using the same resource in terms of space, time, and frequency. In addition, the access scheme is meant to provide enhanced spectrum efficiency, reduced latency with high reliability, and massive connectivity compared to the current Orthogonal Frequency Division Multiple Access (OFDMA).

4.1.4 Holographic Radio

Holographic radio, or holographic beamforming and MIMO, is regarded as a new dynamic beamforming radio technique for 6G indoor/outdoor communications. The holographic communication technique makes use of software-defined antennas or photonics-defined antennas arrays to improve overall efficiency by employing a low-cost, compact size/weight and low-power architecture.

4.1.5 Terahertz Communications

THz radiation consists of electromagnetic waves within the band of frequencies ranging from 0.3-3 THz, as designed by the International Telecommunication Union. THz communications aims at increasing the data transfer rates in the terabit-per-second order. They feature tremendously high frequency and extremely short wavelengths, which are expected also to mitigate the current spectrum scarcity and to promote 6G applications such as holographic communication and digital twins.

4.1.6 Visible light communications

Visible light communication (VLC) is a high-speed communication medium to transmit data by leveraging the visible light spectrum between 400 and 800 THz. VLC should support heterogeneous networks and a higher data rate, by dealing with gigantic traffic growth and by increasing efficiency and reliability of indoor network performance.

4.1.7 Molecular Communications

Molecular communication is an emerging field which aims at merging biophysical models and communication theory. Nowadays, with improved ability to manipulate matter, molecular signals can be used to deliver information through i.e. chemical encoding. In light of current studies, molecular communication is expected to improve system reliability in a deeply interconnected environment as the 6G network infrastructure.

The following table summarizes the main Security and Privacy threats the above-described technologies can be exposed to if not properly mitigated.

Table 4. 6G PHY Technologies main Threats and Mitigations

6G PHY Technologies	Security & Privacy threats	Possible Key Solutions	Open problems	References
mmWave MIMO Beamforming	-Eavesdropping -Jamming -Pilot contamination -Location exposure	-Frequency hopping -Injecting artificial noise or friendly jamming -Utilize beam alignment -Physical key generation -Physical coding	-Optimal beam alignment -AI-based low-complexity anti-jamming -High-performance coding -Energy efficient solutions	[78], [79], [49]
Large Intelligent Surface	-Eavesdropping -Location exposure	-Frequency hopping -Injecting artificial noise or friendly jamming, -Physical key generation -Physical coding	-Optimal LIS deployment -AI-enabled LIS -Specific LIS applications -Energy efficient solutions	[81], [82]
NOMA	-Eavesdropping -Power allocation contamination -Location exposure	-Frequency hopping -Physical key generation -Physical coding	-Security for NOMA-VLC, NOMA-THz, NOMA-LIS networks	[83], [85], [80]
Holographic radio	-Eavesdropping -Location exposure	-Utilize beam alignment -Randomly power limits -Access point placement -Physical key generation	-Optimal radio management -Joint RF and non-RF hardware -Holographic radio-LIS integration	[77], [86]

		-Physical coding		
THz Communications	-Eavesdropping -Jamming -Location exposure	-Frequency hopping -Randomly power limits -Access point placement -Utilize beam alignment -Injecting artificial noise or friendly jamming -Physical key generation -Physical coding	-Optimal THz base stations -Optimal THz-LIS integration -Optimal beam alignment -AI-based low-complexity anti-jamming solutions -High-performance coding -Optimal mmWave-THz links -Energy efficient solutions	[87], [88], [89]
VLC Communications	-Eavesdropping -Obscured attacks	-Frequency hopping -Injecting artificial noise or friendly jamming -Physical key generation -Physical coding	-NOMA-VLC performance -VLC/LiFi deployment -Optimal VLC access points	[90], [91], [92]
Physical-aided security	-Sybil attack -Physical data tampering -Trajectory tracking	-Physical layer authentication	-AI-based low-complexity solution -Multi-attribute multi-observation technique	[94], [95], [96]
Molecular Communications	-Device configuration manipulation, kills the molecules, attacking bio-machines from Internet environment -Data leakage	-Biochemical cryptography -Firewall, IDS to detect attacks from the Internet	-Energy efficient solutions -Secure Internet access	[75], [76], [93]

4.1.8 MIMO Communications threats

- Eavesdropping in MIMO communications is performed by detecting and wiretapping open wireless communications. In order to achieve their objectives, eavesdroppers should locate the beam scope or use a reflector for channel wiretapping.
- Jamming could constitute a serious threat since attacks would be able to influence beamforming matrices in channel estimation processes.
- Pilot Contamination is defined as an interference affecting channel estimation which effects can be highly disruptive by deteriorating data rate results. Generally, it is caused by sharing the non-orthogonal pilots.
- Location Exposure is defined as the risk of mobile users to be tracked while using 6G-based services and thus to have their geo-position location disclosed.

4.1.9 LIS threats

- Eavesdropping can be carried out by overhearing the data stream transmission from a base station towards legitimate users, lying in-between the transmitter and the legitimate receiver. The most conventional attack in mmWave networks appears to be performed by exploiting side-lobes leakage patterns. In addition, the eavesdropper's success also depends on his/her/them location.

Location Exposure is defined as the risk of mobile users to be tracked while using 6G-based services and thus to have their geo-position location disclosed.

4.1.10 NOMA threats

- Eavesdropping in NOMA networks can be carried out both internally and externally due to the interface of the downlink transmission, which makes NOMA vulnerable on both sides.
- Power Allocation Contamination can lead to inter-channel interference and to a decrease in the secrecy rate. Generally, for both uplink and downlink, the optimization of power allocation is deployed from the received Signal-to-Interference-plus-Noise-Ratio.
- Location exposure is defined as the risk of mobile users to be tracked while using 6G-based services and thus to have their geo-position location disclosed.

4.1.11 Holographic Radio threats

- Eavesdropping attempts are strictly linked to the nature of electromagnetic waves movements in the holographic spatial space. Electromagnetic waves uncontrollably propagate within a wireless environment, making them susceptible to wiretapping and malicious interception.
- Location Exposure is defined as the risk of mobile users to be tracked while using 6G-based services and thus to have their geo-position location disclosed.

4.1.12 THz Communications threats

- Eavesdropping in THz bands is considered to be inherently ineffective, especially in the lower THz bands, thanks to several aspects such as: high antenna directivity; sensitivity to atmospheric turbulence; the THz spectrum's short coverage range, making the signal scattering rate lower than other radio bands. However, eavesdropping could still be performed in special scenarios such as the one where the link has non-THz penetrable objects and/or in case of poor atmospheric conditions.
- Jamming attacks in THz bands have the same inherent difficulties to be performed as in the case of eavesdropping. Special scenarios, i.e., can occur in case of mechanical jamming where the adversarial physically places a blockage between the sender and the receiver; or by targeting a beam at the receiver at a particular operating frequency.
- Location Exposure is defined as the risk of mobile users to be tracked while using 6G-based services and thus to have their geo-position location disclosed.

4.1.13 VLC Communications threats

- Eavesdropping in a VLC-based channel can be accomplished into the line-of-sight of the sender VLC link in order to intercept signals.
- Location Exposure is defined as the risk of mobile users to be tracked while using 6G-based services and thus to have their geo-position location disclosed.

4.1.14 Molecular Communications threats

- Molecular communication is an emerging field and theoretical at macro-scale level applications, thus many security concerns are still subject to be properly analysed. Main security issues should probably regard privacy concerns from data leakage and device configuration manipulation from tampering with the molecules used to transport information.

4.1.15 Physical-aided security threats

- Sybil attack is an attack in which the reputation of a system is compromised by the creation of many identities that are used to gain disproportionate influence in the network. As a consequence, a Sybil attack can lead to spoofing the positions and/or identities of other nodes in the network. At the physical layer, this kind of attack can be performed by using physical attributes such as the angle of-arrival or the Received Signal Strength Indicator.
- Physical data tampering refers to any data, system, components unauthorized physical alteration causing the loss of integrity- of the system.
- The trajectory tracking of devices over a long period of time while using 6G-based services.

4.2 Blockchain

Among other requirements, the 6G technology envisages faster transmission rates, higher reliability, increased bandwidth, ultra-low latency, effective resource and energy management as well as strong security, aiming to support a wider range of devices and services. Blockchain technology has certainly demonstrated its potential towards enabling **data exchange**, while providing **auditability** over the data, hence it has direct linkage with the visions and key enablers of 6G technology [237]. According to 5GGP [238], "*The blockchain-based platform is one of the most prominent technologies to unleash the potential of 6G system.*"

Blockchain is a core building block for 6G networks, enabling **intelligent resource management, spectrum sharing,** thus **scalability** and **availability** for the emerging

smart environments (i.e., healthcare, smart cities, industry 4.0, agriculture, etc). The aforementioned capabilities utilise the notion of decentralised transactions, based on Smart Contracts [239]. Elevated connectivity demands on the network slice, for example, can be facilitated between operators by sharing resources as expressed on a smart contract, which constitutes, in essence, a Service Level Agreement (SLA). Numerous works provide scenarios where blockchain technology has managed to provide the basis for such a resource sharing ecosystem [240], [241], [242].

Blockchain is offering reliability over the monitored data utilising SLAs with diverse service level guarantees. Orchestrators may leverage information regarding the use of the available resources, stemming from the monitored data reports and the SLAs, to **enhance the decision-making process**. The collected data can empower 6G based network applications with better resource management (i.e., in terms of handling clusters used for the slices) and extensive reliability and coverage capabilities, leveraging prediction through eXplainable Artificial Intelligence (XAI). These predictions will permit better resource allocation with minimum energy consumption.

Additionally, blockchain, does not only provide flexibility, in terms of resource and spectrum allocation, but also permits **accessibility** of devices with limited computational and storage capabilities (i.e., sensors and nodes) [243], [244]. Consequently, advanced functionalities of next generation networks (i.e., crypto), may be explored even without the need to renew existing hardware.

Hence, since the blockchain technology is device and type-agnostic, it is the most suitable to offer an interoperable environment, with parallel support of **data portability**. This is needed in cases where the data owner might desire to migrate its data from one blockchain environment to another. In this context, there is a set of mechanisms offered by the blockchain technology, to support the secure data migration and secure lifecycle and management through smart contracts, while providing protection against underspending. This is an especially interesting feature considering the variety of stakeholders and the future landscape of networks, which will be comprised of multiple providers and services, and each stakeholder might employ its own blockchain network.

Apart though from the intelligent resource management, future 6G blockchain-based networks, enable data sharing/exchange with certain security guarantees, one of which is the accurate **monitoring, auditability** and **traceability** of the exchanged data, along with their respective supply chain [245]. This feature allows tracking of the origin and exchange of information, within the Blockchain network, increasing the **transparency**. The communication may take place among different service providers that may publish or update data (i.e., policies of Service Providers for service discovery and usage). Providers may also validate the source of the published data or the entity that has updated the data. In 6G and future computing networks,

it is of utmost importance to offer advanced security enablers that allow the verification of the authenticity and source of data.

To this extend, data is considered protected since **integrity** protection mechanisms are applied, along with **authentication and access control** mechanisms, to limit access to authorised entities only, while ensuring **accountability** of actions. An elevated security level is further achieved, leveraging advanced **encryption** mechanisms (i.e., confidentiality) [244].

Nevertheless, this blockchain-enabled data sharing shall not neglect the **privacy** requirements. As a result, to comply with both the security and privacy requirements, distinction among public and private ledgers must be performed, according to use case scenario, while enhanced crypto primitives must be employed. To this extend, the notions of Attribute Based Encryption (ABE) and Attribute Based Access Control (ABAC) can be exploited within the blockchain setup, to offer confidentiality and authentication linking, while restricting the access, based on certain user, system or device properties. However effective identity management is a pre-requirement for ABAC.

In decentralised infrastructures though, that are based on blockchain or distributed ledger solutions, such as the ones proposed by 6G, identity management is a complicated task, which turns even harder by adding the privacy requirements. The current trend, as suggested by the standards, is the concept of Self Sovereign Identity (SSI). The SSI can support the access control needs of such environments, specifically in 6G ecosystems, while providing **trust** in both digital identity and personal data across data transactions (identity and data sovereignty).

As suggested by its definition, the SSI allows the identity owner to maintain the **sovereignty** of their identity. Consequently, there is no central authority that manages the credential. Instead, each owner is responsible for managing their identifiers and credentials, while the blockchain is used to map the public keys of each entity to the identifiers. SSI can be used to identify not only users, but also assets and services. In essence, an SSI is a signed document composed by different claims, based on the issuer. To implement SSI, two new standards, namely the Decentralized Identifiers (DIDs) [248] and the Verifiable Credentials (VCs) [249] have been released by the W3C.

The DID is a globally accepted identifier, representing a digital identity (i.e., of either an asset or a user). Basically, it contains a public key referring to the entity that has possession of the corresponding private key. It is based on the main notion of SSI, meaning that the data object has sovereignty over their identifiers. The VCs are referring to a digitally signed document, contains information about a specific attribute or claim (i.e., software version or person's age). The VC can be either self-issued or issued by a trusted party, while they can be verified. Another point is that in order to provide tamper-proof signed assertions, cryptography notions are

utilized. This allows the reveal of only specific attributes within the document to the entity that requests the VC. More specifically, zero-knowledge proofs [255] and BBS+ signatures [256] have been proposed to achieve zero knowledge proof disclosure [257]. Towards this direction, SSI enables the support of ABAC [246], [247]. DIDs and VCs are regularly used in conjunction, to enable the creation of several attestations regarding a specific DID subject.

It must be clarified though that SSI ecosystem **does not strictly require** a blockchain or distributed Ledger technology in order to function. Nevertheless, the blockchain solution may offer the storage, update, deletion / recall functions.

All of the abovementioned technologies though, may offer an advanced protection in terms of security and privacy nevertheless there is a trade-off between security and efficiency in terms of reliability and coverage. Towards this direction, research will be conducted to discover the effects between security, privacy and performance, considering though the guarantees needed for each individual service (i.e., slice).

4.2.1 Blockchain Security & Privacy main threats in 6G

In general, the literature has identified several threats to blockchain infrastructures. Nevertheless, not all of them are applicable across the different architectures (i.e., permissioned vs permissionless, private vs public). Our implementation will be based on Hyperledger Fabric, which is based, by-design, on the notion of limited trust between the participating parties. Additionally, unlike permissionless infrastructures, the Hyperledger Fabric allows access to the network and the consensus algorithms is restricted to a specific group of participants. It is evident, that some of the attacks described in [250], will not be as common in the Hyperledger Fabric, due to its design. Permissioned networks, for instance, are not thus susceptible to 51% attacks and network partitioning attacks are less of a concern because users are identified, while their activities can be monitored.

The following paragraphs enlist the identified threats according mainly to [250] and [251] that may affect the security and privacy of Blockchain 6G services. The attacks can be summarized in 2 subcategories. The first analyses threats for all blockchain infrastructures, while the second one is more specific to threats against the Hyperledger Fabric. Several of the identified threats against Blockchain infrastructures, such as Denial of Service (DoS) and consensus manipulation, are universal to all distributed systems. Some attacks specifically target the Membership Service Provider (MSP) or another component of a Hyperledger Fabric network. The attacks along with the countermeasures are summarized on Table 6.

Denial of Service (DoS)

The DoS attacks target the availability of the system, with the intent to disrupt the access to the services. One way to launch such an attack is by leveraging traffic overload, to cause the blockchain network to crash or become unresponsive. This

threat may be limited though monitoring of performance indicators, such as transaction throughput and latency, to prevent early on the overloading of the network.

The Hyperledger Fabric network in specific, protects from such attacks through its protocol definition, which prevents unauthorized nodes to participate in the network (i.e., through authentication and access control mechanisms), while the Raft Crash Fault Tolerant protocol (CFT) is supported, to provide service even when a node is under attack [251]. Furthermore, the Hyperledger Fabric allows the administrator to set resource consumption limits for the nodes, thus limit such attacks that request more resources.

Consensus Manipulation

Attacks that target on the network consensus are also probable. The network consensus refers to the method through which the network's nodes agree on the present state of the ledger, i.e., the set of transactions that have been validated and added to the blockchain. The Raft Crash Fault Tolerant protocol (CFT) responsible to transfer the state of each node within the same channel/cluster does not provide protection against a malicious ordered node. Consequently, the orderer may control the state of the nodes and consequently manipulate the network and its transactions.

An example of such an attack is the 51% attack, which occurs when an entity or more, control more than 51% of the computing power within the blockchain network. This enables them to manipulate the blockchain by creating fraudulent transactions, reversing transactions, or double spending [250].

The Hyperledger Fabric network supports CTF, which is based on a particular threat assumption, nevertheless there is ongoing research on Byzantine Fault Tolerant (BFT) algorithms, which will be able to tolerate up to ⅓ of the network being malicious. Even though BFT is not yet supported, such attacks can be also detected and prevented through monitoring (i.e., leadership elections and transaction latencies) [252].

MSP Compromise

Another asset that can be compromised is the identity of the participating entities in the blockchain network. Attacks in this category vary and may stemming from acquiring keys and credentials to creating fake identities. Nevertheless, since the Hyperledger Fabric network implements its own mechanisms some attacks, such as Sybil attacks (i.e., where the attacker manages to create a fake identity or nodes to manipulate the network), are not as hazardous as others. Consequently, attacks against the MSP are considered more probable in the given network setup.

The MSP is in charge of handling the identities in the Hyperledger Fabric network, including the issuance and revocation of digital certificates that authenticate users and their transactions. As a result, if an attacker manages to steal the MSP's private keys or other authentication information, they may create fake certificates and thus, conduct fraudulent transactions. This attack type can be mitigated through secure identity management and access control mechanisms (i.e., SSI which was previously mentioned could add the further layer of security in the identity management system) as well as continuous monitoring of the network for anomalies.

Smart Contract Exploitation

Smart contracts may present vulnerabilities too. Attackers may exploit them either to steal funds or gain control of the network. The smart contracts are, in essence, the processes that execute the transactions, hence enforce the business logic. Smart contracts may enable the transparency feature within the blockchain. However, if certain protection mechanisms are not applied successfully, then they may be used in order to conduct fraud, gain unauthorized access to data or perform DoS. Consequently, the entirety of the smart contract lifecycle should be handled successfully by the blockchain network.

Towards this direction, the Hyperledger Fabric network proposes the use of analysis tools (i.e., Hyperledger Lab Chaincode Analyzer) for performing assessment before deployment. Additionally, security and code audits, network monitoring and formal verification tools are further proposed for sensitive applications in order to detect anomalous behaviour and errors prior and during the deployment of the contracts.

Nonetheless, oracles cannot be fully trusted in terms of un-tampering. Hence, research works imply the use of Trusted Execution Environment (TEE), to isolate the security-critical environment from the untrusted one thus, assure the correct execution of security-related operations. To achieve a decentralized architecture, more than one oracle will support the TEE.

Table 5. 6G Blockchain main Threats and Mitigations

6G Key Tech	Security & Privacy threats	Possible Key Solutions	References
Blockchain	DoS attacks	Select proper DLT solution (i.e., public vs private or consortium). Hyperledger fabric employs the CFT. Also, implementation of monitoring solutions for the infrastructure for performance indicators (i.e., transaction throughput and latency), to prevent early on the overloading of the network.	[250][251]
	Consensus Manipulation	Select proper DLT solution (i.e., public vs private or consortium), as well as proper consensus algorithm (i.e., avoid majority voting which is more susceptible to this type of attack). The Hyperledger Fabric supports CTF, which is based on a particular threat assumption, nevertheless there is ongoing research on Byzantine Fault Tolerant (BFT). Logging threat indicators though may prove an advantageous solution in the meantime of the BLT implementation.	[250][251]
	MSP Compromise	This attack type can be mitigated through secure identity	[250][251]

		management and access control mechanisms as well as continuous monitoring of the network for anomalies.	
	Smart Contract Exploitation	Identify semantic flows and vulnerabilities before and during deployment, using security tools (i.e., for static analysis), perform formal verification, or anomaly detection tools. The use of Trusted Execution Environment (TEE) could further improve the security of the infrastructure.	[250][251] [253][254]

4.3 SDWAN & NFV

The importance of Network Function Virtualization (NFV) and Software-Defined Wide Area Network (SD-WAN) technologies cannot be overstated as we move towards the next generation of wireless technology, 6G. NFV enables network operators to create a more agile, flexible, and scalable network architecture by virtualizing network functions that were previously run on dedicated hardware. This technology is in clear adoption in current 5G networks with the Service Based Architecture (SBA) adoption, that focus on the cloud native functions, and it is expected that will increase in future 6G. Meanwhile, SD-WAN is a software-based and cloud native approach to WAN connectivity that abstracts the underlying infrastructure to simplify network management and operation. Both technologies can work together to meet the growing demand for high-bandwidth, low-latency applications while making network management more efficient and cost-effective and improving performance, reliability, and security. From a Network operators' point of view, this technology improves the deployment and management of services. Furthermore, NFV and SD-WAN can give them more visibility and control over their networks, allowing them to optimize network traffic, reduce latency, and improve network efficiency. While NFV and SD-WAN technologies offer many benefits for 6G networks orchestration for multiple and complex domain interactions, they also introduce new security and privacy challenges that must be addressed. As these technologies move control from hardware to software, they increase the attack surface which could expose new vulnerabilities.

In this regard, multiple disaggregated networks domains will interact to conform the future 6G networks, and some trust information exchanges in these multi-lateral environments are expected. Moreover, privacy aspects could be relevant in these interactions. One of the challenges in establishing trust in network devices is the lack of a centralized mechanism for authenticating and verifying the identity of devices in a network. To address this challenge, Certificate Authority (CA) has been proposed [99] and widely used to certify specific components of the Virtual Network Functions (VNFs) in an NFV environment, such as VM templates and VNFDs, across various vendors and hardware devices. This approach helps to establish trust in the network devices and ensures that only trusted and authorized VNFs can be deployed, reducing the risk of unauthorized access and other possible security threats. But certificate enrolment and management solutions such as CMPv2 are complex and difficult to address. To automate the management and issuance of digital

certificates, new protocols such as the Automated Certificate Management Environment (ACME) [100 can be introduced in the NFV and SD-WAN context. This protocol simplifies the management of digital certificates by automating the process of obtaining, managing, and revoking them. This approach can help to manage many certificates and ensure their validity, reducing the risk of human error in the management and issuance of digital certificates. Also, it can be used to authenticate entities or delegate the management [101] on this multi-lateral network of networks for 6G.

Since providing trust is a key element to protect these technologies, mechanisms like network attestation [102] ensures the integrity of VNFs by verifying that they have not been tampered or compromised, enhancing trust and confidence in the NFV and SD-WAN components. In this context where network traffic is dynamically routed and managed by different services, cloud instances and domains, concepts such as data and traffic attestation complement network attestation to ensure the security and privacy of data. Traffic attestation plays a particularly important role in verifying the integrity and authenticity of network traffic in real-time. Some solutions like the Ordered Proof of transit (OPoT) [103] can overcome this challenge by providing a shared secret that needs to be reconstructed by all network nodes (e.g., VNFs of a predefined path). OPoT can be used to provide assurance and traceability that traffic has transited through a specific set of services or SD-WAN gateways, which can be important for compliance, security, and troubleshooting purposes. For example, it can be used to demonstrate compliance with regulatory requirements, to identify the root cause of a network performance issue and also to detect malicious behaviour in the network. This technology can also provide a granular information disclosure, from detailed node paths involved, traffic attested, up to aggregate verification based on privacy needs.

Table 6. 6G NFV & SD-WAN main Threats and Mitigations

6G Key Tech	Security & Privacy threats	Possible Key Solutions	References
NFV & SD-WAN	Platform integrity	Remote attestation and monitoring (Hypervisor introspection, Boot Integrity Measurement Leveraging TPM, VNF Image Signing) and VNF image signing.	[104][105]
	DDoS attacks	Security Management and Orchestration	[104][105]
	VNFs isolation	Boot Integrity Measurement Leveraging TPM	[104][105]
	Access breach	Volume/swap encryption, Remote attestation, and monitoring	[104][105]
	Regularity compliance failure	Traffic attestation and Remote attestation.	[104]
	Human-instigated attacks	Securing Administrator Accounts	[105]
	Network traffic exposure	Security monitoring and filtering	[105]

4.4 Artificial Intelligence and Machine Learning

Artificial intelligence, machine and deep learning will be one of the core technologies of the 6G landscape and is expected to lay the ground for the "6G connected intelligence" ambition. AI-enabled technologies will be introduced in a wide range of applications across layers, from the radio layer where AI can be employed, e.g., for beam optimization, to self-optimizing at the cell site or between any two endpoints [108]. The main goal will be to achieve better performance, energy efficiency, and strong security at lower complexity.

To achieve high computational efficiency and security at the same time, distributed storage and processing, both, at the edge and central data centres, along with federated-learning approaches will be key ingredients.

Deep-learning based attack prediction methods are promising to promote security for a constantly evolving environment such as 6G with the extreme connectivity. Analytics functions powered by AI and ML will be installed at all layers of the mobile network and will also be employed to enhance the security and privacy of the services, e.g., by employing deep learning for predicting malicious attacks, see, e.g., Ref. [109, 110].

At the same time, while AI/ML will benefit 6G security immensely, it is also likely that AI-initiated attacks as well as attacks directed against the vulnerabilities of AI/ML-based mechanisms in the networks will pose a great threat to the 6G service landscape because a large part of the subnetworks typically reside in untrusted domains. To safeguard the 6G networks, and to guarantee that the AI systems are safe from AI-enabled attacks, it must be constantly verified whether AI models running in user equipment (UE), radio-access network (RAN) or the core have been altered by a malicious attack. Consequently, after an attack has been identified, the system must be repaired automatically [111]. Regarding the new principles and needs of cyber-resilience, the 6G network will rely on automated software generation, static and dynamic bug detection, code optimization and automated code testing.

Also, AI-based privacy-preserving schemes, such as machine learning-based privacy-aware offloading concepts can be used to protect the privacy of the users' location and usage patterns through reinforcement or transfer learning techniques [111, 112].

In the edge layer, ML models are used to store and analyse data, e.g., extract features from gathered data. From this, a particular vulnerability arises regarding data poisoning or evasion as well as privacy leakage. In the control layer, which will be used for resource orchestration and management purposes, attacks are to be expected on the software-defined networking and machine-learning attacks on the ML models [111]. Moreover, in the application layer, ML attacks in the test and

training phases will be possible, such as model extraction, i.e., stealing the functionality of the model, and model inversion attacks to obtain the training data.

There are several techniques that will help enhancing privacy preservation within the 6G framework. Among them are multi-party computation, federated learning (FL), twin synthesis, homomorphic encryption and edge profiling [113].

In the following, federated learning is described in more detail along with probable attack surfaces, because it offers a privacy-preserving paradigm for collaborative computing within the 6G framework.

4.4.1 Federated Learning

FL is a machine-learning paradigm in which a flexible, collaborative and decentralized training of deep neural network models is enabled by sending copies of the global model to multiple clients. The FL process is controlled by a central server, while the training data are stored locally at the clients. These clients can be, for instance, mobile phones, tablets, speakers or other terminal IoT devices. Another type of local party can be large institutions with high data-storage and computing capabilities. They perform the training with their part of the data locally and send the local model back to the central server where aggregation algorithms are employed to obtain the global model. In this way, no training data need to be exchanged and through the aggregation mechanism the influence of possible adversaries is reduced [115,116]. A fully decentralized FL scheme, which is quite effective in preserving privacy, can be combined with distributed-ledger technology [117] or multi-party computation [118]. Because of its privacy-preserving characteristics, FL has been proposed for building machine-learning models in the setting of the Internet of Things and open networks, such as 5G and 6G, as it can enhance the trust of collaborative computing.

However, even this (partially) decentralized paradigm has its limitations and can, in principle, be attacked in various ways. For a comprehensive and recent review, see Ref. [114]. Because of the distributed nature and the different phases of the model computation that are involved in the FL paradigm, there are different possible attack points: during the data gathering and storing phase, the training and the prediction phases. To secure the FL scheme, effective measures must be taken for all phases of the paradigm.

Most probable attack types include eavesdropping, data poisoning, privacy inference, model poisoning, and evasion. Attacks can occur in all phases of the FL: The adversary can compromise the central server or part of the local clients, during the training phase the adversary can manipulate the global model which could leave a backdoor, during the training and the prediction phases the adversary can infer private information, incl. membership and attribute inference.

On the client side, contaminated data and malicious behaviour can lead to label or feature noise and impact the model training. In the training phase, tampering with gradients and parameters leads to a possibly impaired global model performance. Furthermore, eavesdropping can occur during the updates of models, such that the transfer between local clients and server must be protected, e.g., through encryption methods or protocols. The global model is finally deployed on the local clients, such that evasion or privacy inference attacks can occur at this stage. Evasion attacks typically change the outcomes of the prediction of the global model. The effectiveness of the privacy inference attacks depends on the knowledge of the adversaries, i.e., the model structure, weights and gradients.

To prevent adversarial attacks, starting with the data stored at the client side, a data quality assessment or evaluation of historical behaviour of the client leads to credibility verification of the client, e.g., based on the system logs. This, obviously, can only be detected, if a potential adversary changes the behaviour of the client in the uploads to the server after contaminating it and, thereby, differs from other trusted clients. During the training phase, privacy inference attacks can occur by an adversary obtaining gradients on different model layers, from which various information, and sometimes even the initial data, can be restored [119]. Possible defence strategies are gradient compression, encryption and perturbation. Poisoning attacks have the goal to influence the performance or to inject backdoors into the final global model, by manipulating local clients through changing data features, labels, parameters or gradients. Because of the FL architecture and the aggregation mechanism, the effectiveness of this type of attack depends on the number of affected clients. This type of threat can be mitigated by differential privacy (DP), i.e., adding noise to the aggregated model, or robustness aggregation, where the central server verifies the performance of the global model with a validation dataset [120]. During the prediction phase of the global model, which is deployed on the local clients, evasion attacks, where adversarial examples are designed to cheat the global model, and privacy inference attacks are the crucial types of attacks. The privacy inference attacks can be distinguished in three subtypes: model inversion, which can be used to learn relevant information, e.g., properties or attributes, about the original data by analysing the model, membership inference, which aims at testing whether a particular part of data, which can contain sensitive information, was involved in training the model, and model extraction, where relevant information about the target model is obtained, e.g., model parameters or hyperparameters. Fruitful defence mechanisms include information obfuscation methods, e.g., DP where either random or specifically crafted noise is added to the data, functions, gradients and parameters, which reduces the model's generalization performance [121]. DP is a strong notion for privacy that can be used to provide formal guarantees, in terms of a privacy budget, ε, about how much information is leaked by a mechanism. It has become a de facto privacy standard, and nearly all work on

privacy-preserving machine learning employs some form of DP. These works include designs for differentially private versions of prominent machine learning algorithms including empirical risk minimization [122, 123] and deep neural networks [124, 125]. One major task that DP entails is the utility-privacy trade-off. Much scientific effort is put into finding values of this ratio that achieve a good balance between utility and privacy, and into understanding the impact of privacy leakage concretely.

FL is an efficient solution for combining horizontally distributed data, i.e., in settings where all parties provide input to the same columns, but possibly for different rows of data. In addition, one may also want to combine vertically distributed data, i.e., in cases where different parties have distinct information about the same rows. For this application, FL will not work. Instead, one can use secure multiparty computation (MPC) to emulate a trusted aggregator [126]. The parties can contribute randomness to the process to add DP to the resulting model. MPC is a cryptographic tool that allows a set of parties to collaborate to compute a function, but with a guarantee that each party only learns their own input and any output granted to them. This emulates an ideal black box that takes input from each party and gives (possibly selective) output according to its specification.

Adversarial Attacks

An attack based on adversarial examples perturbs the input to the models in a way that may force the model to misclassify it. The changes to the input need to be so small that it still behaves in the same general way [127]. A typical example of this involves adding an imperceptible layer of noise to an image of a panda forcing the model to classify it as a gibbon, even though the image still looks like a panda to the human eye [128]. The exact mechanism for how adversarial examples work is not entirely understood and it is not always necessary to have the exact model to create adversarial examples that fool the model. If two models are trained to solve the same general problem, chances are that an adversarial example created to fool one of them may fool both [129]. As this is an attack in the test phase of the model, the effects and defences against it should be similar, both, inside and outside a federated-learning context. More research is required into the specific effects of adversarial examples in a federated learning context.

Adversarial training is one of the current defensive strategies against this type of attack, where the model is trained against adversarial examples constructed to fool the model [128, 129, 131]. Similarly, a GAN-architecture (Generative Adversarial Network [133]) can be used where the generator network generates adversarial examples and the classifier network is trained to correctly classify, both, original and constructed examples [129, 130].

Other defences include using provable robust machine-learning models, input transformation, using DP, and using a detection mechanism for adversarial examples

[129, 130]. Using provable robust machine-learning models may provide the strongest defence but may provide a lower accuracy and may suffer scalability issues with complex neural networks [128]. Training a model using differential-privacy techniques may help to make the model more robust against adversarial attacks as they introduce "benign" perturbations into the training set [132]. Differential privacy shows many similarities to adversarial training in both method and effects. It can be shown that adversarial training can achieve a good trade-off between privacy and model accuracy [134, 135, 136, 137].

Input transformation is a model-agnostic method for attempting to remove any adversarial elements from the input. This can be done, e.g., by adding random noise to the input to try to counteract the small adversarial perturbations [129, 131]. A GAN-based de-noising technique has also been proposed [131, 132].

Detection of adversarial examples permits handling them before a classification is made. This can be done by observing how a neural network behaves when faced with adversarial examples. For example, dimensional properties, feature attribution scores, and distances between adjacent classes may behave differently with adversarial examples [132]. The use of a variational autoencoder has also been proposed for detecting adversarial examples [132].

4.4.2 Explainable AI (XAI)

With the rise of AI applications, DL algorithms and their relative success at classification and natural language problems the field of XAI has also seen an increasing interest. It is a fact that DL models are often hard to interpret and explain which in mission critical application poses a challenge in key desirable properties such as trustworthiness, confidence, accountability, causality or fairness and ethical decision [138], [139].

Some models provide these properties by their own structure, such models based on conditional probabilities, or decision trees. In both cases, the model can be interpreted by a human operator and the decision process is transparent. These models are classified as white box models in machine learning. On the other side, black box models such as the case with most deep learning models offers little interpretability or explainability for their classification. Despite having the potential for good accuracy and performance as demonstrated by several studies and applications, the lack of human level interpretability creates problems for their application. If a model is not transparent in its decision process how can the researcher prove that the model complies with present law and regulations in its decision process? Even if regulations are not at play, a model with responsibility for security may have the power to alert or take remediation measures that have a non-negligible impact on end-user and end-devices.

To develop a XAI toolbox, it is important to consider XAI taxonomy and relations between each term. XAI itself has different conflicting and complementing areas with need to be understood before any effort to its application. From the literature review, a number of competing and complementary terms can be extrapolated:

Instance based vs Global based: achieve XAI based on global models, trying to obtain interpretability and explicability through the analysis of the whole model. In contrast instance based is preoccupied with satisfying interpretability and explicability to the current context that is being classified.

Before, Between, After Model Training: XAI methods can be introduced in the pipeline at different times such as before the DL model is trained. While before approach is mostly related with data summarization and categorizations of the dataset, the between and after approaches use trained black box models to develop XAI;

- Surrogate vs Visual vs Textual: the methos to describe the model or decision to the user. Any means understandable by a human operator are valid choices under surrogate;
- Confidence vs Causality: while confidence model metric is to assess the model decisiveness under an instance classification, causality classifies if it is actually truth that A implies B. A high probability and confidence score may not necessarily sufficient to state a causality relationship;
- Interpretability vs Expandability: different measures to understand a model decision making. While interpretability is focused on the decision process and how it is made, explicability add another layer with judgments and deliberations to the process and parameters in decision making process;
- Accountability and trustworthiness: while accountability is related to responsibility for the decision being made, the model output or human interpretation trustworthiness is related to the degree a human can actually trust a model output;
- Agnostic vs Specific: XAI can be general or specific to the models it is being applied to. This means agnostic XAI is intended as a general-purpose method while specific XAI is tightly coupled with a model of family of models.

Not directly linked with XAI, but an important related topic is federated learning which adds complexity to the implementation of XAI toolboxes. Often DL models require intensive distributed training across multiple instances. This adds problems such as learning synchronization and data partition for instance. XAI can be centralized in a federated environment in centralized instances or also federated in edge nodes as well. The last approach increases the problems of federated learning upon traditional XAI problems [140]. In applications for 6G networks with multiple intelligent edge devices, federated XAI can be implemented both on the edge and cloud nodes making computation and XAI models distributed across devices. Such

approach was devised for the case of predicting quality of experience in vehicular networks increasing trustworthiness in decisions while considering security and privacy management of edge data [147].

In the design of 6G networks there is a renewed interest in XAI to help further improve AI analytics discussed and applied in the previous 5G projects. Its implementation aims to improve human-machine interface in decision making and human-centric AI-powered 6G network [138],[139],[141].

One approach particularly suited for the 6G development might be a general approach to combine a model representation of a black box algorithm that offers some insights on how a particular black box model creates its decisions. This approach is implemented in generic XAI algorithms such as LIME [143], SHAP [142] or Anchors [144]. An implementation scenario would mean to maintain an interpretable model based on the back box models and the black box models at the edge of network. Protocols to query the validity of models at edge nodes may or may not require information exchange with the edge node.

Other approaches linked with DL and specialized GNN can be found in [145]. In this case Decision Trees (DT) are appended at the end of a DL algorithm to provide explanation based on the activation and backpropagation process of the DL algorithm. In contrary to the previous explanations this approach is model specific but within the scope of models projected to be used in the project.

Implementations or proposals of these algorithm in the area of 6G project currently being implemented can be found in the literature [139], [140]. Relevant implementations of federated learning and XAI can also be found in distributed problems such as wearable AI [146].

Table 7. 6G AI/ML main Threats and Mitigations

6G Key Tech	Security & Privacy threats	Possible Key Solutions	References
AI/ML	Poisonous attacks	Moving target / Input validation / Robustness aggregation / DP	[120]
	Evasions attacks	Defensive distillation / Adversarial training	[114]
	Eavesdropping	Encryption / Agreed-upon Protocols	[114]
	Model inversion attacks	Obfuscation methods / DP	[121]
	Model extraction attacks	Control information provided by ML APIs / Noise injection	[114]
	Adversarial attacks	Adversarial training / Input validation	[128, 128, 131]
	Privacy inference attacks	Gradient compression, (homomorphic) encryption, perturbation, differential privacy	[119, 121]

4.5 Slicing

4.5.1 RAN/Core network slicing:

In 5G technology, enhancing security through isolation using network slicing is paramount. The promise of fully utilizing network slicing at all levels - physical, network, and service layers - is even greater in 6G [148], [149], [150]. Figure 6 [157] demonstrates how RAN and core network slices provide logical isolation to address security concerns for diverse 6G applications. Each RAN/Core slice is logically separated from the others based on specific KPIs [151], [152], [153]. Inter-slice communication is only possible through their respective interfaces since network slicing prohibits crosstalk between slices. Consequently, any potential security interference or breach in a particular slice will not affect others. Ideally, achieving end-to-end isolation will significantly boost 6G security.

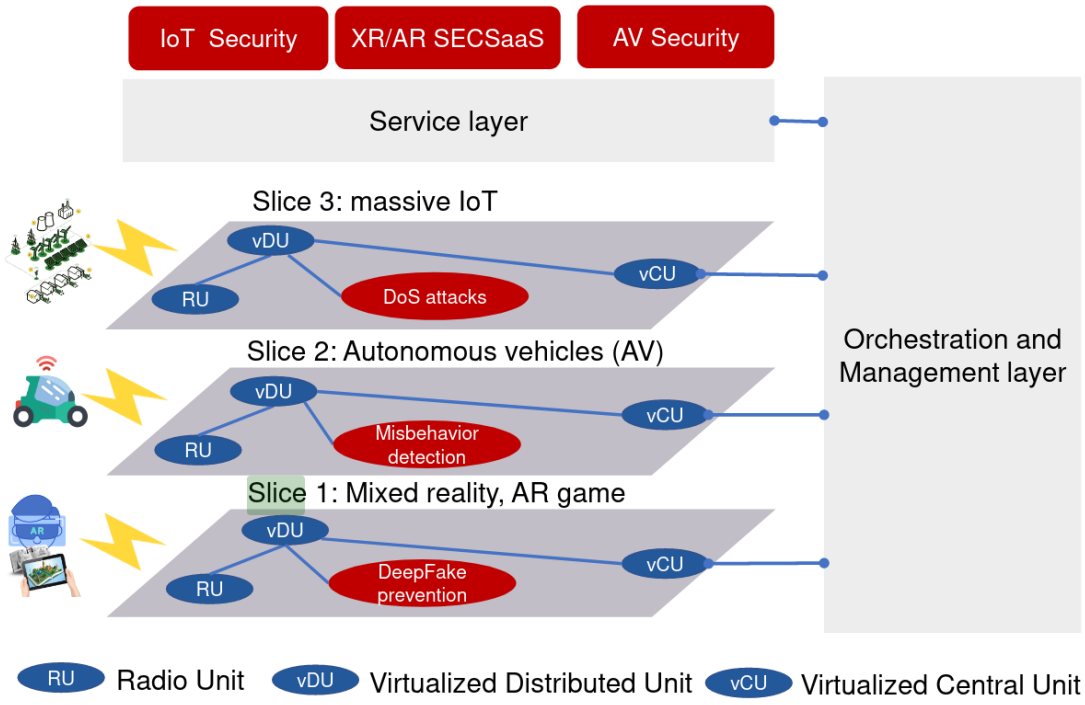

Figure 6 Security isolation through full slicing in conjunction with RAN and core network slicing [157]

As shown in the above Figure, it is important to use full slicing in conjunction with RAN and core network slicing to achieve security isolation. While slicing at the radio level and ensuring strict SLAs will present significant challenges due to costs, these measures are critical to achieving improved security.

Challenges:

Developing a security-isolation solution via network slicing poses a major challenge in meeting all KPI requirements per slice while independently enforcing strong security policies for massive slices. The absence of clear specifications on how to perform end-to-end slicing and develop a framework for automatic deployment remains an open issue. Defining isolation attributes for each slice, setting KPI requirements, and enforcing them are critical aspects of network slicing. Network Slice Management Function (NSMF) [26] serves as a network slice manager responsible for handling abstract virtual networks within its administrative domains. As such, the NSMF must be always readily accessible. However, mitigating large-scale DoS attacks [154] can be exceedingly difficult. Despite several existing protection methods such as Slice Management Service Authorization Procedure and mutual authentication [26], their implementation remains challenging due to the stringent processing and response time requirements.

4.5.2 Virtualized RAN, Cloud-RAN, and Open RAN:

Virtualized Radio Access Networks (vRAN) and Open RAN are emerging technologies that hold promise for enhancing security in 6G [155]. vRAN technology delivers the same functions as conventional RAN but, in this case, in virtualized mode, meaning that virtualized baseband units run on commodity servers instead of vendor-specific hardware. Two significant advantages of vRAN and open RAN for security are improved modularity and reduced inter-dependencies [158]. Modularity allows for more precise security attestation, while reduced dependencies on proprietary software decrease the risks associated with updating live networks. These benefits provide operators with greater control over their security infrastructure, which is crucial given the rapidly increasing network threats in the future. Furthermore, reducing dependencies enables operators to select the best vendors, creating a more robust supply chain that meets their security requirements. Relying on a single vendor can have significant consequences, as demonstrated in 2018 [156].

Challenges:

Most of the downsides of vRAN are related to managing the physical signal spectrum. Firstly, vRAN generates a significant amount of data and complex computation for beam spaces, which require faster baseband processing hardware. As capacity and bandwidth increase, computational requirements will also increase, which will require significant capital expenditures to fully virtualize the RAN. Secondly, signal processing fade and attenuation are more demanding in high-frequency spectra, which presents a technical challenge in managing data transmission efficiency and overheating on compact processors [159]. Finally, vRAN's distributed workload environment, which uses complete hardware and software separation, can result in unknown latency between workloads. These challenges have led the industry to focus on virtualizing 5G networks in the low band mmWave

spectrum, and it is unclear how vRAN will perform when 6G is pushed to even higher frequencies, such as THz.

While open RAN models and software-driven RAN approaches have their benefits, they also have their drawbacks. Firstly, publishing open-source code is intended to provide developers with constructive feedback from the community. However, if the source code is not appropriately designed and inspected intensively by security experts, it may become vulnerable, and hackers can easily find potential vulnerabilities to exploit without reverse engineering. Secondly, if a vulnerable source code is reused (e.g., as a library) for developing other codes, vulnerabilities can be frequently propagated.

Table 8. 6G RAN main Threats and Mitigations

6G Key Tech	Security & Privacy threats	Possible Key Solutions	References
RAN	DDoS attacks	Slice Management Service Authorization Procedure	[26], [154]
	DDoS attacks	Mutual authentication	[26],[154]
	Security attestation	vRAN modularity	[158]
	Live networks updates	vRAN dependencies reduction	[156]
Deep slicing	Load efficiency and network availability	Deep Learning Neural Network (DLNN)	[159]
	Cooperative attack detection	Reinforcement learning	[160]
	Designed jamming attack	Reinforcement learning	[161]
	Resource allocation for Edge Computing	Blockchain Network Slicing Broker (BNSB)	[162]

4.6 Zero-touch

Network automation, extreme edge computing and artificial intelligence are disruptive key enablers of future 6G cellular technologies. Specific 6G use cases shall include, but not limited to, massive digital twinning, Metaverse and full hologrammatic experience, robotics and local trust zones & perimeters. The paramount need for the idle operation of the previous bandwidth exhaustive application scenarios of 6G technologies is to *autonomously* determine the best possible location to deploy the serving 6G virtualized networking functions, in order to fulfil the service requirements. 6G fully cloud-native infrastructures will be meant to require the support of fully automated deployment pipelines, not solely to adapt to *zero-touch* paradigms *(i.e., fully automated networking processes without human intervention)*, but also to dynamically adjust to the extreme performance requirements of 6G infrastructure in terms of bandwidth, latency and computational capacity. The massive cloudification of infrastructures implies that available resources should natively be able to become appended in order to support the full workload or even to translocate specific services to grant latency or computing constraints [175].

It is assumed that 6G cloud-native network services can be perceived as a chain of microservices running on cloud-ready infrastructures. One of the targets aims of the upcoming 6G standards and a most challenging task, at the same time, is the cloudification of the RAN, referred as Cloud-RAN. The digital telecommunication complexity of the Cloud-RAN systems applies onto the minimum latency requirements involved in the physical layer, I.e., the base-band processing of radio communication signals. Explicitly, the time effort to construct and transmit RAN subframes is one and two msec's in the downlink and uplink adjacently, but the ultra-low latency requirements of 6G services will demand even more reduced time slots. Novel RAN architectures will consider splitting apart the RAN functions, and to migrate part of the radio processing higher in the network in order to hold common intelligence to various radio locations. The 3GPP organization aims to separate the RAN functions into three components Central Unit (CU), Distributed Unit (DU) and Remote Unit (RU), where the last one is to be placed near to antennas. The split of such Cloud-RAN infrastructures unfortunately includes several design challenges, like the time effort that must be allocated between the runtime of the RAN functions, and the transmission time between the distant RAN units. Further mitigation trade-offs involve the logical distance between the RU and the DU (known as the fronthaul size) needs to be as far long as possible to enable the centralization merits (like DU coordination), but short enough to meet the extreme low latency needs (1 millisecond). Several standardization efforts as well research outputs have been aiming towards identifying the most beneficial location and inter-distance of such RAN (sub)components trying to minimize the margins and increase the efficiency of the split up. Nevertheless, to better amplify the above aim and work towards the same direction, it is exactly where the zero-touch mechanisms come into display hereby to address such challenges with more beneficial results.

Zero-touch Cloud-RAN management involves the resource discovery (addressing both the computational and latency requirements to address the targeted zone), synchronization and automated re-configuration of RUs and DUs-CUs which are placed on far away Kubernetes-based nodes. The automated deployment can be initiated with the help of an API originating from upper network orchestration and management layers or by utilizing an ad-hoc SDN-driven Network Management System (NMS).

As previously stated, the increasing complexity of 6G cellular network conditions poses a quite challenging scenario for conventional human-centric management systems. The essence to handle the unforeseen dynamic flexibility, reconfigurability, and adaptation of the 5G/6G systems has launched the migration towards Zero Touch Management (ZTM) solutions. The ZTM philosophy aims to exploit the automation provisioning of self-operated and adapted networks in order to improve agility, performance, operational management together with the consecutive reduction of CapEx costs. Motivated by such realism, in 2017 ETSI founded the ZSM

ISG [178], which places the vision of ZTM-driven networks and services into full roll-out. The horizon goal ETSI ZSM is to offer a framework that enables *full end-to-end automation of network and service management* in a multi-tenant environment.

Specifically, the ZSM framework projects to follow the proceeding guidelines without human intervention:

a) *Planning and design*, to accelerate the deployment of automated provisioned networks and services that fulfil the needs of their subscribers.
b) *Delivery*, to provision on-demand delivery and access of online services while meeting requirements at the same time.
c) *Deployment*, to improve resource and service utilization and maximize or fully-allocate the service experience quality.
d) *Provisioning*, to reduce manual configuration losses and errors and fully automate service assurance policy.
e) *Monitoring and optimization*, to efficiently avoid service drop-down and re-assure fast network response.

We can illustrate the ZSM reference architecture in next figure, where a modular, scalable, and extensible Service-Oriented Architecture (SOA) relied on the decomposition of complex building blocks and management functions is presented.

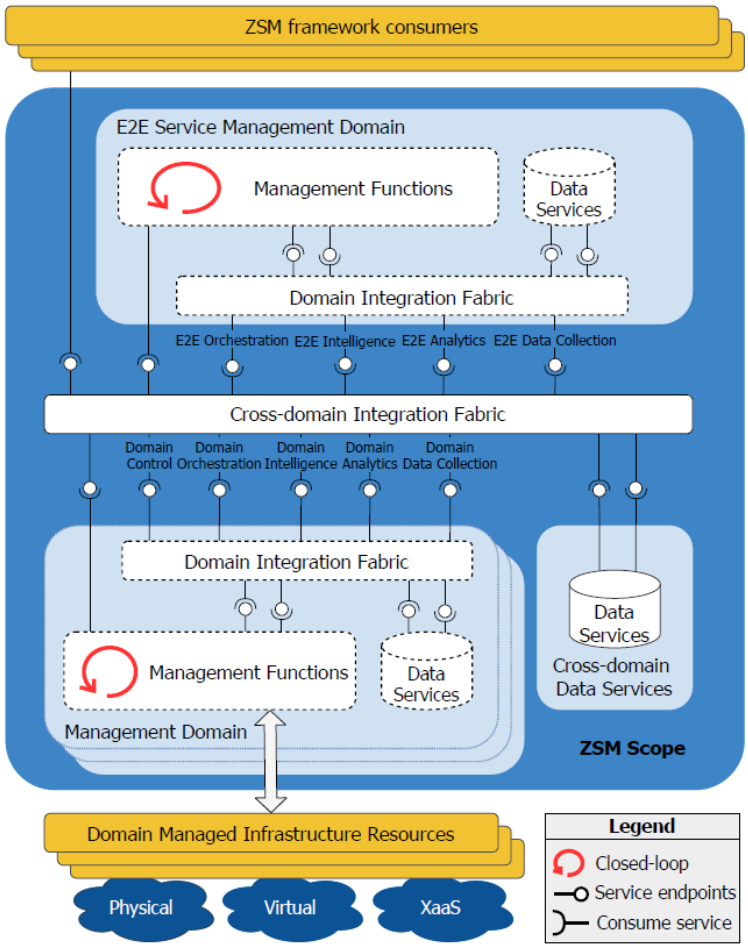

Figure 7 ZSM reference architecture [177]

The design architecture of ZSM shall also be attached to potential technological enablers [176], including (1) *programmatic control loops and management,* (2) *virtualization and orchestration,* (3) *data-analytics and closed-loop controls,* (4) *AI* generic techniques inside the networking domain. The (1) implies of the programmatic control of wireless and mobile networks projecting how network resources are presented to software modules, and how these software modules can affect the network state. The concept of SDN principles could become fully applicable hereby with the consolidation of network management functions at a logically centralized controller. (2) simply relies on the virtualization forces of 5G/6G network domains with the three leading relevant technologies of Virtual Machines (VMs), containers, and unikernels for the purpose the deployment of NFs as Virtualized Network Functions (VNFs). Complex AI/ML assisted data analytics can be referred to (3) with the advancement of Artificial Intelligence for IT Operations (AIOps). Finally, (4) with the adoption of XAI the whole networking system is meant to self-manage, self-sustain, self-adapt, and self-react to disruptions, anomalies, and changes with minimal human intervention (zero-touch).

Table 9. 6G ZTM main Threats and Mitigations

6G Key Tech	Security & Privacy threats	Possible Key Solutions	References
Zero Touch Management (ZTM)	Sybil Attacks: A malicious actor creates many pseudonyms to disrupt the network and influence the system cybersecurity.	Privacy-Preserving: Privacy-preserving is essential to prevent private information disclosure during multidomain slice orchestration, and zero-touch management.	[179], [180]
	Network Partition Attacks: An attacker can isolate a set of nodes to block the consensus or intercept network traffic.	Full Decentralization: To eliminate the security risks in centralized architecture such as single point failure, manipulation attack, etc, multi-domains slice orchestration architecture must be in total decentralization.	[179], [180]
	DoS Attacks: DoS attacks are typically realized by flooding the targeted server or resource with overflown requests in an attempt to overload systems and prevent some or all legitimate requests from being granted.	High Security: It is important to design a multi-domains slice orchestration architecture that possess inherent ability to mitigate DoS attacks, Sybil attacks, etc.	[179]
	Malicious Attacks: An attacker in control of a fraction of nodes may initiate malicious attacks such as tamper-proofing, eavesdropping, replay attacks, etc.	Tamper-Proofing and Consistency: The multi-domain slice orchestration information and ZSM procedure should be tamper-proofing and contain consistency.	[179]

4.7 Distributed computing

6G Network telecommunication systems are a complex set of versatile domains (e.g., dedicated, mobile, core), each one with ad-hoc constraint requirements. Concurrently, they need to offer communication transmission in an End-to-End (E2E) manner in order to adequately provision network services (NSs). The nowadays trend of centralizing the control plane management and dynamically allocating computing resources is being accomplished by the SDN paradigm. SDN allows E2E dynamic provisioning of services among multiple different domains and layers (I.e., WDM, Ethernet, MPLS/GMPLS) within an atomic request across the entire network. NFV permits the most efficient virtualized network functionalities management on available computing assets.

To further improve the network resource efficiency, 6G Edge architecture will forecast to implement Cloud Continuum architecture by placing small scale Data Centres (DCs) in the same access network domain as contrast to retaining them in the core network (cloud). The correlation of NFV with edge/cloud architectures ameliorates the resource orchestration and network flexibility. Utilizing virtualization technologies alongside the distributed DCs permits the deployment of NSs entities - I.e., a chain of VNFs - into the best DC slot possible. At the same time, the co-deployment of SDN allows the interconnection of E2E NSs, the Edge, and the Cloud, in a fully distributed way, clearing the path for creating a fully distributed 6G Cloud Continuum promise.

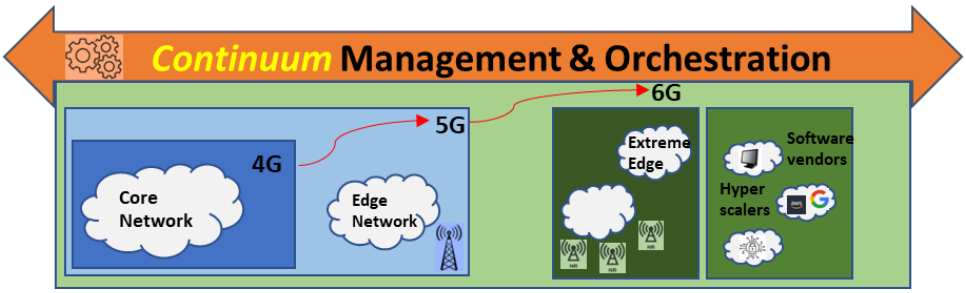

Figure 8 6G Cloud Continuum

6G use cases, alongside their verticals industries, shall require extreme computational components and others extreme low latency fulfilment (e.g., Metaverse). To realize such virtualized network functions (NSs), in 6G network developments, we must require for the establishment of network slices. A Network Slice Manager (NSM) and its internal architecture is dedicated to managing any distributed action related to Slices. Main such features include [181]:

- Shared NS - There might be specific occasions where different Slices may share same NSs. When new Slice deployment takes place, the NSM will check if the asked shared NSs are attached to other deployed Slices in order to make the new attachment decision properly.
- Multi-VIM deployment - *The current (and beyond) network is not anymore, a set of interconnected nodes between end users and the backbone core network where there lies a massive DC.* The future trend will be (6G) cellular networks to distribute DCs from the access to the core domain along with NFV/SDN network architecture. Thus, the Network Slice Manager must be potent to deploy Slices into different network domains and work with E2E Slices in multi-domain fashion.
- Hybrid Slices - The NSM should be supportive of different open-source software technologies to instantiate virtual network elements (e.g., Kubernetes, Open-Stack, etc.).
- NS composition: The NSM must be fully acknowledged of all the previous criteria in order to interconnect the NSs, something that is quite trivial.

The control, orchestration and management of the network is impossible to be done fully automated, without minimum human intervention. This is becoming a critical issue with the exponential growth of network traffic every day. Nonetheless, the nearby future development of the distributed computing cloud continuum in 6G will allow more intelligence, MANO-driven operations, and interoperability among completely different networking technologies, platforms and communication protocols.

Table 10. 6G Distributed Computing main Threats and Mitigations

6G Key Tech	Security & Privacy threats	Possible Key Solutions	References
Distributed Computing	Data breach: Slice customer data theft, file misuse, NSM log tampering	High Security Scalability: High scalability is a crucial factor to aggregate more network administrative domains to share network resources securely.	[179], [183]
	Information leakage: Network slice traffic redirection, security tokens theft, unauthorized access to signalling data, unauthorized access to user plane data.	Privacy-Preserving: Privacy-preserving is necessary to prevent private information disclosure during multidomain slice orchestration.	[179], [183]
	Network slicing specific: Configuration tampering, delete slices, deny access to slices, fake slice creation, misuse of virtualized functions, misuse of resources, unauthorized access.	Fairness and QoE/QoS: It is critical to guarantee the fairness and QoE/QoS in multi-domain slice orchestration by suppressing malicious behaviours in the system.	[179], [183]

4.8 Public-key cryptography and quantum computers

We give a brief overview over the historic and current trends in public-key cryptography.

4.8.1 Public-key cryptography and quantum computers

Private-key cryptography has existed in various forms since time immemorial. However, in order to successfully encrypt and decrypt, both parties need to share a secret key. Only as late as in the 1970's, cryptographers discovered how to generate secret keys from public conversations [184] and encrypt using only public information [185]. The schemes were based on the intractability of computing logarithms in finite fields and factoring large integers, respectively.

To achieve a comfortable level of security against attacks, the keys for Diffie-Hellman key exchange and RSA encryption and signatures must be at least 2048 bits, or 256 bytes. Fortunately, one can also use elliptic curves for Diffie-Hellman key exchange, reducing the key length to just a few hundred bits. We often use public-key encryption to negotiate a private key, which is then used to protect the data traffic.

In 1994, Coppersmith [186] demonstrated how a quantum computer could compute Fourier transforms exponentially faster than a classical computer. Shor [187] built on this result to show that a sufficiently powerful quantum computer could solve the factorisation and discrete log problems in polynomial runtime. This result, when run on an actual machine, renders much of the then existing public-key cryptography insecure. As a consequence of this, we need to consider the consequences and possible opportunities of quantum technology.

4.8.2 Quantum computers

Considerable resources are being used to build quantum computers. Quantum computers take advantage of the fact that while ordinary bits are either 0 or 1, quantum bits ("qubits") can maintain a superposition between these two according to some probability distribution. If we measure the qubit, it will collapse to either 0 or 1. However, the probability of which bit it collapses to depends on the underlying distribution. When combining several qubits, we can build a computer and run an algorithm on it. The algorithm will manipulate the probability distribution, such that the probability of us measuring a correct output of the algorithm is greatly magnified. Contrary to popular belief, a quantum computer does not check all possible combinations simultaneously.

The algorithms of Coppersmith and Shor can be used to solve the discrete log problem and the factorisation problem efficiently on a quantum computer. The application of these algorithms is limited to computations in abelian groups. In addition, Grover [190] demonstrated how a quantum computer can search an unstructured space of size n in approximately √n operations when n is sufficiently large. This implies that the key length of symmetric encryption should be doubled to achieve the same security level as in the classical case. However, due to the large overhead of Grover's algorithm, the actual security loss is considerably smaller [189].

Researchers at IBM have been able to double their performance every year since 2017 [188]. Foreseeing this development, cryptographers have worked hard to find quantum-safe alternatives to Diffie-Hellman and RSA. In 2016, NIST announced a process to find suitable mechanisms for key encapsulation and signatures. In 2022, four schemes were selected for standardisation, and the process will continue to further evaluate and on-board other schemes.

Cryptographers have employed a number of mathematical techniques to create post-quantum cryptography, including error-correcting codes, structured and unstructured lattices, isogenies on elliptic curves, multivariate equations, hash functions and zero-knowledge proofs. Among these, the code-based schemes have the longest track record, but suffer from severe performance issues for most applications.

Lattice-based schemes can trace their line back to 1996 [191]. In 2005, Regev [192] introduced the algebraically phrased learning with errors problem, and proved that even average-case instances of learning with errors are as hard as Ajtai's geometrical problems. Three of the four schemes selected for standardisation by NIST are based on structured lattices [193]. NSA has adopted a subset of NIST's recommendations for classified use. We can expect this selection to enter NATO specification, and therefore also become highly relevant for many European countries. In addition, Germany has selected conservative schemes based on unstructured lattices and error-correcting codes [194].

Isogeny-based cryptography and schemes based on variations of multivariate equations have suffered several attacks the last few years, and are currently not considered central in the short-term.

4.8.3 Cryptography from quantum phenomena

Cryptography has been largely the domain of mathematicians for the last 50 years. With the advent of quantum computers, physicists have also suggested ideas for key distribution. In particular, one can send polarised photon using one of two bases. The recipient choses a basis at random from the same set, and measures. When the measuring basis matches the sending basis, the measurement will be correct. Otherwise, it will be random. The parties can compare their choices of bases over an open channel. Furthermore, any measurement may also change the signal, so that any eavesdroppers will destroy the same key they try to extract [195]. This is called quantum key distribution (QKD).

QKD is positioned as a technology that requires dedicated hardware to provide symmetric keys to integrate with optical transport encryptors among other solutions.

Unfortunately, QKD does not defend against active adversaries ("man-in-the-middle"), who may cut the line altogether and impersonate both of the parties. Such an adversary will negotiate one key on each side, and just decrypt, read, encrypt and relay any future traffic between the parties. In order to solve this problem, the parties need to authenticate the basis comparison. This requires quantum-safe signature schemes based on the same mathematics that the QKD protocol is trying to replace.

Additionally, QKD schemes require a quantum channel between the parties, which limits the number of readily available applications. Nonetheless, the technology is generating interest for network operators and equipment providers [196], since optical and satellite networks (as part of future 6G networks) can integrate this technology. There are standardized interfaces for use by applications and protocols [197], which facilitates faster adoption.

4.9 Programmable HW platforms

The ability of 6G networks to handle computationally intensive applications like Machine Learning, render HW accelerators such as Field Programmable Gate Arrays (FPGAs) and Graphics Processing Units (GPUs) a necessity.

FPGAs are integrated circuits that can be programmed after manufacturing and as a result they are able to efficiently accelerate computations tailored to a specific application. FPGAs achieve better performance and lower power consumption than traditional CPUs, while being reconfigurable and having a relatively low design cost, unlike Application Specific Integrated Circuits (ASICs). GPUs are also useful HW

accelerators that are optimized for parallel processing of data, commonly used in Machine Learning applications.

Despite these HW accelerators achieving significant improvements in performance and latency, security issues appear. In general:

- Low power edge devices, connected to the end of a network, often become targets of security attacks (for example DDoS)
- There is often a difficulty in detecting malicious software/attacks, allowing for unwanted access to edge devices, taking control of other nodes or disrupting their functionality
- Early detection of unusual signals (anomalies), is essential in discovering compromised nodes and restricting error propagation in the network

Moreover, sensor circuits that can be implemented in programmable HW, such as Ring Oscillators and Time to Digital converters, can be used to extract information, while other types of techniques are used to cause miscalculations. Such security attacks are:

4.9.1 Side-Channel Attack

A Side-Channel Attack is a type of security exploit that takes advantage of information leaked from sources such as power consumption, electromagnetic radiation, or timings.

Due to FPGA long-wires having small distances with each other, there is a possibility of crosstalk, impacting the signal's integrity. Using a Ring Oscillator (RO) which consists of a closed loop of inverters, someone can extract data being transmitted in neighbouring wires. Thus, information can leak without the need of physical access.

Another method of stealing information is using an Electro-Magnetic (EM) probe and an oscilloscope, measuring electromagnetic emanation leakage during application execution. Demonstrations have shown that an attacker can obtain crucial information including the weights/parameters of AI models and general implementation elements.

Finally, Time to Digital Converter circuits, consisting of an inverter and a long carry chain, enable the attacker to identify key moments to initiate attacks.

4.9.2 Fault Injection Attack

One Fault Injection Attack type, focuses on modifying the clock waveform of the FPGA (Clock Glitching), causing timing violations, thus changing the output/inputs of different segments of the circuit. These faulty calculations accumulate over time resulting in poor accuracy.

Also, through the Power Attack that is implementing power hungry circuits (combinational loop-circuits) in HW that share a common power supply unit with the victim HW, the attacker can cause a voltage drop. Voltage drops influence the timing constraints of HW and result in incorrect Computations.

4.9.3 Covert-channel Attack

Usage of hidden channels to transfer information. The main threat of this method is when multiple devices (ie. GPUs, different FPGAs) are connected with the same power supply, taking advantage of sensing and stressing circuits in order to gain information.

4.9.4 Rowhammer Attack

Activating and deactivating DRAM rows rapidly, can leak charge to neighbouring DRAM cells causing bit flips. An attacker can thus alter data in memory addresses that he should not have access to.

4.9.5 Integrity and Authentication

Many of the attacks mentioned above, such as fault injection and rowhammer attacks, additionally constitute integrity threats. Thus, Integrity Verification is required, to make sure that changes in data have not been made without proper permission or approval.

When it comes to authentication threats, programmable HW is prone to cloning, counterfeiting and impersonation attempts from an attacker. Physical Unclonable Functions (PUF) are a solution that produces a unique identifier, taking into account physical characteristics of the HW that vary, due to manufacturing inaccuracies.

4.9.6 Denial of-service Attacks (DDoS)

Denial-of-service attacks aim to disrupt the normal operation of a system by overwhelming it with traffic or resource demands. Denial-of-service attacks can be carried out against GPUs or FPGAs by saturating their memory or computational resources, causing performance degradation or system crashes.

Table 11. 6G Programmable HW main Threats and Mitigations

6G Key Tech	Security & Privacy threats	Possible Key Solutions	References
Programmable HW	Side Channel Attacks	Routing Strategies / Power Spectral Averaging / Dynamic Frequency Scaling / FPGA Trusted Execution Environment / Noise Generating FSM	[198]
	Fault Injection Attacks		
	Covert Channel Attacks		
	Row Hammer Attack	Memory Access Scheduling / Guard rows / ECC Memory / Higher Refresh Rates	[202]
	Integrity and Authentication	Physical Unclonable Functions (PUF)	[200]

	DDoS Attack	Power Monitoring / Clock Gating / Over-Temperature Shutdown	[201]

4.10 Container-based virtualization

Currently, NFV technology is dominated by the use of Virtual Machines (VM), that use a hypervisor (i.e. KVM, QEMU) to abstract and virtualise the hardware, thus making it possible to run several guest OSs on the same physical machine. However, containers provide an isolation capability that allows multiple apps to share the same host OS without the need for a separate guest OS for each app. This creates a number of benefits for network virtualization and makes it a key ingredient for realizing the promise of NFV. Container images tend to be very small, as they do not (in most cases) contain complete operating system images, leading to (i) less overhead, since they have a far smaller memory footprint than VMs, (ii) reduced maintenance, and (iii) faster startup speed, enabling cloud native applications to scale and heal extremely quickly, and allowing for new and simpler approaches to system design in which containers are spawned to process individual transactions, and are disposed of as soon as the transaction is complete.

Furthermore, containers provide a high degree of portability across operating environments, making it easy to move a containerized application from development through testing into production, or between private and cloud environments, without having to make changes along the way. Being much more straightforward to deploy in the cloud than virtual machines are, they are also much easier to orchestrate. All of these benefits translate into cost savings, operational efficiency and service agility for CSPs.

5G and B5G networks are deeply based on virtualization technologies, allowing VNF in virtual machines. Virtualization platforms face different threats depending on the different virtualization approaches followed in the network, like server virtualization security threats (hypervisor-based attacks, VM-based attacks (such as cross-VM side-channel attacks), VM image attacks) and container management security threats, which will be our focus.

Two major types of container-based threats are:

- the compromise of an image or container
- the misuse of a container to attack other containers, the host OS and other hosts.

i) A container image that is missing critical security updates, or has an improper configuration, embedded malware, or straightforward text secrets, can be the target of exploitation that compromises the security of the rest of the system. Likewise, images often contain sensitive components like an organization's proprietary software and embedded secrets. If connections to registries run over insecure

channels, the contents of images are subject to the same confidentiality risks as any other data transmitted in the clear [203].

ii) By default, in most container runtimes, individual containers can access each other and the host OS over the network. If a container is compromised and acts maliciously, allowing this network traffic may risk other resources in the environment. Moreover, a container running in privileged mode has access to all the devices on the host, thus allowing it to essentially act as part of the host OS and impact all other containers running on it.

Container-based virtualization has also inherited security threats from other typed of virtualization technologies. The Emerging micro-architectural attacks, such as (i) cache-based side-channel attacks, (ii) transient execution attacks [204], [205] (meltdown, spectre), (iii) co-location attacks and (iv) others, also impose severe security risks for cloud users in container environments.

(i) Cache-Based side-channel attacks, such as FLUSH+RELOAD [206] exploit the side effects of different access time between cached and not cached data.

(ii) Modern processors leverage out-of-order execution mechanisms to maximize the utilization of all the execution units of the CPU core [204]. Meltdown can construct a section of instructions and use out-of-order execution to execute unauthorized address access in advance. Although this instruction will raise an exception (i.e., page fault) and then retire, the data from the unauthorized address will be temporarily loaded into the CPU cache. Finally, the data in cache can be recovered through the cache-based side-channel attacks.

Speculative execution and branch prediction are more optimization techniques of modern CPU, which can minimize latency and increase parallelism through prediction of the most likely path of the program and execute the next instructions in advance [205]. Similarly, the attacker can carefully structure the code to allow speculatively executed instructions to access private data, and the data will also be loaded into the CPU cache, which can be recovered through the cache-based side-channel attacks. Unlike meltdown attacks, spectre attacks cannot achieve privilege escalation and need to be customized for the software environment of the victim process.

(iii) An important prerequisite to initiating a micro-architectural attack is achieving co-location, i.e., managing to run on the same nodes as the victims. It has been shown that cloud schedulers can be exploited by attackers to achieve co-location [207], [208]. Both policy-based schedulers [208] and machine learning-based schedulers [207] can be exploited to achieve relatively high co-location rates in the heterogeneous cloud. These attack methods exploit the fact that schedulers in heterogeneous clouds tend to place application instances on the most suitable machines. Furthermore, because heterogeneity is considered during the scheduling

process, there is a higher chance that schedulers can be tricked and place attack instances on the same node as the victim.

(iv) Targeting hardware design flaws, rowhammer attacks [209], [210] utilize circuit features in DRAM chips, like electromagnetic coupling effects, to issue attacks and stealthily cause bit-flips in DRAMs. Fault attacks [211], [212] exploit frequency/voltage adjustment features in modern computer systems and maliciously insert faults during the execution of a program.

Table 12. 6G Container based virtualization main Threats and Mitigations

6G Key Tech	Security & Privacy threats	Possible Key Solutions	References
Container-based Virtualization	Image or container compromise	support images with security updates, not embed secrets in images; encryption during data transit to/from registries and use of secure channels	[203], [213], [214]
	Misuse of a container to attack other containers	restrict network traffic on suspicion of container malicious act; not running containers in privileged mode	[213]
	Cache-based side-channel attacks	cache leakage free code, page colouring for cache isolation, intel CAT, unusual behaviour detection (eg. performance counters)	[215]
	Transient execution attacks	keep systems updated with security fixes, only allow trusted images, use a whitelisting approach at runtime to only allow legitimate behaviour, container-level firewall for network control	[216]
	Co-location attacks	strategies to lower heterogeneity of cloud environment (eg. HLD, R-HLD)	[217]
	Rowhammer attacks	static physical kernel isolation enforcement (eg. CATT), defence against page table based privilege escalation attacks (eg. SoftTTR), rowhammer vulnerability detection in DRAM-based systems (eg. DRAMDig)	[218]
	Fault attacks	hardware/temporal/information redundancy	[219]

5 Privacy aspects

Privacy preservation refers to the ability to safeguard sensitive information across various stages of the data life cycle, including data collection, processing, and use. Unlike security, privacy preservation is guided by three distinct principles known as linkability, identifiability, and traceability (LIT)[107]. Linkability refers to the ability to link consecutive activities of the same identity in sequence. Identifiability pertains to the ability to recognize the true identity of a party within a system through collected information. Finally, traceability describes the capacity to track the activities of a specific identity. Privacy preservation is a long-standing issue, but it becomes more urgent in 6G networks for various reasons. Firstly, in the era of supercomputing and intelligent agents, safeguarding personal information is challenging. With a vast network like 6G that connects things and people, the demand for AI-powered smart applications is expected to grow exponentially. These applications can extract more context-related information of an individual and their environmental context, thus providing more precise and smarter personalized services that users may enjoy. However, this type of experience also poses a threat to users' privacy. Users may not be aware of being targeted by massive data collections for unsolicited advertisements or, worse, stalking and extortion powered by AI. There is a trade-off between two conflicting goals: high privacy preservation for individuals and their right to be forgotten and mining personal data to maximize the accuracy of recommendations and guidelines for users. The border between providing useful information and being abused for monetization is fragile, especially in a data-driven industry [6].

Thus, while 6G networks are not yet fully defined and implemented, there are some potential privacy issues that could arise as these networks are developed and deployed. In addition, 6G networks are expected to play a key role in enabling the next generation of Internet of Things (IoT) devices, creating a more interconnected and pervasive network.

Overall, while 6G networks have the potential to offer many benefits, it will be important to address these privacy concerns in order to ensure that individuals' privacy rights are protected. This will require a collaborative effort between technology companies, policymakers, and other stakeholders to develop and implement privacy-preserving technologies and regulations.

In 6G, the preservation of data privacy is of greater concern due to various reasons. Firstly, safeguarding personal data in a world of supercomputing and smart agents is challenging, especially with the growing demand for AI-enabled applications. Such applications can reveal more context-related information about a specific individual and their environment, leading to a trade-off between privacy preservation and

providing personalized services. Secondly, 6G is expected to provide more sensitive information from key applications like smart clothing and implant cyborgs, which can be collected illegally and abused. Thirdly, making more core cloud components and applications in 6G may increase the risk of unauthorized access to and exposure of personal information. Lastly, the more accurate localization through telecommunication in dense networks may raise concerns about surveillance. Given these concerns, many countries have begun to tighten rules for protecting users' personal information.

5.1 Regulatory context of Privacy

In today's digital and network economy, collecting and sharing data are critical functions. Consequently, the misuse and dissemination of collected data in a deeply interconnected and interdependent network can pose significant threats to users, allowing adversaries to steal sensitive data or to blackmail them. With the increasing complexity of managing data privacy compliance requirements already present in 5G networks, these risks are likely to become more severe with the implementation of 6G networks. To gain public trust, many organizations and companies have recently started paying serious attention to implementing advanced protection of customer data.

Thus, in light of such developments, new questions arise: How the usage of 6G services could lead to privacy leaks? What is the state of the juridical framework at the EU level? And how effective is it in preserving the privacy of the upcoming mobile users?

In general, privacy is accounted as a fundamental human right, recognized by many international human rights law instruments, including the Universal Declaration of Human Rights as stated in Art. 12. The EU has also recognized privacy as a fundamental right and has established various legal frameworks and regulations to protect individuals' privacy in the digital age.

The EU's definition of privacy is based on the idea that individuals have the right to control their personal data and protect their private life and communications. This is enshrined in Article 8 of the Charter of Fundamental Rights of the European Union, which states that:

i. Everyone has the right to respect for his private and family life, his home and his correspondence.
ii. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime,

for the protection of health or morals, or for the protection of the rights and freedoms of others.

With the development of Internet and the proliferation of its users, it has been deemed as necessary to further expand the concept of privacy so as it would have been included within the electronic communication sector. The first regulated EU act has been the Privacy and Electronic Communications Directive 2002, widely known as the ePrivacy Directive.

The EU's approach to privacy is based on the principle of data protection, which seeks to ensure that individuals have control over their personal data and that organizations and businesses that collect and process personal data do so in a way that respects individuals' privacy. Specifically, the ePrivacy Directive regulates the processing of personal data and the protection of privacy in the electronic communications sector. It requires that providers of electronic communications services obtain users' consent before using tracking technologies, and it requires that the confidentiality of communications be protected.

The EU has established various legal frameworks and regulations to protect individuals' privacy, including the General Data Protection Regulation (GDPR). The GDPR, which came into effect in 2018, sets out rules for the processing of personal data by organizations and businesses operating within the EU. It requires that organizations obtain individuals' consent before collecting and processing their personal data, and it gives individuals the right to access and control their personal data.

In addition to these legal frameworks, the EU has established various bodies and agencies to oversee the protection of privacy and data protection, such as the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS).

Article 4 of the GDPR defines several key terms that are essential to understanding the regulation. Inter alia these include:

- Personal Data - any information that relates to an identified or identifiable natural person, also known as the data subject. Examples of personal data include names, addresses, email addresses, IP addresses, and financial information.
- Processing - referring to any operation performed on personal data, such as collection, storage, use, and deletion. In addition, a restriction of processing is envisaged to limit the processing of stored data in the future.
- Profiling – any automatic means used to process personal data by collecting such data from evaluations related to the natural person.

- Data Controller - the legal entity that determines the purposes and means of the processing of personal data. In most cases, this is the organization that collects and processes the data.
- Data Processor – the legal entity that processes personal data on behalf of the data controller. Examples of data processors include cloud service providers and data analytics firms.
- Consent – one of the most important of the legal bases for processing personal data. Consent must be freely given, specific, informed, and unambiguous, and data subjects have the right to withdraw their consent at any time.

For almost two decades, the ePrivacy Directive has been the benchmark legislative text regarding privacy and data confidentiality in the context of public network electronic communications. Being a law that applies only to a specific context, the ePrivacy Directive has always been object to amendment and reinterpretations (I.e. from the European Court of Justice), as it can be inferred from its relationship with the GDPR. In fact, according to the principle *lex specialis derogat lex generalis*, the ePrivacy Directive applicability (special context) is subordinated to the applicable measures of the GDPR (general context).
The current ePrivacy Directive has not been sufficient in describing and tackle the whole digital privacy ecosystem, so there are ongoing works for the development of a new and more comprehensive regulation, in order to overcome also the special applicability of the old privacy Directive. The new ePrivacy Regulation is expected to strengthen and update, aiming to address changes in the digital landscape since the previous revisions, including the widespread use of smartphones and other mobile devices, and the rise of new forms of online tracking and advertising. It will consist of a set of regulations and guidelines designed to protect individuals' privacy when using electronic communications services, such as email, messaging apps, and social media platforms. The purpose of ePrivacy regulations is to ensure that individuals have control over their personal data and to protect their privacy rights when using electronic communications.
Overall, the GDPR and 6G networks are linked in that companies and organizations involved in the development and deployment of 6G networks will need to ensure that they are compliant with GDPR requirements for data protection and privacy. This will require the implementation of appropriate technical and organizational measures to ensure the security and confidentiality of personal data, as well as the provision of information to individuals about the processing of their personal data and the ability to exercise their rights with respect to their data.

5.2 Privacy as a security property proposal

The terms *privacy* and *security* are often used interchangeably, but often without sufficient context. In PRIVATEER, we will need to contextualise these terms, as there

is a number of actors on the system that may need both, but against different threats.

Assume we have a system of *n* players. These may be either *malicious* or *honest*. Notice that a closed system that consists entirely of honest players need neither security nor privacy measures, as an honest player will never abuse data or diverge from the protocol. Conversely, the term malicious does not necessarily mean cunning or bad intent in this context: It may also be due to outsiders entering the system, new management, programming errors, or even requirements from authorities. We name these changes to a player as *corruptions*. Any other behaviour than what is specified by the protocol is considered malicious, but without taking a moral stance to what or why.

As a first example, consider a simple conversation between a user Alice and a service provider, using a communication channel. If we assume that the channel is used in an honest way, Alice and the provider do not need to protect their communications. However, if we assume (as one should) that the channel can be controlled by malicious parties, then the other players should use cryptography in order to enforce honest behaviour in the channel: encryption will enforce confidentiality in the channel, whereas authentication will force the channel to deliver messages as the sender sent them, lest it be caught in action. This is how and why we set up our TLS or VPN connections.

GDPR and other regulations lay out a number of practices to follow to maintain the privacy of end users. One of these is data minimisation, which requires the service provider to only collect data that is strictly necessary to provide the service. The underlying reasoning is that this will limit the damages if the service provider becomes malicious at a later stage. This is privacy-by-regulation, which implicitly assumes and requires that all players are honest at the outset.

As in the above example, we can also build privacy directly into protocols. One relatively recent example is the DP^{3}T contact tracing protocol [220], which Google and Apple partly adapted as their exposure notification system during 2020. The first contact tracing ideas required the users to provide data about their interactions to a central service, which would then match contacts, and provide alerts to users. However, this data would also allow the central service to learn about meetings between any users. From the user's perspective, we must assume that this service could become malicious, and that would leave the user defenceless, regardless of the quality of the TLS channel or the length of the server passwords. One can both provide confidentiality guarantees against outsiders, and ensure privacy for users against insider threats. These concepts are fundamentally not the same.

In contrast to this, the data gathered by the central service in DP^{3}T was worthless for the central service in order to detect whether two people had met. Users continually broadcast random messages and record any messages from other users within

range. Infected users would anonymously post their random messages on a public bulletin board. If other users checked the board, and detected an overlap between their records, they would know that they had been in the proximity of an infected person. This is privacy-friendly, since the bulletin board never sees data that allows it to learn any of the users' private data. In a conceptual way, the protocol has forced any would-be malicious bulletin board to be unable to learn anything more than an honest bulletin board.

In essence, privacy is one player's defence against the prying eyes of others. In this sense, we can view privacy as a security property alongside confidentiality and authenticity, when properly quantified *for whom* and *against whom*.

Finally, assume that the service provider from the above example has a private algorithm. If the provider ensured that any data sent to the user, regardless of malformed input from the user, was untainted by the algorithm, this could be characterised as the provider's privacy against the user.

Notice that this understanding of privacy includes the intensions of current EU regulations, but fundamentally assumes that other players in the system may be malicious. This framing of privacy does not itself imply properties such as data minimisation but facilitates reasoning about the necessary trade-offs between different requirements such as service availability and privacy.

5.3 6G Main Privacy Concerns

This section presents and analyses the main predicted 6G ecosystem privacy concerns, as well as the possible approaches to mitigate the threats.

5.3.1 Privacy concerns in the processing of infrastructure and network usage data for security analytics

It is foreseen that 6G network components will be highly heterogeneous and more distributed across the network in contrast with 5G, which already implements a distributed architecture. As already highlighted in this TL, this cloud-continuum will create an enormous amount of diverse data (mostly logs, flow data and monitoring information), from the infrastructure, the core functions and the applications, whose timely analysis can lead to effective inference of security incidents. Current security analytics mechanisms perform this processing in a centralised fashion, which can be a privacy issue both for users as well as infrastructure providers.

A possible approach to address this concern is to decentralise the security analytics process and engage anti-adversarial AI techniques towards more robust models. Decentralisation will leverage edge/fog computing assets as well

as federated AI techniques to distribute both the storage as well as the processing of data. Use of XAI also gives to the human operator can directly align the operations with privacy constraints.

5.3.2 Privacy concerns in the slicing and security orchestration processes

Network Slicing allows for the creation of multiple end-to-end logical networks with specific requirements to fit the different needs of verticals. Network slices traverse a heterogeneous infrastructure, comprised of physical and virtualized computing, storage and networking components. Confidentiality, integrity and availability dictate the isolation of the network slices, the level of which depends on the slicing requirements and its intended usage. Isolation may vary from strict isolation to the need for inter-communication between slices. Thus, it becomes imperative to identify the needs of the underlying applications and impose security measures that isolate the slice components boundaries, preventing the lateral movement of attackers to other network slices.

Knowledge regarding slice topology information, such as which Network Slice Component (NSC) belongs to which Network slice, is valuable information for attackers that aim to attacks NSC of deployed slices. Using certificate-based mutual-authentication, NSCs exchange secure information between other peers. An attacker may take advantage of such protocols by posing as a legitimate NSC and then initiate the authentication process to source certificate issuer data [222]. An attacker with access to multiple authentication messages can derive the network slice topology. As a result, the privacy of end users and infrastructure providers can be infringed.

5.3.3 Privacy concerns in infrastructure and service attestation and integrity check procedures

Compromised IT devices can lead to user privacy violations, network security damage, or personal security threats. In this historical situation, Remote Attestation (RA) becomes a valuable security service that outsources the computing and verification load to another source, such as a server. Makes it easy to run on devices such as IoT devices that were created to simplify our way of life and can hold our private information and are, therefore, a good source of attack and intrusion. Devices have remote control interfaces that are attacked through these connections. Since most of these devices are cheap and low-end, they have problems with not having complex calculations. The malware present in the attacked devices will bring risks for the users and the network and may secretly provide the users' information to a third party. This issue becomes especially important when we talk about national defence, health systems, and industrial processes.

RA procedures are such that the decision-making party (verifier) evaluates the other party's situation (prover). A trusted person verifies the cloud server, which does not require any significant changes to the audio devices [223].

RAs are divided into three categories: 1) based on software, 2) based on hardware, and 3) hybrid. Software techniques exploit the computational limitations of devices. These techniques do not require any hardware and are very suitable for low-cost devices, however, they are vulnerable to complex and physical computing techniques.

Hardware techniques have little computational complexity, but as far as we know, most IoT devices are very cheap and cannot support this type of hardware machine.

A Hybrid technique provides a solution with less computational complexity and the use of minimum hardware suitable for low-end devices. This solution can support high computing power with very low energy consumption. Its working method is as follows. According to Figure 9, the verifier sends a challenge to the prover. Using the challenge, the prover calculates a hash of the contents of its memory and returns a checksum to the verifier. The verifier uses a checksum to determine whether the verifier is compromised. However, calculating the hash summary of the entire memory is a computationally intensive operation. In this method, the verifier sends a challenge to the prover, and the prover uses the challenge to randomly sample its memory. These random bits are then sent to the verifier. The verifier uses a stored state of the prover's memory to perform a random sampling of bits. The confirmation bits sent by the prover (σ) are compared with the confirmation bits generated by the verifier (σ∗). Following this scheme, confirmation is accepted [224] if σ = σ ∗

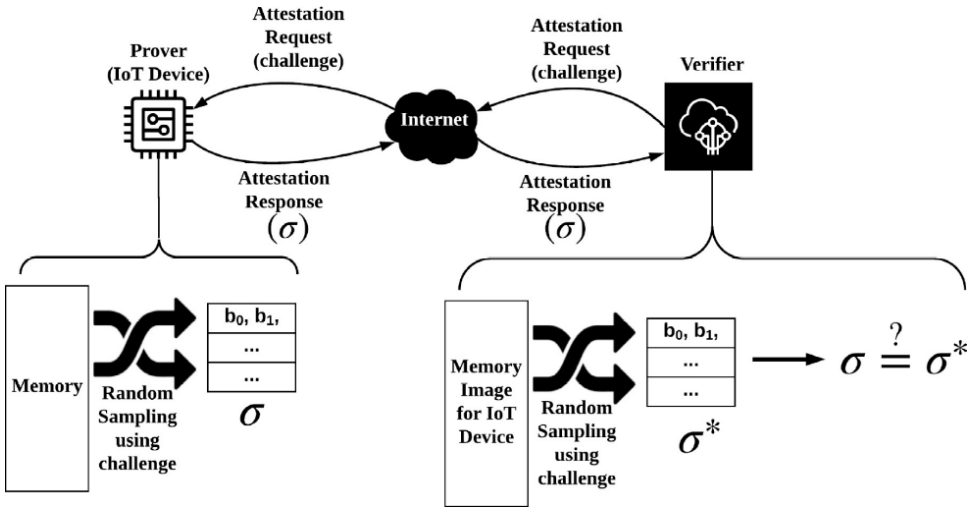

Figure 9 Hybrid technology attestation [223]

Network infrastructure is considered the backbone of operations and providing services to customers. Compromising the integrity of nodes in network infrastructure

such as virtual network devices in infrastructure-as-a-service clouds or even sensor nodes in a smart energy grid can have a tremendous impact on the reliability of this system and a devastating impact on the industry. Remote attestation schemes traditionally focus on verifying the integrity of a single node and providing evidence of its current state to the remote verifier.

However, attestation techniques may bring privacy issues. In the hardware-based approach, neighbouring groups learn the authentication result of previous groups, this can be problematic in terms of transmitting reliable information to other nodes, and as a result, Verifier receives the certificate that, if a malicious node injects, the injection results will not be correct [225]. It is difficult for any verifier at risk to infer any meaningful information about the state or configuration. It is essential to ensure not only the security of the main host and other hosted nodes but also their privacy and confidentiality. An attacker should not be able to obtain information about the configuration of the loaded nodes [226]. Therefore, a method for relaying certificate results without knowledge of network interface groups is beneficial to improve the privacy of an authentication scheme [225]. We can no longer rely on the perimeter security of systems only through firewalls and PKIs. Technologies such as trusted computing are explicitly designed to address points of device identity and integrity and have a special place in protecting devices. This would at least allow us to establish the origin, identity, and integrity of such components throughout the supply chain and at runtime with remote verification [227]. One such approach involves primitive cryptography that preserves privacy and hides information from potential adversaries. Direct Anonymous Attestation (DAA) is one of the most common encryption schemes based on anonymous credentials and group signatures [225].

One way to use signature schemes and zero-knowledge proof protocols is to convince neighbouring provers that the network structure is unknown, but the true structure is not revealed to other provers because a malicious prover who is in the vicinity of a number from other groups, can discover the network structure from the verification results of other groups. This method ensures that the verifier also does not know the network structure from the results collected from the network groups [225].

How can a prover prove its integrity without revealing any information about the configuration of its software stack? One overarching approach, which is the bedrock of the presented work, is to have a centralized entity (e.g., orchestrator in charge of deploying and managing the lifecycle of nodes) that determines what is correct and what is not, and then have that party setup appropriate cryptographic material (i.e., restrained attestation keys) on each node in the network and distribute them to all neighbouring nodes. The ability to then use such restrained keys is physically “locked” from the node until the node can prove its correctness - supply correct

measurements that will “unlock” its usage. Once released, the node can use the key to sign nonces supplied by the surrounding verifiers, acting as verifiable statements about its state so that other components can align their actions appropriately and an overall system state can be accessed and verified. Similarly, if verifiers receive no response or the signature is not produced using the key initially agreed upon and advertised by the centralized entity, they can justifiably assume that the prover is untrusted. Note that verifiers need only to know that the prover is in an authorized state, not what that state is. However, one main challenge of such approaches is the strong link between the restrained cryptographic material and the specific Configuration Integrity Verification (CIV) policies: Whenever an updated policy must be enforced, due to a change to the configuration of the overall system, a new attestation key must be created. Managing and updating such symmetric secrets creates an overwhelming key distribution problem [226].

Another way proposes a remote attestation security model based on a privacy-preserving blockchain. This approach is called the RASM. The remote attestation security model based on a privacy-preserving blockchain involves two stages. The first is reliable identity authentication and the second one is using calculation nodes to make decisions and accounting nodes to inscribe the data blocks [228].

Opera is an open platform for remote attestation based on Intel-SGX, where it seeks to achieve the following goals to achieve privacy: information about these approved enclaves (a trusted execution context that protects code and data against physical and software attacks [229]) and their developers is only available for SGX [230].

GS-Ram is a remote authentication solution using group signatures on centralized networks. This mechanism is proposed to preserve privacy and ensure authenticity, which has features such as unforgeability, anonymity, traceability, and security [231].

5.3.4 Privacy concerns in cyber threat intelligence (CTI) sharing

The timely exchange of cyber threat information, including zero-day vulnerabilities and threat insights or related information, using sharing platforms such as Malware Information Sharing Platform (MISP), is of utmost importance for improving the detection and response capabilities of 6G stakeholders.

Still, privacy concerns are common in Cyber Threat Intelligence (CTI) sharing, holding organisations back from sharing threat intel, especially if they are associated with sensitive data. A possible concern for organisations is that when they share that they identified a specific information of a specific threat, that may mean that the organization suffered such an attack. If such attack is, for instance, platform specific, it would also mean that the organization uses such platform, increasing its public exposure, once again. Possibly even making it a future target for attacks that for that platform.

Another candidate concern that may lead to reduce the sharing of CTI is the related to the ones having access to the information. If the CTI is publicly shared, on the one side, it would have a better and faster impact on its identification by others, on the other, such information could also be exploited by the attacker. For instance, an attacker could use such public sharing of CTI to understand if the attack has been detected. If the CTI is only shared within a selected community, there can also be the case that a member of the community has been compromised by the attacker with the specific interest of accessing the shared information. Such would classify as a supply-chain attack, nowadays more common [232].

Looking at CTI sharing from the perspective of individuals that do not have cybersecurity monitoring and response teams in place, such individuals would have a lot to gain from CTI sharing. Nonetheless, similar privacy-related problems arise. An attacker could generate attack traffic or patterns to a specific user and, by monitoring its public CTI sharing messages, could determine all CTI shared from a specific user, and thus break its privacy.

A candidate solution to mitigate this problem would be to pursue a mechanism that encrypted data before sharing it but still enabled search operations to be performed over the encrypted data. Moreover, if the CTI information that is to be shared is all encrypted, a central service can be built so that such information is easily accessible, confidential but still searchable and useful. A similar approach is proposed by Fernandes et al. [233].

5.3.5 Privacy-aware network slicing and orchestration

In the 6G context (like its 5G predecessor), network slicing permits to launch different virtualized networks, where each such network paradigm imposes versatile network services from the physical network hardware. Via the recent incorporation of SDN and NFV technologies, it has been made feasible to segment unary network connections into multiple virtual distinct lines. Network slicing offers virtual applications that are instantly directed to user's service delivery. As a desirable outcome, cellular-driven business applications that are being deployed on slices possess massive-scale connections and extremely low latency services with high user quality of experience. The ultimate benefit of network slices, for 6G, is that it adds network automation (zero-touch) and is able to reduce network complexity via complicated virtualization techniques. However, such functionalities include new slice creation, removal, attachment, and dynamic configuration, and dynamic wireless resource sharing, for this purpose security and especially privacy concerns emerge as of paramount importance. *Privacy-awareness in network slicing and orchestration should come along with user Trust, Transparency and explicit privacy, or anonymity preservation*.

Traditional multi-domain network slice architecture orchestration lacks privacy constraints considerations. For instance, all these 5G and beyond solutions rely heavily on a centralized authority, to intershare complete network resource information. *However, in real 6G network conditions network and cloud operators are not willing to disclose their private network resource information such as network monitoring traffic, OPEX/CapEx costs and customer billing, which may allow their competitors to find estimations on their future bidding prices.* Moreover, the most essential element under threat is the slice privacy itself, as the particular centralized actor is a single point of attack and technical failure. To be objective in this section, we need not to underestimate the fact that multi-domain network slicing relies for all network administrative domains to transparently share their network status information, *thus lack privacy considerations*. Privacy-awareness in 6G network slicing and orchestration comes together with the *least* user information leakage. Further solutions, such as *Trusted Execution Environments (TEE) to guarantee the information privacy and a distributed enclave key generation system to produce enclave keys are mandatory for privacy-aware 6G slicing orchestrators.* Other mitigation points to ensure privacy under strict virtualization scenarios in 6G will be, in the near future, hardware-enabled technologies like Intel SGX, and Multi Party Computations (MPC). MPC (also known as *secure computation*, *multi-party computation* or *privacy-preserving computation*) is a subfield of cryptography with the goal of creating methods for parties to jointly compute a function over their inputs while keeping those inputs private. Unlike traditional cryptographic operations, where cryptography assures security and integrity of communication or storage and the malicious actor is outside the system of participants (an eavesdropper on the sender and receiver), the cryptography in this model protects participants' privacy from each other.

There exist quite recent research efforts to ensure privacy aware slicing in 6G networks by leveraging the Blockchain and Federated Learning. Specifically, in [234] the Authors are addressing privacy reassurance inside deep network slicing with context-based authentication, and secure handover schemes by using the Markov decision making (MDM) and weighted product model, adjacently. To invoke further privacy constraints to the SDN controllers and switches, the Authors suggest intruder packets classification and packets migration through hybrid neural decision tree (HyDNT) and Hybrid Political optimizer together with a Heap-based Optimizer (HPoHO). In [179] the Authors incorporated a consensus ready scheme for a multidomain network slice orchestration framework for data consistency, scalability, and security. Their results seem promising in terms of guaranteeing users' data security and privacy with high throughput and low latency. Finally, in [236] they focused more on blockchain-based optical network slicing scheme mainly for IoT applications. User's data security and trust issues are maintained especially during complicated and high-quality slicing transactions.

5.3.6 Privacy SLAs As-a-Service (PAaS)

As mentioned in the earlier subsection, there is an operational trade-off between information disclosure from cloud operators and privacy levels. Hence, such often (undesirable) information disclosure tends to compromise more or less *slice domain privacy*. For example, the information about the residual capacity of virtualized servers can be misused for DDoS attack, predicting business policies, bidding competitor prices etc. Thus, we should be referring to the concept of the *exploitation or not of the domain privacy*.

Quantitative evaluation of privacy preservation is critical for developing secure and efficient methods for multi-domain coordination, slice orchestration and eventually delivering the concept of Privacy SLA across the whole 6G infrastructure – As-a-Service; from the fully-shared virtualized infrastructure versus the dedicated virtual machines versus dedicated hardware. *Each specific network resource will obtain different, yet still privacy aware, PAaS. Since* multi-domain coordination is crucial for efficient 6G network slicing and orchestration, we need to *(1) privacy issue multi-domain QoS routing, (2) use only aggregated topology information and (3) hide the network performance data. To measure privacy metric as an SLA we need to define an ad-hoc metric for the slicing method.* The privacy gain is quantitatively evaluated by deriving a new metric called the *Privacy Index (PI)* based on the actor-community model. For the scope of PRIVATEER and to produce this exact PAaS SLA guarantee(s) our goal should be two-fold: (1) to be able to achieve high privacy, we must maximize PI for (Multi-Domain Service Function Chaining (SFC) MD-SFC orchestration while, at the same time, satisfying the basic resource constraints for SFC deployment, and (2) to minimize the average response time of MD-SFC orchestration for faster deployment of SFC. Sub-goals will include *defining privacy-aware MD-SFC orchestration*, *abstracting the network topology*, and abstracting the resource availability information via a lightweight solution framework.

6 Gap Analysis

There are significant gains to be reaped by the users of B5G technological advances. As a prime example, the automotive industry is set to benefit significantly from the implementation of 5G and 6G technology. While 5G technology promises to revolutionise the sector with faster data speeds, lower latency, and connected cars, 6G technology is expected to bring even greater capabilities. This gap analysis will explore the numbers behind what is missing from the 5G technology that 6G can implement and what potential new gaps may arise with 6G.

One of the most significant advantages of 6G technology is its ability to provide much faster data speeds and lower latency than 5G. While 5G promises to deliver data speeds of up to 10 Gbps, 6G technology could provide speeds up to 1 terabit per second (Tbps), a 100x increase. This increased speed could enable real-time communication between vehicles and infrastructure, making it easier for cars to coordinate with each other and avoid collisions. Additionally, 6G technology could provide a more reliable and secure communication network, which is essential for safety-critical applications such as autonomous driving.

Moreover, 6G technology will be able to support more complex and sophisticated communication protocols. 6G could provide support for up to 10 times the number of connected devices as 5G, up to 10 million devices per square kilometre. This in turn could enable more advanced features such as predictive maintenance, where vehicles can anticipate and address potential maintenance issues before they become serious. Additionally, 6G technology could provide better support for artificial intelligence and machine learning algorithms, allowing vehicles to make more accurate predictions and decisions.

However, there are also potential gaps that may arise with 6G technology. One of the key challenges is developing the necessary infrastructure to support it. While 5G is still being rolled out in many parts of the world, 6G is in the early stages of development, and it may be some time before the necessary infrastructure is in place. As such, it is crucial to ensure that investments in 6G infrastructure are made to support its widespread adoption.

Another potential gap is the need to develop new security protocols to protect the growing number of connected devices in the automotive industry. As more vehicles become connected and communicate with each other, the risk of cyber-attacks also increases. Therefore, it is essential to develop robust security protocols to protect against these threats.

6.1 5G vs 6G Security Gap Analysis

According to the current research and studies about the security and privacy risk in 6G, all agree that the more complex the networks are, the more the related risks we will face, an even more due to the increased in connected devices, novel technologies and services to the users.

In the research paper "Security and privacy for 6G: A survey on prospective technologies and challenges" [6] they summarized some prospective technologies for enhancing 6G security and privacy toward the 5G along 5 main criteria of automation, trustworthiness, privacy, reliability, and openness, as illustrated in the following figure:

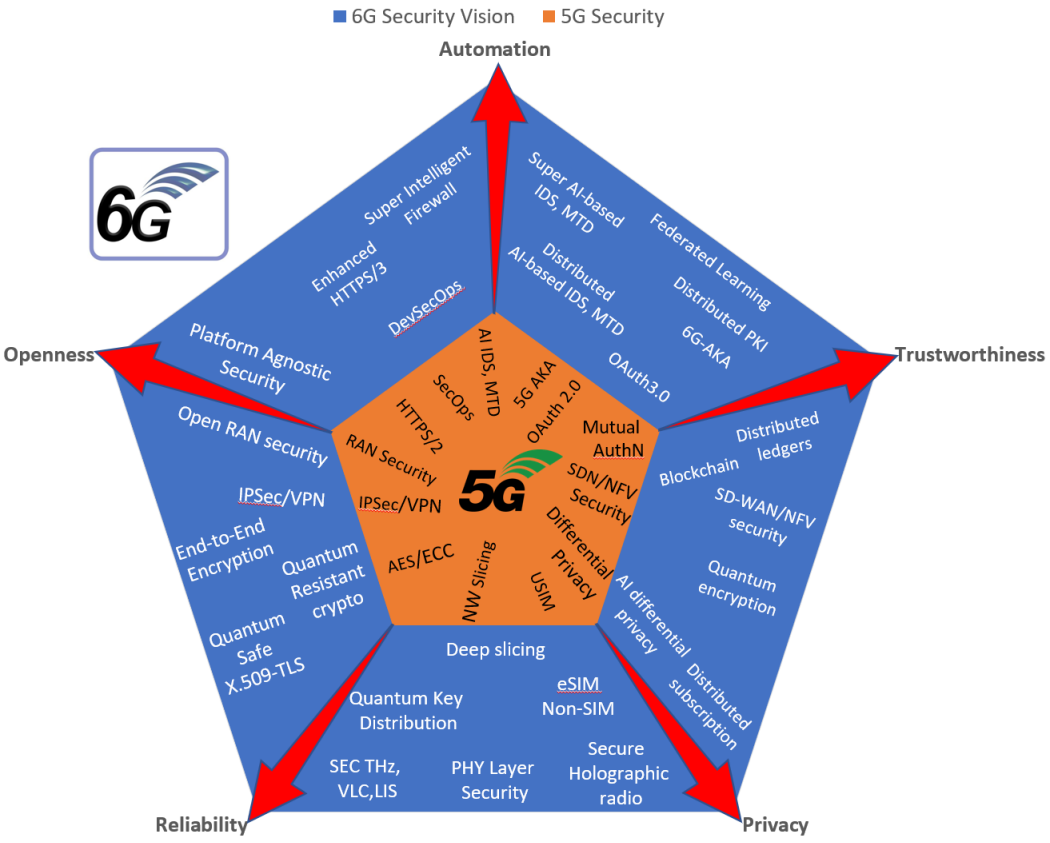

Figure 10.11 6G vs 5G Security evolution

The farther away from the centre of the picture a technology is, the more mature and applied it will be. One example is about the quantum-safe TLS protocols, before they fully operate, a temporary quantum-resistance ciphersuites period can be reasonably envisioned.

Some of the envisioned security technologies are still in a research phase or just theoretics, others are already in PoC or testing phase.

The following table summarizes a gap analysis vision between the 5G and the potential changes of 6G security and privacy technological solutions to mitigate the main threats to the Connection and Service Layer.

Table 13. GAP Analysis 5G vs 6G main Threats and Technologies for mitigation [6]

6G Layer	Security Domain	Securiy & privacy issues	5G mitigation solution	6G mitigation solution	Open challenges	References
Connection Layer	Network access authentication	Impersonation attacks SUPI/identifier exposure	3GPP: 5G-AKA Non-3GPP: EAP-TLS 5G USIM, SUCI/SUPI	3GPP: 6G-AKA Non-3GPP: Quantum-safe EAP-TLS 6G nuSIM/non-ID	-Many components of 6G remain undefined so no clear relationship among stakeholders. -System-on-Chip SIM (nuSIM) integration and non-SIM model are still under development	[9], [7], [8]
	Signalling data encryption	Man-in-the-middle Eavesdropping Tampering traffic Data leakage	128-NEA1/128-NEA2/128-NEA3 128-NIA1/128-NIA2/128-NIA3	256-NEA1/256-NEA2/256-NEA3 256-NIA1/256-NIA2/256-NIA3 (Quantum-safe support)	-Heavy computation, energy consumption	[10], [11], [12]
	Transport security protocol	Man-in-the-middle Data leakage	TLS 1.2/1.3	Quantum-safe TLS (AES-256) Quantum key distribution (QKD)	-Heavy computing if using for user data plane -Quantum-based technology remains no explicit economical gain for now.	[13], [14], [15]
	Interconnection security	Man-in-the-middle Data leakage	SEPP with HTTP/2 and TLS 1.3	SEPP with HTTP/3 and Quantum-safe TLS	-Heavy computing if using for user data plane -Quantum-based technology remains no explicit economical gain for now.	[16], [17]
	Trust networks	Compromised/insider attacks Data leakage	Blockchain/Distributed Ledgers supported in several applications	Blockchain/Distributed Ledgers widely used in many applications	-High energy consumption -High complexity -Vulnerable to 51% attacks -Select proper DLT Solution	[18], [19], [20]
	Network management	DoS attacks Network topology leakage	SDN security	SD-WAN security, Full Decentralization	-The risk of centralized SDN control	[21], [22], [23]
	Network isolation	DoS attacks	Network slicing	Deep slicing, Slice Management Service Authorization Procedure	-Heavy computing to manage massive slices -High expenditure and energy consumption.	[24], [25], [26]
	Endpoint/network nodes	DDoS attacks Adversarial attacks Traffic meta profile	Firewall/IDS/MTD	AI-empowered Firewall/IDS/MTD	-Breakthroughs in AI -High computing Adversarial defence	[27], [28]
Service Layer	Service authentication	Credential exposure Unauthorized access, personal info leakage Impersonation Biometric data leakage	Public key infrastructure (PKI) 5G AKA for applications Face ID, Touch ID	PKI with quantum-safe algorithms PKI with blockchain 6G AKA for applications Face ID, Touch ID, IRIS, Heart rate, brain signal ID (Biometric AuthN)	Under trials, no standard till now Efficient cooperation between network operators and service Providers Biometric data protection	[29], [30], [31] [32] [33], [34], [35]
	Application protocol	Man-in-the-middle Fingerprinting a specific client	HTTP/2 over TLS 1.2/1.3 HTTP/3 over QUIC	Enhanced HTTP/3 over QUIC	Update many deployed security infrastructures such as load balancers	[37], [16]
	Service authorization	Flawed redirect Access code leakage	OAuth 2.0	OAuth 3.0	The proof-of-concept is still under development	[16], [36]
	Software security	API vulnerabilities, Data breach	Container-based security	Platform-agnostic security	Security features can synchronize to support different devices	[40], [41]
	Secure computation	Data breach	Homomorphic encryption	AI Gradient Compression AI homomorphic Encryption, perturbation, differential privacy Quantum homomorphic encryption	High computation, data mining performance degradation	[38], [39]
	Security service	Malware/Virus/spam Deepfake	Cloud security-as-a-service (SECaaS)	Enhanced AI-empowered SECaaS Everywhere	Support interoperability	[42], [43]

The 6G physical layer was not part of the above gap analysis table because it is expected to adopt many novel technologies that can bring with them possible directly related threats as discussed in chapter 4.1, a direct gap analysis with the 5G was not possible.

As high-level takeaways of this TL for the **physical layer** it is possible to summarize that the new envisioned technologies are susceptible at least in the same measure as the 5G to Eavesdropping and Jamming attacks, and have a **higher Location Exposure risk** toward 5G for the users.

About the AI Layer, many studies also indicate the AI as the game changer for enhancing 6G security with respect of previous technologies, 5G included.

The following table illustrates, as the outcome of different studies, how the future AI can aim to improve security for enabling technologies in **Physical**, **Connection** and **Service** layers with a gap analysis between 5G and 6G:

Table 14. GAP Analysis 5G vs 6G main Security Threats and Mitigation in PHY, Connection and Service layer [6]

6G Layer	Securiy & privacy issues	AI-based defense methods	5G	6g "vision"	Open challenges	References
Physical Layer	-Eavesdropping, jamming -Location tracking -Compromised IoT devices	> Channel coding -Signal detection in PLS -CSI estimation in PLS -Beamforming alignment -Mis-behaviour detection -Anti-jamming -Physical layer authentication	SVM, CNN, LSTM, DNN, RL, DRL, Autoencoder, Deep autoencoder, RNN, RBM	*-More generative learning Meta learning, Deep RL, Experienced DRL, Deep Convolutional GAN, Causal Learning, Adversarial training* *-More large-scale learning Distributed Learning Federated Learning Transfer Learning* *-More explainable learning* *-Toward end-to-end learning Deep autoencoder* -	-High computing/ training cost -Lack of physical-based datasets -Energy efficiency -Realtime processing -Reliable signal generation	[44], [45], [46], [47], [48], [49], [50], [51]
Connection Layer	-Man-in-the-middle -DoS, DDoS attacks -IP Spoofing -SDN controller attacks -Traffic trace	>Risk-based authentication -Network intrusion detection -Deep packet inspection (DPI) -Protocol vulnerability detection -Encrypted traffic inspection -Proactive intrusion prevention	CNN, DNN, RBN, Autoencoder, LSTM, RBN, DBN, RL		-High computing/training cost -Online learning -Real-time processing -High generative learning	[52], [53], [54] [55],
Service Layer	-Malware/virus/ spam -NFV and VNF attacks -Malicious microservices -Data breach	>Biometric authentication -Anti-virus/malware detection -Trusted program verification -Trusted updates verification -Edge/Cloud control verification -Container/Runtime protection	CNN, DNN, LSTM, DNN, DBM, RBM, Autoencoder Deep RL		-High computing/training cost -Massive surveillance -Bias learning -Lightweight model for IoT devices -Vulnerable to AI-targeted attacks -High generative learning	[56], [57], [52], [55]

Physical layer security (PLS), Support Vector Machine (SVM), Convolutional Neural Network (CNN), Long-Short-Term Memory (LSTM), Reinforcement Learning (RL), Autoencoder, Deep autoencoder, Recurrent Neural Network (RNN), Restricted Boltzmann machine (RBM), Deep Neural Network (DNN)

6.2 5G vs 6G Privacy Gap Analysis

Privacy Enhancing Technologies (PETs) [58][59] is a term for set of novel techniques to address the privacy concerns and the main ones are namely:

- differential privacy [69]
- homomorphic encryption [70]
- secure multi-party computation [71]
- confidential computing [72]

PETs are used to bring advanced solutions for challenges that cannot solely be handled by classical privacy techniques, such as anonymization or consent mechanisms.

PETs are based on privacy preservation methods, which are techniques and practices used to protect the privacy of individuals by preventing the unauthorized or unwanted disclosure of their personal information. The goal of privacy preservation methods is to limit the collection, use, and dissemination of personal information to only what is necessary and with the explicit consent of the individual. Essentially, privacy preservation exists to answer to a specific question: “Who is the entity you can trust in sharing your sensitive data?”.

Generally, in the specialistic literature three methods are identified:

- Trusted: in such case, the idea behind trusted methods is that users can entrust their personal data to a third party that is responsible for ensuring the privacy and security of that data by managing and protecting their personal information. Usually, trusted methods are applied in situations where individuals may not have the expertise or resources to manage their own privacy, or where, of necessity, to rely on a trusted entity to provide a service or product.
- Untrusted: conversely, those are techniques designed to protect the privacy of users' data while not requiring the users to trust any third-party entity or authority. Thus, users should be able to protect themselves from any misuse or leak. They are the only entities that they can trust, and, generally, untrusted techniques are methods directly implemented by users without the help of a third party.
- Semi-Trusted: techniques and practices used to protect the privacy of individuals when some level of trust exists between the data provider and the data processor. These practices are based on a distributed trust model functioning through specific protocols [106] with some level of data sharing or collaboration between multiple parties. Another example is the so-called differential privacy, in which users are eager to provide data to a server running the algorithm for the dataset. The “untrusted” part of this process

comes from the output of the algorithm since any personal information related to the user's sensitive data should not be publicly released.

Focused on PETs, the table below builds frames the abovementioned privacy preservation models to present a comparison between 5G and 6G privacy differences:

Table 15. GAP Analysis 5G vs 6G main Privacy Threats and Mitigation in PHY, Connection and Service layer [6]

6G Layer	Feature method	Model	5G mitigation solution	6G mitigation solution	Open challenges	References
Physical Layer	Authentication	Untrusted	Radio fingerprinting	-Physical layer authentication (AI-empowered)	Location exposure Experience degradation	[56], [34]
Connection Layer	Communication anonymization	Trusted	-Proxy servers	-Proxy servers	IP exposure at fake proxy	[58]
	Pseudonymization	Trusted	-IMSI/GUTI/SUCI -Blockchain networks	-SUCI, Non-ID -Blockchain/ Distributed ledger with Smart Contracts	Complicated management Energy consumption	[60], [20], [61]
	Data anonymization	Trusted	-Randomization -Generalization	-Enhanced anonymization (AI-empowered)	Complexity to implement for large-volume data	[62]
Service Layer	Differential privacy	Semi-trusted	-Laplace mechanism	-Enhanced differential privacy (AI-empowered)	Challenge detecting changes of particular values	[63], [64]
	Homomorphic encryption	Semi-trusted	-Homomorphic encryption	-AI Gradient Compression, AI homomorphic Encryption, perturbation, differential privacy -Quantum homomorphic encryption	Complexity, high computation	[65]
	Group-based signatures	Semi-trusted	-Attribute-based signatures	-Group-based signatures	Can identify user if few participants	[58]
	Self-destructing data	Semi-trusted	-Self-destructing data	-Enhanced self-destructing data	Only apply for specific applications	[66], [58]
	Data masking	Semi-trusted	-Substitution, Shuffling, Nulling out, Encryption, Character scrambling	-Enhanced data masking (AI-empowered)	Privacy-data utility trade-off, traffic overhead	[66], [58]
	Secure Multi-Party Computing	Untrusted	-Federated learning	-Federated learning -Distributed learning	All participants need to be present, High vulnerable to collusion attacks	[67], [68]
	Data perturbation	Untrusted	-Probability distribution -Value distortion	-Enhanced data perturbation (AI-empowered)	Traffic overhead	[58]

7 Elicited Use Case Scenario

This section briefly overviews the initial evaluation scenarios already identified in the Grant Agreement, grouped in two high-level use cases/domains: ITS and Smart City. The aim of this scenarios will be to unveil the actual value of the project results, against actual stakeholder needs and requirements. Each scenario is mapped to the security and privacy threats identified earlier in this document.

The scenarios will be expanded and re-shaped during the first phase of the project and the revised set will be documented under D2.2 (Use cases, requirements and design report).

7.1 ITS context

7.1.1 Edge service compromise

Edge computing poses significant security risks, particularly when it comes to data management. Since devices interacting with the network may not be fully secured by the network, they may be compromised, which could lead to network compromise as well. Edge computing requires that devices manage sensitive data, and without adequate security measures, this data may be vulnerable to attack. In addition, edge computing may be at a higher risk of physical security breaches since devices may not be adequately secured or accessible only to authorized personnel. Logical security measures such as strong authentication and authorization controls and data encryption in transit and at rest can help mitigate some of these risks.

Moreover, the integration of edge, fog, and cloud computing in the 6G-V2X network can also pose significant security risks. The fast-changing vehicular network and communication conditions can lead to degraded performance, making it challenging to train ML models. Local training of ML models is a potential solution, but privacy concerns arise when base stations and vehicles share training samples. Federated learning has emerged as a potential solution to address privacy and communication overhead issues associated with training ML models. However, it is still a relatively new technique and requires careful consideration to ensure that the benefits outweigh the risks. Overall, it is critical to implement robust security measures to mitigate the risks associated with edge computing and its integration with other computing technologies.

Following a possible Use Case scenario with its main threats and mitigations to be validated:

A Service Provider has deployed a 6G network slice across a highway for the needs of the road operator, including low-latency edge functions for assisting automated driving. By exploiting an unknown vulnerability in the edge functions, an attacker

manages to hijack them and obtain access to a central database, accessing sensitive vehicle data. In the SP Security Operations Centre, the rule-based detection workflows fail to detect the stealthy attack; which is, however, detected as an anomaly by the PRIVATEER distributed security analytics mechanism, running at each edge node and leveraging the AI accelerators for reducing the inference time. By inspecting the Explainable-AI-generated reports, the SP security operators quickly identify the breach and its cause, apply remedial actions to the network slice by temporarily deactivating the compromised service and inform the road operator accordingly. At the same time, they will want to share Cyber Threat Intelligence (CTI) concerning the attack but, on the other hand, want to stay anonymous and not disclose the identity of either the SP or the user (road operator); the consequences of such attack may affect e.g. QoS agreements with other SPs. For this purpose, they leverage the privacy-friendly CTI sharing mechanism of PRIVATEER and communicate the threat without exposing sensitive information. This would allow the user (road operator) to make informed decisions on the exploit, for instance disabling sensor sharing to ensure the safety of road users.

Threats associated with the scenario:

- Disclosure of sensitive information
- Data manipulation
- DoS
- Safety implications

PRIVATEER framework solution:

- Decentralised Security Analytics
  - AI Accelerators
  - exAI
- Privacy-friendly CTI sharing

7.1.2 Privacy-friendly security service orchestration for logistics

One of the risks of supply chain orchestration is the potential for data breaches and cybersecurity threats. The integration of various systems and software may create vulnerabilities in the supply chain that can be exploited by malicious actors. This could result in the theft of sensitive information, disruption of operations, and financial losses. Additionally, the use of AI and ML could also pose privacy risks if personal data is not properly secured.

Therefore, it's crucial to prioritize privacy-friendly security measures in supply chain orchestration. This involves implementing robust data protection policies and using secure communication channels. It's also important to ensure that all third-party vendors and partners comply with privacy regulations and standards. Encryption and access controls can further enhance the security of sensitive information. By

implementing these measures, companies can minimize the risks of data breaches and cybersecurity threats while still reaping the benefits of supply chain orchestration.

Following a possible Use Case scenario with its main threats and mitigations to be validated:

A big cargo company needs to lease a 6G network slice for assisting its logistics operations, orchestrating distributed resources at the network core, public and private edge (at its warehouse). The slice will include also virtualised security functions in order to harden the service chain. The company needs distributed security, while also ensuring the privacy of its communications. It uses the PRIVATEER privacy-preserving slice orchestration mechanism to orchestrate the slice resources across heterogeneous domains with varying levels of trust, and place the more critical service components on the most trusted infrastructure segments. It also employs the PRIVATEER proof-of-transit mechanism to verify that the traffic is not diverted to an untrusted component by malicious action and to ensure secure communications with the clients of the cargo company.

Threats associated with the scenario:

- Disclosure of sensitive information
- Data manipulation
- Service availability / QoS

PRIVATEER framework solution:

- Privacy-aware slice orchestration
- Proof-of-Transit

7.1.3 Verification of mass transportation application

On a possible use case for the apps related to mass transportation is the use of electronic payment technology in public transportation systems has led to concerns about privacy and security. The current systems require passengers to sacrifice privacy in order to take advantage of the convenience of electronic payment. As systems migrate from contact-based technologies to contactless ones, there is an increased risk to privacy and security due to the inherent broadcast nature of radio frequency (RF) technology.

Passive RFID transponders, which are used in electronic ticketing systems, are severely resource-constrained computing devices, with limited memory and processing power. This makes it difficult to implement secure communication protocols between the transponder and the reader. Despite these limitations, recent advances in cryptography have made it possible to develop new cryptographic primitives suitable for these resource-constrained devices. The key management

problem for a transit system involving hundreds of readers and hundreds of thousands of tickets has traditionally been difficult. Recent advances in re-encryption and re-signatures have been used to address this issue. However, the risks associated with the verification of mass transportation applications include privacy concerns, security vulnerabilities, and the challenges of managing large-scale systems.

Following a possible Use Case scenario with its main threats and mitigations to be validated:

A mass transportation company has leased a multi-domain 6G slice in order to operate a distributed application -at the core and the edge- for supporting its transportation services. The integrity of the application, as well as of the underlying infrastructure, is of utmost importance for the safety of the passengers. The SP operating the network performs periodic remote attestation of the network service (software) and the infrastructure (hardware); upon successful attestation, it issues verifiable credentials which the infrastructure operators present to the end user (transportation company) upon request, without disclosing sensitive details about the attestation and verification process. In case of integrity violation, the incident is reported using the privacy-preserving CTI sharing feature, thus keeping sensitive information confidential.

Threats associated with the scenario:

- Disclosure of sensitive information
- Data manipulation
- Safety implication

PRIVATEER framework solution:

- Distributed identification and attestation
    - Trusted Platform Secure Identification
    - Code / data integrity and authenticity verification
    - FPGA Accelerator
- Privacy-friendly CTI sharing

7.2 Smart City context

7.2.1 Onboarding of a “neutral host” edge network

Following a possible Use Case scenario to address the “neutral host” model, with its main threats and mitigations to be validated:

A municipality has just installed a new network of “smart lamps”, consisting of multi-tenant edge nodes and microcells. The municipality intends to offer this network

(under the “neutral host” model), as a shared access infrastructure to be leased by multiple Service Providers. The municipality requests a full integrity check and certification of its infrastructure. Due to an outdated firmware of some of the smart lamps, an attacker exploits a discovered vulnerability and obtains access to the infrastructure.

Threats associated with the scenario:

- Disclosure of sensitive information during the integrity check
- Damage to the neutral host’s reputation due to the breach
- Disruption of the services already running on the infrastructure
- Failure to detect the breach

PRIVATEER framework solution:

- Decentralised Security Analytics
- Distributed identification and attestation
- Privacy-friendly CTI sharing

7.2.2 Multi-domain infrastructure verification for 6G smart city app

Following a possible Use Case scenario to address the secure multi-domain infrastructure verification, with its main threats and mitigations to be validated:

A startup has developed an innovative smart city 6G application, for which a pilot deployment in two neighbouring cities is planned. The startup leases a multi-domain network slice across the two cities, which also makes use of the neutral-host infrastructure offered by the two municipalities.

Threats associated with the scenario:

- User traffic traversing untrusted nodes (resulting in eavesdropping/data leakage)
- Leakage of neutral host sensitive information during multi-domain orchestration

PRIVATEER framework solution:

- Distributed identification and attestation
- Privacy-aware slice orchestration
- Proof-of-Transit

8 Security/Privacy-related KPIs and KVIs for 6G

8.1 Related work to 6G KPIs/KVIs

Section 4 demonstrates that researchers are actively investigating innovative technologies to realize the anticipated capabilities of 6G networks. One critical area of research involves the development of Key Performance Indicators (KPIs) and Key Value Indicators (KVIs) for 6G networks, emphasizing security and privacy. This subsection offers an overview of relevant studies that contribute to the definition of 6G KPIs and KVIs, explicitly focusing on security and privacy aspects:

Hexa-X [258], [259]: As a flagship initiative for 6G technology, the Hexa-X project has proposed a comprehensive set of KPIs and KVIs related to 6G networks. The project has been instrumental in advancing the understanding and establishment of relevant KPIs and KVIs for the future 6G networks, addressing various aspects of 6G, such as network performance, security, and privacy. The KPIs and KVIs produced by Hexa-X serve as essential guides for evaluating the progress and effectiveness of 6G solutions in various domains, including network capacity, latency, and the critical areas of security and privacy.

White Paper "Beyond 5G/6G KPIs and Target Values", 5G-PPP [260]: In this white paper, the 5G Public Private Partnership (5G-PPP) presents the available Beyond 5G (B5G) and 6G Key Performance Indicators (KPIs) as of 2022, obtained from 5G PPP Phase III Projects. While the majority of these KPIs primarily focus on network-related aspects (e.g., area traffic capacity, bandwidth, latency), the paper also identifies three KPIs specifically addressing security and privacy concerns:

- *Anomaly detection precision*: This KPI measures the Precision-recall area under curve (AUC) with at least minimum scoring in precision and recall. The project that provided this set a target value of >0.85 with at least 85% scoring in both precision and recall.
- *Security conformance*: Conformance to security constraints. Network slice controller authentication. Date integrity of a network slice. No target value is provided, because the use of security or the violation of this SLO is not directly observable by the network slice consumer and cannot be measured as a quantifiable metric.
- *Tenant data privacy*: This is the amount of confidential information shared between the tenants and the infrastructure owner, needed to optimize performance of whole system. The target value is not provided.

White Paper "Beyond 5G, Message to the 2030s", Beyond 5G Promotion Consortium [261]: Japan's Beyond 5G Promotion Consortium (B5GPC) actively supports Beyond 5G (B5G) advancement by conducting relevant studies and identifying trends based on societal needs toward its commercialization in the 2030s. This White Paper delves into B5G concepts, requirements, and architectures considering key technologies and anticipated use case scenarios. Additionally, the Consortium proposes several KPIs, including target indicators for "Trustworthiness, Security, and Robustness":

- Cryptographic processing speeds exceeding the peak data rate (100Gbps and more)
- Support for 256-bit key length for post-quantum cryptography
- Instantaneous recovery from disasters and failures

Strategic Research and Innovation Agenda, Networld Europe [262]: Networld Europe is a European initiative that brings together researchers, industry professionals, and policy-makers to coordinate research efforts in advanced communication networks and services, such as 5G and beyond. Networld Europe published the Strategic Research and Innovation Agenda (SRIA) 2022, addressing various aspects of next-generation communication technologies in Europe, including system services, network and service security, radio access innovations, and future emerging technologies. The document also proposes representative KPIs in the field of Security, such as the "*Response time of protection and restoration mechanisms*," with a target value of below 1sec by 2025.

The roadmap to 6G Security and Privacy, Porambage et al.[250]: This paper discusses the potential security and privacy challenges and solutions in 6G wireless networks. The authors present the possible 6G threat landscape based on the anticipated 6G network architecture and examine security considerations associated with 6G enabling technologies, such as distributed ledger technology (DLT), physical layer security, and AI/ML, among others. They also share their vision on 6G security and privacy KPIs, including a guaranteed *Protection level* against threats and attacks, *Time to respond* against malicious activity, the *Coverage* of security functions over the 6G service elements and functions, *AI robustness*, *i.e.*, AI algorithms hardened for security, *Security AI model convergence time* (training time), *Security Function Chain round-trip-time*, referring to the time it takes for chained security functions to process, analyse, decide and act, and *Cost to deploy security functions*, measuring the cost of deploying security functions.

8.2 Security and Privacy KPIs/KVIs for 6G

This Section proposes representative KPIs and KVIs for 6G networks as a contribution to the SNS Programme, emphasizing Security and Privacy. As 6G is expected to

incorporate various advanced technologies, augmenting these KPIs with technology-specific indicators is essential. This will ensure that these emerging technologies are adequately assessed and integrated into the envisioned 6G architecture, providing robust performance, security and privacy guarantees. Table 15, at the end of this Section, summarizes the proposed KPIs.

8.2.1 Security-related KPIs for machine-learning models

In order to quantify how well intrusion-detection mechanisms work, a number of KPIs are typically defined. Firstly, the accuracy of threat classification models is measured and a reasonable reference value is greater than 80%. Moreover, *the number of false positives* and *false negatives* should be reduced to less than 10% in a federated scheme. Another aspect that is insightful regarding the security aspects of intrusion-detection and prevention systems is the mean time of detection: Two numbers can be measured, the *mean time to detect a threat* and the *mean time to classify* it. Both should be smaller than 10 seconds, which can be compared to the KPIs envisaged in previous projects [**https://www.palantir-project.eu/documents/project-deliverables/**]. Finally, for federated-learning schemes, the *accuracy loss* can be defined relating the centralised to the federated models, which is given by (1 – accuracy of federated model/accuracy of centralized model). This accuracy loss should be less than 10%.

8.2.2 Privacy-related KPIs for machine-learning systems

Differential privacy KPIs

Differential Privacy (DP) is a probabilistic privacy mechanism that provides an information-theoretic security guarantee. Given two neighbouring data sets D and D' differing by one record, differential privacy defines privacy loss of a randomized algorithm as its sensitivity on the datasets. Differential privacy and its variants guarantee the upper bounds on privacy loss of a ML model. Those bounds are affected by the DP mechanism applied to the algorithm, the iterations and complexity of the algorithm as well as the communication of the participants in the case of Federated Learning Framework.

DP may be accurately parametrised using two numbers (ε, δ), where ε describes the maximum distance between two data sources, and δ describing the probability of data being leaked accidentally.

Privacy guarantees come with utility trade-offs. Since more noise is needed to provide higher privacy guarantees, usually the performance of the models tends to deteriorate. A metric that has the capacity of tracking that trade-off is *Accuracy loss* [266] which is calculated as follows:

```
Accuracy Loss = 1 - (Accuracy of Private Model/Accuracy of Non-Private Model)
```

Another way to evaluate the privacy perseverance of a ML model is to evaluate *the success of adversarial privacy attacks*.

Such attacks are the following:

- Inference of Membership: Privacy attack that attempts to determine whether a specific individual's data was included in a dataset that was used to train a machine learning model. In this case we could use the reverse of the Adversarial Accuracy during Inference [265].
- Inferring properties of private training data (model inversion): The basic idea behind an inference of private training data attack is to use the trained model to infer properties of the training data, such as the distribution of the data. This can be done by analysing the output of the model and using it to construct a proxy for the training data. Most of the times this proxy is used to train meta classifiers, so one way that we could measure the adversarial success is by the Precision and Recall of meta-classifiers [264].
- Inferring Training Input & labels (reconstruction attack): These attacks aim to reconstruct the original training data samples and the corresponding labels. In this case we could measure the *MSE (Mean Squared Error) between a target and its reconstruction* [263].

Finally, for measuring quality/utility of data after anonymization usually a *quality loss* metric is employed, that measures how much quality is lost by reporting anonymised data instead of real data. It is the difference/distance between the anonymized data and the original data, and, therefore, data-type dependent (for example, for location data it could be the Euclidean distance between original data and anonymized data). The *accuracy loss* metric proposed above is equivalent, by measuring the accuracy loss of applying a private vs non-private model. It can be applied at the exit of the AI/ML mechanism, or at the exit of the anonymization mechanism (e.g., before data being fed to the AI/ML mechanism). Therefore, the *accuracy loss* serves as a general-purpose quality metric that can be used for both ML models as well as anonymization models.

Adversarial protection

As mentioned above, for privacy, adversarial protection comes with utility trade-offs. One possible KPI is that introducing adversarial protection mechanisms have negligible performance reduction with respect to common incident detection metrics, such as accuracy, precision, recall and F1. When training a detection engine using secure multiparty computation (MPC), a run-time performance overhead (from

introducing adversarial protection mechanisms) of no more than 10x seems reasonable[1]. For differential privacy, *sensitivity* [271] could be used as a measure, and it should be less than a given value with negligible performance reductions with respect to common incident-detection metrics (e.g., with epsilon at 1 and delta around 10^{-6}). For model poisoning attacks, one potential KPI is the *amount of adversarial workers/agent that can be tolerated (with negligible performance loss)*. For example, the system should handle 10% adversarial workers.

Orchestration (Intrusion Response) KPIs:

In an envisioned 6G network environment, the rapid response to security incidents becomes crucial due to the increased network complexity and the massive number of interconnected devices. The "Mean Time to Respond" (MTTR) is a KPI that measures the average time it takes for security functions or network management systems to detect, analyze, and counteract malicious activities or security incidents.

A shorter MTTR indicates that the 6G network can quickly identify and respond to security threats, thereby minimizing the impact of attacks on network performance, user experience, and data integrity. To streamline and accelerate the response process, the MTTR is essential to monitor the effectiveness of automated incident response solutions, i.e., Security Orchestration, Automation, and Response (SOAR) systems.

The "Decision Time" is a KPI used to evaluate the efficiency of a trained ML model in making predictions or decisions about network resource orchestration. In the context of 6G, where an ML model is orchestrating resources, the decision time becomes critical to the overall performance and responsiveness of the network. When an ML model orchestrates resources in a 6G network, it must make real-time or near real-time decisions to allocate resources effectively, manage network traffic, and adapt to changing conditions, e.g., induced by malicious activity. The Decision Time KPI indicates how fast the ML model can process input data, analyze the current network state, and make informed decisions to protect the network. Representative values from the literature include 220ms for a deep reinforcement learning model trained on a simulated 5G environment [272]. Several design considerations affect this KPI, including the ML model optimization techniques, whether hardware acceleration is used, and whether edge computing is employed to reduce the latency associated with data transfer.

[1] As a reference point, Microsoft were able to achieve 4x overhead for a specific data set, using a 3-party, semi-honest, specialized secure multiparty computation protocol. This is as ideal as it gets and we thus consider 10x more realistic.

We further elaborate with more ad-hoc Key Performance Indicators (KPIs) exclusively specialized on the slicing & orchestration of 6G networks infrastructure, specifically *after* a malicious cybersecurity incident takes place*.

Time to resource preparation end-to-end: from the moment an order is expressed as intent, until all multi-party resources that comply to corresponding privacy service requirements have been discovered and provisioned. *KPI target:* discover and provision multi-party resources in *less than 1 minute*.

Time to repair: from the moment a security anomaly breach is detected (or predicted) until relevant intra- or inter-domain adaptation primitives have been triggered and completed, bringing the system back to a stable and privacy-by-default SLA-compliant state. *KPI target:* complete intra-domain adaptation actions in *less than 1 minute* and inter-domain in *less than 5.*

Time to compose: from the moment a slice that includes PaaS services (from Cloud to Edge) as well as IoT devices (Far Edge), is requested until the time that it is successfully deployed over the compute continuum infrastructure with full Privacy SLAs guaranteed; *< 5 min.*

Time to migrate: from the moment that it is decided that a PaaS service should migrate, until the time that migration is completed, bringing the PaaS in a fully operational state (in terms of PAaS fulfilment of agreed condition); *< 1 min* in case of intra-domain migration, and *< 3 min* in case of inter-domain migration.

**Iquadrat Informatica SL holds the literature sources and the data*

Distributed Ledger KPIs:

Blockchain and distributed ledger solutions have been around for some years nevertheless, their integration with 6G services is a field currently under research, thus specific KPIs have not been established yet. Consequently, the proposed KPIs for the Blockchain technology are based on values from existing implementations that are not dedicated to 6G.

In general, the blockchain has two basic metrics those are i) the latency and ii) the throughput. While the latency is referring to the time between the receival of the request to the commitment of the transaction (i.e., the operation), while the throughput is referring to the total number of transactions supported. Quantifiable metrics, based on scalability and unit testing regarding the number of transactions and the trust anchors that can be supported by a blockchain peer, can be acquired from [268] [269]. Based on this, regarding the KPIs for the latency it is further broken down into writing and reading transaction requirement, while for the throughput a single blockchain peer shall be able to perform > 1000 transactions concurrently and engage with 3 sources.

According to [267] there are several factors that may influence the two metrics, depending on the use case scenario. One of this metrics is the number of the nodes that constitute the network. An increased number of nodes signifies that more time is needed for the execution of the transaction. For this indicator, 1 peer is considered per 200 devices per [269]. [267] further defines other factors that may influence the latency and throughput such as the consensus protocol used and the geographical distribution of the nodes, nevertheless these metrics are highly dependent on the chosen Hyperledger technology and the use case.

Apart from the traditional metrics though, an important KPI for blockchain in 6G may be the network security. The 6G networks have adopted the concept of security by design, to deploy virtual elements with adequate trust anchors. Nevertheless, this is far from reaching maturity, while the complexity and the growing size of such an infrastructure introduces new challenges through new threat vectors. Towards this direction, Privateer has defined some metrics that can be utilised in order to evaluate the security of the network. These are the following:

- Auditability of data on the blockchain: Auditability is a key feature for the transparency of blockchain networks in general, providing the ability to trace and verify records, thus transactions, within the decentralised ledger. The key metric here is to audit the *correctness of the transaction* and its effects on the latency. The correctness of the transaction is achieved by employing crypto primitives (i.e., signatures). These crypto mechanisms though should not affect the latency >10%.
- Representation of chain of trust: Similarly to the auditability, the representation of the *chain of trust* is a basic characteristic of distributed ledgers, to maintain transparency, by providing tamper-proof record of the history of transactions. In blockchain each transaction is cryptographically linked to the previous one (i.e., using hashes or signatures), creating a chain of blocks. This chain of blocks ensures the integrity of the transactions, while it represents the history for each actor/device/ virtual element, based on history of trust indicators on the blockchain. This metric again is considered in terms of its effects on the latency, when queuing the data. Note that this data is linked with each other due to the chain format. Consequently, the transaction representing a reading query for on-chain data should be efficient in time (in the order of ms) and should not consume more than 5% of the peer resources
- Certifiability: Processes and functionalities shall be updated in a certifiable manner. This aspect is translated to the assurance provided to the stakeholders that the blockchain follows certain standards (i.e., ISO 27001). Similarly to the auditability, the certifiability, which is achieved by employing crypto primitives, shall not introduce overhead (in the order of ms) to the

network. In a quantifiable definition, they should not consume more than 5% of the peer resources

- Secure and Privacy preserving data sharing: Offering support to different data sharing profiles, with different level of granularity while differentiating parts of these data in terms of access (i.e., attribute based). As mentioned in section 4.2, the ability to share data securely, leveraging a distributed architecture is pivotal. Towards this direction, tamper-proof, verifiable records of transactions are available, while advanced encryption techniques are also employed to ensure access to data and to the blockchain for only authorised entities. In terms of quantifiable metrics, >3 *crypto primitives*, supporting the selected data sharing profiles, should be available.
- Decentralised Identity Management and Service Requirements: Provide service discovery based on the concept DIDs. As mentioned in section 4.2, the identity management is an important feature for the security of the distributed network, to ensure access to authorised entities only both to the network and to the actual data exchanged. DIDs can be employed towards this direction of managing identities in distributed environments. Additionally, DIDs, combined with the notion of Verifiable Credentials (VCs) can further provide privacy protection, by employing advanced encryption techniques.
- Data portability: Each provider may support different blockchain and distributed ledger solution. In the forecasted 6G environment, where multiple service or infrastructure providers may support their own distributed ledger solution, data portability is a critical feature. It provides the option to individuals to transfer securely their data from one solution to the other, without losing the sovereignty of their data. Therefore, this metric should ensure that the state of the data is not different from one solution to another thus double spending cannot be achieved.

8.2.3 Key Value Indicators (KVIs)

Trustworthiness is one of the crucial KVIs for 6G networks. Trustworthiness encompasses multiple facets, such as “security, privacy, availability, resilience, compliance with ethical frameworks” [258]. Other sources use similar descriptions, which have in common that security and privacy are considered as crucial properties of trustworthy systems. A relevant aspect is how to translate and assess trustworthiness properties of 6G systems. A potential solution is to combine several metrics related to the above mentioned into the concept of a Level of Trust (LoT). The LoT can be calculated as a combination of several metrics that can be monitored on different domains or the combination of them into services and give the user assurance on the trustworthiness of a service. The metrics can include the following: Attestation level (SW, HW), Traffic Attestation (confirmed Proof-of-Transit), Traceability (e.g., via Smart Contracts: allows conducting verifiable accounting &

SLAs), Security issues related to the SDN Controller, NFVO & Slice Manager (e.g., compromised slices), AI-related and Privacy KPIs.

It should be noted that as it pertains to the trustworthiness metric, any new system should be able to support the appropriate indicators of trust that can enable the classification of at least 5 levels of assurance, as defined by ETSI [270]. These levels of assurance capture the required level of trust compared to the actual one of elements and actors comprising a 6G infrastructure, stemming from the infrastructure to the virtual elements and the exchanged data.

There are six distinct levels of assurance (LoA) defined by ETSI, using a number from 0-5 to represent a scale of relative trust, where a greater number denotes a higher level of trust. These are the following:

- LoA 0: denoting the complete absence of any form of integrity verification.
- LoA 1: covering the local integrity verification of the hardware and virtualization platform's (hypervisor) during boot and application loading. No proof of integrity is offered.
- LoA 2: Adding to LoA 1 the remote attestation of the hardware and virtualization platform integrity. Measurements of boot time and application load time are considered.
- LoA 3: Adding to LoA 2, LoA 3 incudes the local verification of VNF software packages as they are loaded on VNF startup.
- LoA 4: Adding to LoA 3 the remote attestation of VNF software packages.
- LoA 5: Adding to LoA 4 the remote verification of the infrastructure network set up to enable the VNF as well as the remote verification of the virtualization layer and VNF software.

Table 16. Proposed KPIs to the SNS Programme by PRIVATEER

	Suggested Representative Security/Privacy KPIs for 6G
AI Intrusion Detection	Accuracy of threat classification models
	Number of False Positives
	Number of False Negatives
	Mean Time to Detect a Threat
	Mean Time to Classify a Threat
	Accuracy Loss (1 – Accuracy of Federated Model/Accuracy of Centralized model)
AI Privacy Preservation of ML model Data Anonymization	Accuracy Loss (1 – Accuracy of Private Model/Accuracy of non-Private model)
	Adversarial Model Accuracy as evaluation metric of Privacy perseverance of an ML model: • Inference of Membership attacks: Reverse of the Adversarial Accuracy during Inference

	• Inferring properties of private training data (model inversion): Precision and Recall of meta-classifiers. • Inferring Training Input & labels (reconstruction attack): *MSE (Mean Squared Error) between a target and its reconstruction*
	Quality Loss: how much quality is lost by reporting anonymized data instead of real data
AI Adversarial Protection	Negligible performance loss (by introducing protection vs no protection) w.r.t accuracy/precision/recall/AUC/F1)
	Performance overhead by introducing secure/privacy preserving distributed learning
	Differential privacy sensitivity
	Model Poisoning: % of Adversarial Workers/agents that can be tolerated (with negligible performance loss)
Security Orchestration (Intrusion Response)	Mean Time to Respond to detected threats
	Decision Time
	Time to resource preparation end-to-end
	Time to compose
	Reduction in energy consumption
Distributed Ledger	Time between receival of the request to the commitment of the transaction (Latency)
	Total number of transactions (Throughput)
	Correctness of the transaction
	Chain of Trust
	Data Portability

9 Conclusions

Through the process of preparing this this document it has been clear that the 6G architecture is yet to be fully defined, but many promising key enabling technologies have been identified supported by a plethora of studies and researches that are still ongoing. It is foreseen that these technologies will enable a new era of advanced user and business case scenarios. The analyses have also highlighted how some of these technologies, compared with the 5G, will bring benefits able to overcome some known security and privacy concerns It is to consider that some of them could also be treated as a new attack surface that could be exploited if not properly designed and developed by a “security-by-design” and “privacy-first” approach.

The analysis conducted during the production of this artifact was not only focused to discover possible threats related to 6G; a step further has been done trying to understand which possible countermeasures could be designed and then developed to mitigate the risks related to the identified threats.

Focusing on the privacy concerns elicited in document, promising solutions have been identified, they must be further analysed, refined and then developed in the next phases of the PRIVATEER project (Work Packages 3, 4 and 5).

To be able to design the “privacy-first” technological building blocks, that will become the PRIVATEER Framework, a further refinement and elaboration of the elicited initial set of realistic Use Case scenarios depicted in this document during the task T2.2 is needed.

Sound Use Cases, a set of a measurable KPIs and KVIs along with a future phase for an Adversary-based threat modelling for the PRIVATEER Framework, will finally allow to validate the effectiveness of the PRIVATEER technological building blocks to properly address 6G privacy concerns.

References

[1] "ENISA Threat Landscape Methodology" 06/07/2022, https://www.enisa.europa.eu/publications/enisa-threat-landscape-methodology/@@download/fullReport

[2] "ENISA Threat Landscape Report 2018" 28/01/2019, https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018/@@download/fullReport

[3] "ENISA Threat Landscape 2022" 03/11/202, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022/@@download/fullReport

[4] "ENISA Threat Landscape for 5G Networks Report" 14/12/2020, https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks/@@download/fullReport

[5] "ENISA Threat Taxonomy" 09/2016, https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends/enisa-threat-landscape/threat-taxonomy/@@download/file/Threat%20taxonomy%20v%202016.xlsx

[6] Van-Linh Nguyen, Member, IEEE, Po-Ching Lin, Member, IEEE, Bo-Chao Cheng, Ren-Hung Hwang, Senior Member, IEEE, Ying-Dar Lin, Fellow, IEEE "Security and privacy for 6G: A survey on prospective technologies and challenges", Sep 2021

[7] D. Basin, J. Dreier, L. Hirschi, S. Radomirovic, R. Sasse, and V. Stettler "A formal analysis of 5g authentication," ACM SIGSAC Conference on Computer and Communications Security (CCS), 2018.

[8] R. P. Jover and V. Marojevic, "Security and protocol exploit analysis of the 5g specifications," IEEE Access, vol. 7, pp. 24956–24963, 2019.

[9] ETSI, "Etsi ts 133.501 v15.2.0, security architecture and procedures for 5g system," Technical Specification Group Services and System Aspects, 2018

[10] Verizon, "5g privacy preservation," https://www.verizon.com/about/sites/default/files/2020-09/200574 Schulz 07242020.pdf, accessed on 10 August 2021.

[11] T. M. Fern´andez-Caram´es, "From pre-quantum to post-quantum iot security: A survey on quantum-resistant cryptosystems for the internet of things," IEEE Internet of Things Journal, vol. 7, no. 7, pp. 6457–6480, 2020

[12] P. Wright, C. White, R. C. Parker, J. S. Pegon, M. Menchetti, J. Pearse, A. Bahrami, A. Moroz, A. Wonfor, R. V. Penty, T. P. Spiller, and A. Lord, "5g network slicing with qkd and quantumsafe security," IEEE/OSA Journal of Optical Communications and Networking, vol. 13, no. 3, pp. 33–40, 2021.

[13] ETSI, "Quantum safe cryptography and security," White Paper No. 8, 2015.

[14] Y.-A. Chen, Q. Zhang, and T.-Y. C. et al., "An integrated spaceto-ground quantum communication network over 4,600 kilometres," Nature, vol. 589, p. 214–219, 2021.

[15] J.-P. Chen, C. Zhang, and Y. L. et al., “Twin-field quantum key distribution over a 511km optical fibre linking two distant metropolitan areas,” Nature Photonics, vol. 68, 2021.
[16] 3GPP.SA3, “Technical specification group services and system aspects; security architecture and procedures for 5g system,” 3GPP TS 33.501 V16.4.0, 2020.
[17] C. Skouloudi, A. Malatras, and R. Naydenov, “Guidelines for securing the internet of things,” European Union Agency for Cybersecurity, 2020.
[18] M. Ylianttila et al., “6g white paper: Research challenges for trust, security and privacy,” https://arxiv.org/pdf/2004.11665.pdf, accessed on 10 August 2021.
[19] R. Kantola, “Trust networking for beyond 5g and 6g,” 2020 2nd 6G Wireless Summit (6G SUMMIT), pp. 1–6, 2020.
[20] T. N. N. Tran, L. Loven, J. Partala, M.-T. Kechadi, and S. Pirttikangas, “Privacy-aware blockchain innovation for 6g: Challenges and opportunities,” 2nd 6G Wireless Summit (6G SUMMIT), 2020.
[21] J. C. C. Chica, J. C. Imbachi, and J. F. B. Vega, “Security in sdn: A comprehensive survey,” Journal of Network and Computer Applications, vol. 159, 2020.
[22] S. Troia, F. Sapienza, L. Var´e, and G. Maier, “On deep reinforcement learning for traffic engineering in sd-wan,” IEEE Journal on Selected Areas in Communications, pp. 1–1, 2021 (early access).
[23] Z. Duli´nski, R. Stankiewicz, G. Rzym, and P. Wydrych, “Dynamic traffic management for sd-wan inter-cloud communication,” IEEE Journal on Selected Areas in Communications, vol. 38, no. 7, pp. 1335–1351, 2020.
[24] M. Chahbar, G. Diaz, A. Dandoush, C. C´erin, and K. Ghoumid, “A comprehensive survey on the e2e 5g network slicing model,” IEEE Transactions on Network and Service Management, pp. 1–1, 2020.
[25] 3GPP.SA3, “Study on security aspects of 5g network slicing management,” 3GPP TR 33.811 V15.0.0, 2018.
[26] S. Lal, T. Taleb, and A. Dutta, “Nfv: Security threats and best practices,” IEEE Communications Magazine, vol. 55, no. 8, pp. 211–217, 2017.
[27] A. Aldweesh, A. Derhab, and A. Z.Emam, “Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues,” Knowledge-Based Systems, vol. 189, p. 105124, 2020.
[28] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, and P. Faruki, “Network intrusion detection for iot security based on learning techniques,” IEEE Communications Surveys & Tutorials, vol. 21, no. 3, pp. 2671–2701, 2019.
[29] Y. Li, Y. Yu, C. Lou, N. Guizani, and L. Wang, “Decentralized public key infrastructures atop blockchain,” IEEE Network, vol. 34, no. 6, pp. 133–139, 2020.
[30] C. Lin, D. He, X. Huang, N. Kumar, and K.-K. R. Choo, “Bcppa: A blockchain-based conditional privacy-preserving authentication protocol for vehicular ad hoc networks,” IEEE Transactions on Intelligent Transportation Systems, pp. 1–13, June 2020.

[31] S. Boeyen, S. Santesson, T. Polk, R. Housley, S. Farrell, and D. Cooper, “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.” RFC 5280, 2008.
[32] 3GPP, “Authentication and key management for applications (akma) based on 3gpp credentials in the 5g system (5gs),” Technical Specification, 2021.
[33] V. Talreja, M. C. Valenti, and N. M. Nasrabadi, “Deep hashing for secure multimodal biometrics,” IEEE Transactions on Information Forensics and Security, vol. 16, pp. 1306–1321, 2021.
[34] C. Yuan, S. Jiao, X. Sun, and Q. M. J. Wu, “Mfffld: A multi-modal feature fusion based fingerprint liveness detection,” IEEE Transactions on Cognitive and Developmental Systems, pp. 1–1, 2021 (early access).
[35] P. Arnau-Gonz´alez, S. Katsigiannis, M. Arevalillo-Herr´aez, and N. Ramzan, “Bed: A new dataset for eeg-based biometrics,” IEEE Internet of Things Journal, pp. 1–1, 2021 (early access).
[36] J. Richer, A. Parecki, and F. Imbault, “Grant Negotiation and Authorization Protocol,” Internet-Draft draft-ietf-gnap-core-protocol-06, Internet Engineering Task Force, 2021. Work in Progress.
[37] M. Bishop, “Hypertext Transfer Protocol Version 3 (HTTP/3),” Internet-Draft draft-ietf-quic-http-34, Internet Engineering Task Force, 2021.
[38] P. Yang, N. Xiong, and J. Ren, “Data security and privacy protection for cloud storage: A survey,” IEEE Access, vol. 8, pp. 131723–131740, 2020.
[39] J. Zeuner, I. Pitsios, S.-H. Tan, A. N. Sharma, J. F. Fitzsimons, R. Osellame, and P. Walther, “Experimental quantum homomorphic encryption,” npj Quantum Information, vol. 1, no. 1, pp. 38–45, 2021.
[40] E. Peltonen et al., “6g white paper on edge intelligence,” CoRR, vol. abs/2004.14850, 2020.
[41] Y. Wang, Q. Wang, X. Chen, D. Chen, X. Fang, M. Yin, and N. Zhang, “Container guard: A real-time attack detection system in container based big data platform,” IEEE Transactions on Industrial Informatics, pp. 1–1, 2020.
[42] S. Iqbal, M. L. Mat Kiah, B. Dhaghighi, and Muzammil, “On cloud security attacks: A taxonomy and intrusion detection and prevention as a service,” Journal of Network and Computer Applications, vol. 74, pp. 98–120, 2016.
[43] 5GIA, “Strategic research and innovation agenda 2021-27 - smart networks in the context of ngi,” European Technology Platform NetWorld 2020, Sep 2020.
[44] Q. Mao, F. Hu, and Q. Hao, “Deep learning for intelligent wireless networks: A comprehensive survey,” IEEE Communications Surveys Tutorials, vol. 20, no. 4, pp. 2595–2621, 2018.
[45] N. Ye, X. Li, H. Yu, A. Wang, W. Liu, and X. Hou, “Deep learning aided grant-free noma toward reliable low-latency access in tactile internet of things,” IEEE Transactions on Industrial Informatics, vol. 15, no. 5, pp. 2995–3005, 2019

[46] W. Kim, Y. Ahn, and B. Shim, “Deep neural network-based active user detection for grant-free noma systems,” IEEE Transactions on Communications, vol. 68, no. 4, pp. 2143–2155, 2020.
[47] N. Ebrahimi, H. S. Kim, and D. Blaauw, “Physical layer secret key generation using joint interference and phase shift keying modulation,” IEEE Transactions on Microwave Theory and Techniques, pp. 1–1, 2021 (early access).
[48] N. Xie, Z. Li, and H. Tan, “A survey of physical-layer authentication in wireless communications,” IEEE Communications Surveys & Tutorials, vol. 23, no. 1, pp. 282–310, 2021.
[49] J. B. Perazzone, P. L. Yu, B. M. Sadler, and R. S. Blum, “Artificial noise-aided mimo physical layer authentication with imperfect csi,” IEEE Transactions on Information Forensics and Security, pp. 1–1, 2021.
[50] [M. Yan, G. Feng, J. Zhou, Y. Sun, and Y. C. Liang, “Intelligent resource scheduling for 5g radio access network slicing,” IEEE Transactions on Vehicular Technology, vol. 68, no. 8, pp. 7691–7703, 2019.
[51] Y. J. Liu, G. Feng, Y. Sun, S. Qin, and Y. C. Liang, “Device association for ran slicing based on hybrid federated deep reinforcement learning,” IEEE Transactions on Vehicular Technology, vol. 69, no. 12, pp. 15731–15745, 2020.
[52] V. Talreja, M. C. Valenti, and N. M. Nasrabadi, “Deep hashing for secure multimodal biometrics,” IEEE Transactions on Information Forensics and Security, vol. 16, pp. 1306–1321, 2021.
[53] A. Aldweesh, A. Derhab, and A. Z.Emam, “Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues,” Knowledge-Based Systems, vol. 189, p. 105124, 2020.
[54] J. Chen, J. Chen, and H. Zhang, “Drl-qor: Deep reinforcement learning based qos/qoe-aware adaptive online orchestration in nfv-enabled networks,” IEEE Transactions on Network and Service Management, pp. 1–1, 2021 (early access).
[55] S. Sengupta, A. Chowdhary, A. Sabur, A. Alshamrani, D. Huang, and S. Kambhampati, “A survey of moving target defenses for network security,” IEEE Communications Surveys & Tutorials, vol. 22, no. 3, pp. 1909–1941, 2020.
[56] M. Haghighat, S. Zonouz, and M. Abdel-Mottaleb, “Cloudid: Trustworthy cloud-based and cross-enterprise biometric identification,” Expert Systems with Applications, vol. 42, no. 21, pp. 7905–7916, 2015.
[57] D. Y. Hwang, B. Taha, D. S. Lee, and D. Hatzinakos, “Evaluation of the time stability and uniqueness in ppg-based biometric system,” IEEE Transactions on Information Forensics and Security, vol. 16, pp. 116–130, 2021.
[58] N. Kaaniche, M. Laurent, and S. Belguith, “Privacy enhancing technologies for solving the privacy-personalization paradox: Taxonomy and survey,” Journal of Network and Computer Applications, vol. 171, p. 102807, 2020.
[59] S.-C. Cha, T.-Y. Hsu, Y. Xiang, and K.-H. Yeh, “Privacy enhancing technologies in the internet of things: Perspectives and challenges,” IEEE Internet of Things Journal, vol. 6, no. 2, pp. 2159–2187, 2019.

[60] Y. Dai, D. Xu, S. Maharjan, Z. Chen, Q. He, and Y. Zhang, “Blockchain and deep reinforcement learning empowered intelligent 5g beyond,” IEEE Network, vol. 33, no. 3, pp. 10–17, 2019.

[61] H. Xu, P. V. Klaine, O. Onireti, B. Cao, and M. Imrana, “Blockchainenabled resource management and sharing for 6g communications,” Digital Communications and Networks, vol. 6, no. 3, pp. 261–269, 2020.

[62] P. Silva, E. Monteiro, and P. Sim˜oes, “Privacy in the cloud: A survey of existing solutions and research challenges,” IEEE Access, vol. 9, pp. 10473–10497, 2021.

[63] B. Jiang, J. Li, G. Yue, and H. Song, “Differential privacy for industrial internet of things: Opportunities, applications and challenges,” IEEE Internet of Things Journal, pp. 1–1, 2021 (early access).

[64] M. U. Hassan, M. H. Rehmani, and J. Chen, “Differential privacy techniques for cyber physical systems: A survey,” IEEE Communications Surveys & Tutorials, vol. 22, no. 1, pp. 746–789, 2020.

[65] Y. Rahulamathavan, S. Dogan, X. Shi, R. Lu, M. Rajarajan, and A. Kondoz, “Scalar product lattice computation for efficient privacy reserving systems,” IEEE Internet of Things Journal, vol. 8, no. 3, pp. 1417–1427, 2021.

[66] L. U. Khan, I. Yaqoob, N. H. Tran, Z. Han, and C. S. Hong, “Network slicing: Recent advances, taxonomy, requirements, and open research challenges,” IEEE Access, vol. 8, pp. 36009–36028, 2020.

[67] Y. Liu, X. Yuan, Z. Xiong, J. Kang, X. Wang, and D. Niyato, “Federated learning for 6g communications: Challenges, methods, and future directions,” China Communications, vol. 17, pp. 105–118, 2020.

[68] Y. Xiao, G. Shi, and M. Krunz, “Towards ubiquitous ai in 6g with federated learning,” https://arxiv.org/pdf/2004.13563.pdf, 2020.

[69] C. Dwork and A. Roth, “The algorithmic foundations of differential privacy,” Foundation and Trends in Theoretical Computer Science, vol. 9, no. 3–4, pp. 211–407, 2014, available online at: 10.1561/0400000042.

[70] R. L. Rivest, L. Adleman, and M. L. Dertouzos, “On data banks and privacy homomorphisms.” Foundations of Secure Computation, vol. 4, no. 11, pp. 169-180, 1978.

[71] A. C. Yao, “Protocols for secure computations.” 23rd annual symposium on foundations of computer science (sfcs 1982), IEEE, pp. 160-164, 1982.

[72] “Confidential Computing: Hardware-Based Trusted Execution for Applications and Data”, available online at: https://confidentialcomputing.io/wp-content/uploads/sites/85/2021/03/confidentialcomputing_outreach_whitepaper-8-5x11-1.pdf

[73] Semiconductor Research Corporation. (Jan. 2021). The Decadal Plan for Semiconductors. [Online]. Available at: https://www.src.org/about/decadal-plan/

[74] Z. Zhang, Y. Xiao, Z. Ma, M. Xiao, Z. Ding, X. Lei, G. K. Karagiannidis, and P. Fan, “6g wireless networks: Vision, requirements, architecture, and key

technologies," IEEE Vehicular Technology Magazine, vol. 14, no. 3, pp. 28–41, 2019.

[75] F. Dressler and F. Kargl, "Towards security in nano-communication: Challenges and opportunities," Nano Communication Networks, vol. 3, no. 3, pp. 151–160, 2012.

[76] C. Huang, S. Hu, G. C. Alexandropoulos, A. Zappone, C. Yuen, R. Zhang, M. D. Renzo, and M. Debbah, "Holographic mimo surfaces for 6g wireless networks: Opportunities, challenges, and trends," IEEE Wireless Communications, vol. 27, no. 5, pp. 118–125, 2020.

[77] Y. Liu, H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: Theories, technologies, and challenges," IEEE Communications Surveys & Tutorials, vol. 19, no. 1, pp. 347– 376, 2017.

[78] J. Tang, L. Jiao, K. Zeng, H. Wen, and K. Y. Qin, "Physical layer secure mimo communications against eavesdroppers with arbitrary number of antennas," IEEE Transactions on Information Forensics and Security, vol. 16, pp. 466–481, 2021.

[79] H. M. Furqan, J. M. Hamamreh, and H. Arslan, "Physical layer security for noma: Requirements, merits, challenges, and recommendations," 2020.

[80] M. Wijewardena, T. Samarasinghe, K. T. Hemachandra, S. Atapattu, and J. S. Evans, "Physical layer security for intelligent reflecting surface assisted two–way communications," IEEE Communications Letters, pp. 1–1, 2021.

[81] M. Hafez, T. Khattab, T. Elfouly, and H. Arslan, "Secure multiple-users transmission using multi-path directional modulation," in 2016 IEEE International Conference on Communications (ICC), pp. 1–5, 2016.

[82] M. Shakiba-Herfeh, A. Chorti, and H. V. Poor, "Physical layer security: Authentication, integrity and confidentiality," https://arxiv.org/pdf/2001.07153.pdf, accessed on 10 August 2021.

[83] "Next G Alliance Report:6G Distributed Cloud and Communications Systems" [Online] Available: https://www.nextgalliance.org/white_papers/6g-distributedcloud-andcommunicationssystems/

[84] H. Peng, Z. Wang, S. Han, and Y. Jiang, "Physical layer security for miso noma vlc system under eavesdropper collusion," IEEE Transactions on Vehicular Technology, pp. 1–1, 2021.

[85] C. Liaskos, S. Nie, A. Tsioliaridou, A. Pitsillides, S. Ioannidis, and I. Akyildiz, "A new wireless communication paradigm through software-controlled metasurfaces," IEEE Communications Magazine, vol. 56, no. 9, pp. 162–169, 2018.

[86] R. Singh and D. Sicker, "Thz communications - a boon and/or bane for security, privacy, and national security," in TPRC48: The 48th Research Conference on Communication, Information and Internet Policy, 2020.

[87] J. Ma, R. Shrestha, J. Adelberg, C.-Y. Yeh, Z. Hossain, E. Knightly, J. M. Jornet, and D. M. Mittleman, “Security and eavesdropping in terahertz wireless links,” Nature, vol. 563, pp. 89–93, 2018.

[88] J. Qiao and M.-S. Alouini, “Secure transmission for intelligent reflecting surface-assisted mmwave and terahertz systems,” IEEE Wireless Communications Letters, vol. 9, no. 10, pp. 1743–1747, 2020.

[89] N. Chi, Y. Zhou, Y. Wei, and F. Hu, “Visible light communication in 6g: Advances, challenges, and prospects,” IEEE Vehicular Technology Magazine, vol. 15, no. 4, pp. 93–102, 2020.

[90] X. Wu, M. D. Soltani, L. Zhou, M. Safari, and H. Haas, “Hybrid lifi and wifi networks: A survey,” IEEE Communications Surveys Tutorials, vol. 23, no. 2, pp. 1398–1420, 2021.

[91] E. Panayirci, A. Yesilkaya, T. Cogalan, H. V. Poor, and H. Haas, “Physical-layer security with optical generalized space shift keying,” IEEE Transactions on Communications, vol. 68, no. 5, pp. 3042–3056, 2020.

[92] V. Loscr´ı, C. Marchal, N. Mitton, G. Fortino, and A. V. Vasilakos, “Security and privacy in molecular communication and networking: Opportunities and challenges,” IEEE Transactions on NanoBioscience, vol. 13, no. 3, pp. 198–207, 2014.

[93] V. L. Nguyen, P. C. Lin, and R. H. Hwang, “Enhancing misbehavior detection in 5g vehicle-to-vehicle communications,” IEEE Transactions on Vehicular Technology, vol. 69, no. 9, pp. 9417–9430, 2020.

[94] T. Jian, B. C. Rendon, E. Ojuba, N. Soltani, Z. Wang, K. Sankhe, A. Gritsenko, J. Dy, K. Chowdhury, and S. Ioannidis, “Deep learning for rf fingerprinting: A massive experimental study,” IEEE Internet of Things Magazine, vol. 3, no. 1, pp. 50–57, 2020.

[95] L. Senigagliesi, M. Baldi, and E. Gambi, “Comparison of statistical and machine learning techniques for physical layer authentication,” IEEE Transactions on Information Forensics and Security, vol. 16, pp. 1506– 1521, 2021.

[96] J. B. Perazzone, P. L. Yu, B. M. Sadler, and R. S. Blum, “Artificial noise-aided mimo physical layer authentication with imperfect csi,” IEEE Transactions on Information Forensics and Security, pp. 1–1, 2021.

[97] Telecom Infra Project (TID). MUST Open Transport SDN Architecture. Online: https://cdn.brandfolder.io/D8DI15S7/at/jh6nnbb6bjvn7w7t5jbgm5n/OpenTransportArchitecture-Whitepaper_TIP_Final.pdf

[98] Chica, J. C. C., Imbachi, J. C., & Vega, J. F. B. (2020). Security in SDN: A comprehensive survey. Journal of Network and Computer Applications, 159, 102595.

[99] ETSI GR NFV-SEC 005 V1.1.1 https://www.etsi.org/deliver/etsi_gr/NFV-SEC/001_099/005/01.01.01_60/gr_nfv-sec005v010101p.pdf

[100] RFC 8555: Automatic Certificate Management Environment (ACME) https://www.rfc-editor.org/rfc/rfc8555.txt

[101] RFC 9115 An Automatic Certificate Management Environment (ACME) Profile for Generating Delegated Certificates: https://www.rfc-editor.org/rfc/rfc9115.txt
[102] ETSI GR NFV-SEC 007 V1.1.1: https://www.etsi.org/deliver/etsi_gr/NFV-SEC/001_099/007/01.01.01_60/gr_nfv-sec007v010101p.pdf
[103] Draft-ietf-sfc-proof-of-transit-08 Proof of Transit: https://www.ietf.org/archive/id/draft-ietf-sfc-proof-of-transit-08.txt
[104] Shankar Lal, Tarik Taleb, and Ashutosh Dutta "NFV: Security Threats and Best Practices" - http://anastacia-h2020.eu/publications/NFV_Security_Threats_and_Best_Practices.pdf
[105] Enisa "NFV Security in 5G - Challenges and Best Practices, February 24, 2022" https://www.enisa.europa.eu/publications/nfv-security-in-5g-challenges-and-best-practices
[106] European Union Agency for Cybersecurity (ENISA), "ENISA THREAT LANDSCAPE FOR 5G NETWORKS", Threat assessment for the fifth generation of mobile telecommunications networks (5G), NOVEMBER 2019
[107] Pleva, P. (2012) A revised classification of anonymity, arXiv.org. Available at: https://arxiv.org/abs/1211.5613 (Accessed: March 27, 2023).
[108] G. Kunzmann, et al., Technology innovations for 6G system architecture, Whitepaper Nokia Bell Labs https://www.bell-labs.com/institute/white-papers/technology-innovations-for-6g-system-architecture 2022
[109] M. S. Akhtar, et al., 2022. "Malware Analysis and Detection Using Machine Learning Algorithms" Symmetry 14, no. 11: 2304. https://doi.org/10.3390/sym14112304
[110] O. Kompougias et al., "IoT Botnet Detection on Flow Data using Autoencoders," 2021 IEEE International Mediterranean Conference on Communications and Networking (MeditCom), Athens, Greece, 2021, pp. 506-511, doi: 10.1109/MeditCom49071.2021.9647639.
[111] S. A. Abdel Hakim, et al., Security Requirements and Challenges of 6G Technologies and Applications, Sensors 22, 1969, 2022
[112] M. Min et al., "Learning-Based Privacy-Aware Offloading for Healthcare IoT With Energy Harvesting," in IEEE Internet of Things Journal, vol. 6, no. 3, pp. 4307-4316, 2019, doi: 10.1109/JIOT.2018.2875926
[113] V. Ziegler et al., "Security and Trust in the 6G Era," in IEEE Access, vol. 9, pp. 142314-142327, 2021, doi:10.1109/ACCESS.2021.3120143
[114] Liu et al., "Threats, attacks and defenses to federated learning: issues, taxonomy and perspectives", Cybersecurity, 2022, 5:4, https://doi.org/10.1186/s42400-021-00105-6
[115] Bingyan Liu et al., "Recent Advances on Federated Learning: A Systematic Survey", arXiv:2301.01299, 2022
[116] S. Warnat-Herresthal et al, 2021 "Swarm learning for decentralized and confidential clinical machine learning", Nature 594:265–270. https:// doi. org/ 10. 1038/ s41586- 021- 03583-3

[117] L. Song et al., “Sok: training machine learning models over multiple sources with privacy preservation”, arXiv: 2012. 03386

[118] Hongyi Wang et al., Attack of the Tails: Yes, You Really Can Backdoor Federated Learning, NIPS'20: Proceedings of the 34th International Conference on Neural Information Processing Systems, 2020, 1348, 16070–16084

[119] Ligeng Zhu et al., “Deep leakage from gradients”, NIPS'19: Proceedings of the 33rd International Conference on Neural Information Processing Systems, 2019, 1323, 14774–14784

[120] A. N. Bhagoji et al., Proceedings of the 36th International Conference on Machine Learning, Analyzing Federated Learning through an Adversarial Lens, 97:634-643, 2019

[121] N. Papernot, et al., “Security and privacy in machine learning”, IEEE European symposium on security and privacy, 399–414. https://doi.org/10.1109/EuroSP, 2018.

[122] Kamalika Chaudhuri and Claire Monteleoni. Privacy-preserving logistic regression. In Advances in Neural Information Processing Systems, 2009.

[123] Kamalika Chaudhuri, Claire Monteleoni, and Anand D. Sarwate. Differentially private Empirical Risk Minimization. Journal of Machine Learning Research, 2011.

[124] Martin Abadi, Andy Chu, Ian Goodfellow, H. Brendan McMahan, Ilya Mironov, Kunal Talwar, and Li Zhang. Deep learning with differential privacy. In ACM Conference on Computer and Communications Security, 2016.

[125] Reza Shokri and Vitaly Shmatikov. Privacy-preserving deep learning. In ACM Conference on Computer and Communications Security, 2015.

[126] S. Pentyala et al., “Training Differentially Private Models with Secure Multiparty Computation”, Cryptology ePrint Archive, 2022/146, 2022, https://eprint.iacr.org/2022/146

[127] X. Yuan, P. He, Q. Zhu and X. Li, "Adversarial Examples: Attacks and Defenses for Deep Learning," in IEEE Transactions on Neural Networks and Learning Systems, vol. 30, no. 9, pp. 2805-2824, Sept. 2019, doi: 10.1109/TNNLS.2018.2886017.

[128] I. J. Goodfellow, J. Shlens, and C. Szegedy, “Explaining and harnessing adversarial examples,” in Proc. Int. Conf. Learn. Represent. (ICLR), 2015.

[129] Zhang, Jiliang, and Chen Li. "Adversarial examples: Opportunities and challenges." IEEE transactions on neural networks and learning systems 31.7 (2019): 2578-2593.

[130] Lee, Hyeungill, Sungyeob Han, and Jungwoo Lee. "Generative adversarial trainer: Defense to adversarial perturbations with gan." arXiv preprint arXiv:1705.03387 (2017).

[131] Zhou, Shuai, et al. "Adversarial Attacks and Defenses in Deep Learning: From a Perspective of Cybersecurity." ACM Computing Surveys 55.8 (2022): 1-39.

[132] Pouya Samangouei, Maya Kabkab, and Rama Chellappa. 2018. Defense-GAN: Protecting classifiers against adversarial attacks using generative models. In Proceedings of the 6th International Conference on Learning Representations.
[133] Goodfellow, Ian, et al. "Generative adversarial networks." Communications of the ACM 63.11 (2020): 139-144.
[134] M. Nasr, R. Shokri and A. Houmansadr, "Comprehensive Privacy Analysis of Deep Learning: Passive and Active White-box Inference Attacks against Centralized and Federated Learning," 2019 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 2019, pp. 739-753, doi: 10.1109/SP.2019.00065.
[135] M. Nasr, R. Shokri, and A. Houmansadr, "Machine learning with membership privacy using adversarial regularization," in Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2018, pp. 634–646.
[136] J. Hamm, "Minimax filter: learning to preserve privacy from inference attacks," The Journal of Machine Learning Research, vol. 18, no. 1, pp. 4704–4734, 2017.
[137] C. Huang, P. Kairouz, X. Chen, L. Sankar, and R. Rajagopal, "Generative adversarial privacy," arXiv preprint arXiv:1807.05306, 2018.
[138] Guo W.: "Explainable Artificial Intelligence (XAI) for 6G: Improving Trust between Human and Machine" (2019)
[139] Wu Y., Lin G., Ge J.: "Knowledge-powered Explainable Artificial Intelligence (XAI) for Network Automation Towards 6G" (2022)
[140] Huong T.T., Bac T.P., Ha K.N., Hoang N.V., Hoang N.X., Hung N.T., Tran K.P.: "Federated Learning-Based Explainable Anomaly Detection for Industrial Control Systems" IEEE Access, 10, pp. 53854–53872 (2022) & FFI
[141] Wang S., Qureshi M.A., Miralles-Pechuán L., Huynh-The T., Gadekallu T.R., Liyanage M.: "Applications of Explainable AI for 6G: Technical Aspects, Use Cases, and Research Challenges" (2021)
[142] Lundberg S.M., Lee S.I.: "A unified approach to interpreting model predictions", (2017)
[143] Ribeiro M.T., Singh S., Guestrin C.: "Why should i trust you?" Explaining the predictions of any classifier Proc. ACM SIGKDD Int. Conf. Knowl. Discov. Data Min., 13-17-Augu, pp. 1135–1144 (2016)
[144] Ribeiro M.T., Singh S., Guestrin C.: Anchors: "High-precision model-agnostic explanations" 32nd AAAI Conference on Artificial Intelligence, AAAI 2018. pp. 1527–1535 (2018)
[145] Xie J., Liu Y., Shen Y.: "Explaining Dynamic Graph Neural Networks via Relevance Back-propagation" (2022)
[146] Nasiri S., Nasiri I., Van Laerhoven K.: Wearable xAI: "A Knowledge-Based Federated Learning Framework The 8th International Symposium on Sensor Science". p. 79. MDPI, Basel Switzerland (2021)
[147] Renda A., Ducange P., Marcelloni F., Sabella D., Filippou M.C., Nardini G., Stea G., Virdis A., Micheli D., Rapone D., Baltar L.G.: "Federated Learning of

Explainable AI Models in 6G Systems: Towards Secure and Automated Vehicle Networking Information", 13, pp. 395 (2022)

[148] B. Zong, C. Fan, X. Wang, X. Duan, B. Wang, and J. Wang, "6g technologies: Key drivers, core requirements, system architectures, and enabling technologies," IEEE Vehicular Technology Magazine, vol. 18, no. 3, pp. 18–27, 2019

[149] L. U. Khan, I. Yaqoob, N. H. Tran, Z. Han, and C. S. Hong, "Network slicing: Recent advances, taxonomy, requirements, and open research challenges," IEEE Access, vol. 8, pp. 36009–36028, 2020.

[150] Q. Bi, "Ten trends in the cellular industry and an outlook on 6g," IEEE Communications Magazine, vol. 57, no. 12, pp. 31–36, 2019

[151] M. Chahbar, G. Diaz, A. Dandoush, C. C ́erin, and K. Ghoumid, "A comprehensive survey on the e2e 5g network slicing model," IEEE Transactions on Network and Service Management, pp. 1–1, 2020.

[152] H. Zhang and V. W. S. Wong, "A two-timescale approach for network slicing in c-ran," IEEE Transactions on Vehicular Technology, vol. 69, no. 6, pp. 6656–6669, 2020.

[153] 3GPP.SA3, "Study on security aspects of 5g network slicing management," 3GPP TR 33.811 V15.0.0, 2018.

[154] M. Juntti, R. Kantola, P. Ky ̈osti, S. LaValle, C. M. de Lima, M. Matinmikko-Blue, T. Ojala, A. Pouttu, A. P ̈arssinen, and S. Yrj ̈ol ̈a, "Key drivers and research challenges for 6g ubiquitous wireless intelligence," 6G First Sumit, 2019

[155] C. Reichert, "Ericsson: Expired certificate caused o2 and softbank outages," https://www.zdnet.com/, accessed on 10 August 2021.

[156] Nguyen, V. L., Lin, P. C., Cheng, B. C., Hwang, R. H., & Lin, Y. D. (2021). "Security and privacy for 6G: A survey on prospective technologies and challenges". IEEE Communications Surveys & Tutorials, 23(4), 2384-2428

[157] E. Hanselman, "Security benefits of open virtualized ran," https://www.redhat.com/cms/managed-files/ve-451-research-telco- vran-security-analyst-material-f23695-en.pdf, accessed on 10 August 2021.

[158] C. Sexton, N. J. Kaminski, J. M. Marquez-Barja, N. Marchetti, and L. A. DaSilva, "5g: Adaptable networks enabled by versatile radio access technologies," IEEE Communications Surveys & Tutorials, vol. 19, no. 2, pp. 688–720, 2017.

[159] Thantharate, A.; Paropkari, R.; Walunj, V.; Beard, C. "DeepSlice: A deep learning approach towards an efficient and reliable network slicing in 5G networks". In Proceedings of the 2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York, NY, USA, 10–12 October 2019; pp. 762–767.

[160] Sedjelmaci, H. "Cooperative attacks detection based on artificial intelligence system for 5G networks". Comput. Electr. Eng. 2021, 91, 107045

[161] Shi, Y.; Sagduyu, Y.E.; Erpek, T.; Gursoy, M.C. "How to attack and defend 5G radio access network slicing with reinforcement learning". arXiv 2021, arXiv:2101.05768.

[162] Gong, Y.; Sun, S.; Wei, Y.; Song, M. "Deep Reinforcement Learning for Edge Computing Resource Allocation in Blockchain Network Slicing Broker Framework". In Proceedings of the 2021 IEEE 93rd Vehicular Technology Conference (VTC2021-Spring), Helsinki, Finland, 25–28 April 2021; pp. 1–6.
[163] ”An intelligent self-sustained RAN slicing framework for diverse service provisioning in 5G-beyond and 6G networks”
[164] ”The Road Towards 6G: A Comprehensive Survey”
[165] ”3GPP, NR; Overall description; Stage-2. Technical Specification” TS-38.300, 3GPP, v16.1.0
[166] “Towards a Fully Virtualized, Cloudified, and Slicing-Aware RAN for 6G Mobile Networks”
[167] “A Perspective of O-RAN Integration with MEC, SON, and Network Slicing in the 5G Era”
[168] ”Understanding O-RAN: Architecture, Interfaces, Algorithms, Security, and Research Challenges”
[169] “Open RAN Architecture” https://www.o-ran.org/
[170] https://futurenetworks.ieee.org/tech-focus/december-2017/multi-access-edge-computing-overview-of-etsi
[171] "ETSI White Paper No. 28 MEC in 5G networks" First Edition –june 2018
[172] "MEC ETSI - GS MEC 003 v3.1.1"
[173] https://www.ericsson.com/en/blog/2022/6/edge-use-cases-need-a-5g-and-beyond-user-plane
[174] "Survey on Multi-Access Edge Computing Security and Privacy" - Pasika Ranaweera
[175] Angui, B., Corbel, R., Rodriguez, V.K., & Stephan, E. (2022). Towards 6G zero touch networks: The case of automated Cloud-RAN deployments. 2022 IEEE 19th Annual Consumer Communications & Networking Conference (CCNC), 1-6.
[176] Coronado, E., Behravesh, R., Subramanya, T., Fernández-Fernández, A., Siddiqui, M.S., Costa-Pérez, X., & Riggio, R. (2022). Zero Touch Management: A Survey of Network Automation Solutions for 5G and 6G Networks. IEEE Communications Surveys & Tutorials, 24, 2535-2578.
[177] ETSI, “Zero-touch Network and Service Management (ZSM); Reference Architecture,” European Telecommunications Standards Institute, Group Specification (GS) ZSM 002, Aug. 2019, version 1.1.1.
[178] ETSI, “Zero-touch Network and Service Management (ZSM); Terminology for concepts in ZSM,” European Telecommunications Standards Institute, Group Specification (GS) ZSM 007, Aug. 2019, version 1.1.1.
[179] He, G.; Su, W.; Gao, S.; Liu, N.; Das, S.K. “NetChain: A Blockchain-Enabled Privacy-Preserving Multi-Domain Network Slice Orchestration Architecture”. IEEE Trans. Netw. Serv. Manag. 2022, 19, 188–202.

[180] Kalpana D. Joshi and Kotaro Kataoka. 2020. PSMART: A lightweight, privacy-aware service function chain orchestration in multi-domain NFV/SDN. Comput. Netw. 178, C (Sep 2020). https://doi.org/10.1016/j.comnet.2020.107295

[181] Manso, C., Alemany, P., Vilalta, R., Muñoz, R., Casellas, R., & Martínez, R. (2021). "End-to-End SDN/NFV Orchestration of Multi-Domain Transport Networks and Distributed Computing Infrastructure for Beyond-5G Services". IEICE Trans. Commun., 104-B, 188-198.

[182] Nadeem, L., Amin, Y., Loo, J., Azam, M.A., & Chai, K.K. (2021). "Efficient Resource Allocation Using Distributed Edge Computing in D2D Based 5G-HCN With Network Slicing". IEEE Access, 9, 134148-134162.

[183] Farooqui, Muhammad & Arshad, Junaid & Khan, Muhammad. (2022). "A Layered Approach to Threat Modeling for 5G-Based Systems". Electronics. 11. 1819. 10.3390/electronics11121819.

[184] Whitfield Diffie, Martin E. Hellman. New directions in cryptography. IEEE Trans. Inf. Theory 22(6): 644-654 (1976)

[185] Ronald L. Rivest, Adi Shamir, Leonard M. Adleman. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Commun. ACM 21(2): 120-126 (1978)

[186] Coppersmith, D. (1994). "An approximate Fourier transform useful in quantum factoring". Technical Report RC19642, IBM. arXiv:quant-ph/0201067

[187] Peter W. Shor. Polynominal time algorithms for discrete logarithms and factoring on a quantum computer. ANTS 1994: 289

[188] IBM: https://research.ibm.com/blog/quantum-volume-256

[189] Matthew Amy, Olivia Di Matteo, Vlad Gheorghiu, Michele Mosca, Alex Parent, John M. Schanck: Estimating the Cost of Generic Quantum Pre-image Attacks on SHA-2 and SHA-3. SAC 2016: 317-337

[190] Lov K. Grover: A Fast Quantum Mechanical Algorithm for Database Search. STOC 1996: 212-219

[191] Miklós Ajtai: Generating Hard Instances of Lattice Problems (Extended Abstract). STOC 1996: 99-108

[192] Oded Regev: On lattices, learning with errors, random linear codes, and cryptography. STOC 2005: 84-93

[193] NISTIR 8413 Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process

[194] BSI: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Brochure/quantum-safe-cryptography.pdf?__blob=publicationFile&v=4

[195] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing", Theor. Comput. Sci., vol. 560, no. 12, pp. 7-11, 2014.

[196] P. Sharma, A. Agrawal, V. Bhatia, S. Prakash and A. K. Mishra, "Quantum Key Distribution Secured Optical Networks: A Survey," in IEEE Open Journal of the

Communications Society, vol. 2, pp. 2049-2083, 2021, doi: 10.1109/OJCOMS.2021.3106659.

[197] "Quantum Key Distribution (QKD); Application Interface", vol. 2, pp. 1-22, 2020,[online] Available at : https://www.etsi.org/deliver/etsi_gs/QKD/001_099/004/02.01.01_60/gs_QKD004v020101p.pdf

[198] Duan, Shijin, et al. "A survey of recent attacks and mitigation on FPGA systems." 2021 IEEE Computer Society Annual Symposium on VLSI (ISVLSI). IEEE, 2021.

[199] Husain, Baydaa Hassan, and Shavan Askar. "Survey on edge computing security." International Journal of Science and Business 5.3 (2021): 52-60.

[200] Anandakumar, N. Nalla, Mohammad S. Hashmi, and Mark Tehranipoor. "FPGA-based Physical Unclonable Functions: A comprehensive overview of theory and architectures." Integration 81 (2021): 175-194.

[201] La, Tuan, et al. "Denial-of-Service on FPGA-based Cloud Infrastructures—Attack and Defense." IACR Transactions on Cryptographic Hardware and Embedded Systems (2021): 441-464.

[202] Van der Veen, Victor, et al. "GuardION: Practical mitigation of DMA-based rowhammer attacks on ARM." Detection of Intrusions and Malware, and Vulnerability Assessment: 15th International Conference, DIMVA 2018, Saclay, France, June 28–29, 2018, Proceedings 15. Springer International Publishing, 2018.

[203] M. P. Souppaya, J. Morello, and K. Scarfone, "Application container security guide," May 2021. [Online]. Available at: https://www.nist.gov/publications/application-container-security-guide

[204] M. Lipp, M. Schwarz, D. Gruss, T. Prescher, W. Haas, A. Fogh, J. Horn, S. Mangard, P. Kocher, D. Genkin et al., "Meltdown: Reading kernel memory from user space," in Proceedings of the USENIX Security Symposium (USENIX Security), 2018, pp. 973–990.

[205] E. M. Koruyeh, K. N. Khasawneh, C. Song, and N. Abu-Ghazaleh, "Spectre returns! speculation attacks using the return stack buffer," in Proceedings of the USENIX Workshop on Offensive Technologies (WOOT), 2018.

[206] Y. Yarom and K. Falkner, "Flush+ reload: A high resolution, low noise, l3 cache side-channel attack," in Proceedings of the USENIX Security Symposium (USENIX Security), 2014, pp. 719–732.

[207] H. M. Makrani, H. Sayadi, N. Nazari, A. Sasan, K. N. Khasawneh, S. Rafatirad, and H. Homayoun, "Cloak & co-locate: Adversarial railroading of resource sharing-based attacks on the cloud," in Proceedings of the International Symposium on Secure and Private Execution Environment Design (SEED). IEEE, 2021, pp. 1–13.

[208] C. Fang, H. Wang, N. Nazari, B. Omidi, A. Sasan, K. N. Khasawneh, S. Rafatirad, and H. Homayoun, "Repttack: Exploiting cloud schedulers to guide co-location attacks," in Proceedings of the Network and Distributed Systems Security (NDSS) Symposium, 2022.

[209] Y. Kim, R. Daly, J. Kim, C. Fallin, J. H. Lee, D. Lee, C. Wilkerson, K. Lai, and O. Mutlu, “Flipping bits in memory without accessing them: An experimental study of dram disturbance errors,” ACM SIGARCH Computer Architecture News, vol. 42, no. 3, pp. 361–372, 2014.

[210] M. Seaborn and T. Dullien, “Exploiting the dram rowhammer bug to gain kernel privileges,” Black Hat, vol. 15, p. 71, 2015.

[211] K. Murdock, D. Oswald, F. D. Garcia, J. Van Bulck, D. Gruss, and F. Piessens, “Plundervolt: Software-based fault injection attacks against intel sgx,” in Proceedings of the IEEE Symposium on Security and Privacy (SP), 2020, pp. 1466–1482.

[212] A. Tang, S. Sethumadhavan, and S. Stolfo, “CLKSCREW: exposing the perils of security-oblivious energy management,” in Proceedings of the USENIX Security Symposium (USENIX Security), 2017, pp. 1057–1074.

[213] Senevirathna, Thulitha, Zujany Salazar, Vinh Hoa La, Samuel Marchal, Bartlomiej Siniarski, Madhusanka Liyanage, and Shen Wang. "A survey on XAI for beyond 5G security: technical aspects, use cases, challenges and research directions." arXiv preprint arXiv:2204.12822 (2022).

[214] “Docker build secrets” [Online]. Available at: https://pythonspeed.com/articles/docker-build-secrets

[215] Irazoqui, Gorka, and Xiaofei Guo. “Cache side channel attack: Exploitability and countermeasures.” Black Hat Asia 2017, no. 3 (2017) : 1-72.

[216] “Do containers provide better protection against meltdown and spectre” [Online]. Available at: https://blog.aquasec.com/do-containers-provide-better-protection-against-meltdown-and-spectre

[217] Fang, Chongzhou, Najmeh Nazari, Behnam Omidi, Han Wang, Aditya Puri, Manish Arora, Setareh Rafatirad, Houman Homayoun, and Khaled N. Khasawneh. "HeteroScore: Evaluating and Mitigating Cloud Security Threats Brought by Heterogeneity." (2023).

[218] Zhang, Zhi. "Software-only Rowhammer Attacks and Countermeasures." PhD diss., UNSW Sydney, 2021.

[219] Potestad-Ordóñez, Francisco Eugenio, Erica Tena-Sánchez, Antonio José Acosta-Jiménez, Carlos Jesús Jiménez-Fernández, and Ricardo Chaves. "Hardware Countermeasures Benchmarking against Fault Attacks." Applied Sciences 12, no. 5 (2022): 2443.

[220] Carmela Troncoso, Dan Bogdanov, Edouard Bugnion, Sylvain Chatel, Cas Cremers, Seda F. Gürses, Jean-Pierre Hubaux, Dennis Jackson, James R. Larus, Wouter Lueks, Rui Oliveira, Mathias Payer, Bart Preneel, Apostolos Pyrgelis, Marcel Salathé, Theresa Stadler, Michael Veale. Deploying decentralized, privacy-preserving proximity tracing. Commun. ACM 65(9): 48-57 (2022)

[221] National Security Agency, ESF Potential Threats to 5G Network Slicing, Available at: https://media.defense.gov/2022/Dec/13/2003132073/-1/-

1/0/POTENTIAL%20THREATS%20TO%205G%20NETWORK%20SLICING_508C_FINAL.PDF

[222] V. N. Sathi, M. Srinivasan, P. K. Thiruvasagam and C. S. R. Murthy, "Novel Protocols to Mitigate Network Slice Topology Learning Attacks and Protect Privacy of Users' Service Access Behavior in Softwarized 5G Networks," in IEEE Transactions on Dependable and Secure Computing, vol. 18, no. 6, pp. 2888-2906, 1 Nov.-Dec. 2021, doi: 10.1109/TDSC.2020.2968885.

[223] Kuang, Boyu, Anmin Fu, Willy Susilo, Shui Yu, and Yansong Gao. "A survey of remote attestation in Internet of Things: Attacks, countermeasures, and prospects." Computers & Security 112 (2022): 102498.

[224] Aman, Muhammad Naveed, Mohamed Haroon Basheer, Siddhant Dash, Jun Wen Wong, Jia Xu, Hoon Wei Lim, and Biplab Sikdar. "HAtt: Hybrid remote attestation for the Internet of Things with high availability." IEEE Internet of Things Journal 7, no. 8 (2020): 7220-7233.

[225] Sfyrakis, Ioannis, and Thomas Gross. "A survey on hardware approaches for remote attestation in network infrastructures." arXiv preprint arXiv:2005.12453 (2020).

[226] Debes, Heini Bergsson, Thanassis Giannetsos, and Ioannis Krontiris. "Blindtrust: Oblivious remote attestation for secure service function chains." arXiv preprint arXiv:2107.05054 (2021).

[227] Oliver, Ian. "Trust, security and privacy through remote attestation in 5G and 6G systems." In 2021 IEEE 4th 5G world forum (5GWF), pp. 368-373. IEEE, 2021.

[228] Xu, Cheng, Hongzhe Liu, Peifeng Li, and Pengfei Wang. "A remote attestation security model based on privacy-preserving blockchain for V2X." Ieee Access 6 (2018): 67809-67818.

[229] Weichbrodt, Nico, Pierre-Louis Aublin, and Rüdiger Kapitza. "sgx-perf: A performance analysis tool for intel sgx enclaves." In Proceedings of the 19th International Middleware Conference, pp. 201-213. 2018.

[230] Chen, Guoxing, Yinqian Zhang, and Ten-Hwang Lai. "Opera: Open remote attestation for intel's secure enclaves." In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, pp. 2317-2331. 2019.

[231] Huang, Jing, Hui-Juan Zhang, Shen He, Jia Chen, and Zhe-Yuan Sun. "A remote attestation mechanism using group signature for the perception layer in centralized networking." EURASIP Journal on Wireless Communications and Networking 2022, no. 1 (2022): 1-19.

[232] ENISA, Threat Landscape for Supply Chain Attacks, July 29, 2021. (online at https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks)

[233] "On the Performance of Secure Sharing of Classified Threat Intelligence between Multiple Entities", Ricardo Fernandes, Sylwia Bugla, Pedro Pinto, and António Pinto, Sensors, 23, 2023. (online at: https://www.mdpi.com/1424-8220/23/2/914)

[234] I. H. Abdulqadder and S. Zhou, "SliceBlock: Context-Aware Authentication Handover and Secure Network Slicing Using DAG-Blockchain in Edge-Assisted SDN/NFV-6G Environment," in IEEE Internet of Things Journal, vol. 9, no. 18, pp. 18079-18097, 15 Sept.15, 2022, doi: 10.1109/JIOT.2022.3161838.

[235] Rathod T, Jadav NK, Tanwar S, Sharma R, Tolba A, Raboaca MS, Marina V, Said W. "Blockchain-Driven Intelligent Scheme for IoT-Based Public Safety System beyond 5G Networks". Sensors. 2023; 23(2):969. https://doi.org/10.3390/s23020969

[236] Chen, F.; Li, Z.; Li, B.; Deng, C.; Tian, Z.; Lin, N.; Wan, Y.; Bao, B. "Blockchain-based Optical Network Slice Rental Approach for IoT". In Proceedings of the 2020 IEEE Computing, Communications and IoT Applications (ComComAp), Beijing, China, 20–22 December 2020; pp. 1–4.

[237] Xu, H., Klaine, P. V., Onireti, O., Cao, B., Imran, M., & Zhang, L. (2020). Blockchain-enabled resource management and sharing for 6G communications. Digital Communications and Networks, 6(3), 261-269.

[238] 5G PPP Architecture Working Group, “The 6G Architecture Landscape European perspective”, December 2022 [Available] https://5g-ppp.eu/wp-content/uploads/2022/12/6G-Arch-Whitepaper_v1.0-final.pdf

[239] T. Hewa, G. Gür, A. Kalla, M. Ylianttila, A. Bracken and M. Liyanage, “The Role of Blockchain in 6G: Challenges, Opportunities and Research Directions,” 2020 2nd 6G Wireless Summit (6G SUMMIT), Levi, Finland, 2020, pp. 1-5, doi: 10.1109/6GSUMMIT49458.2020.9083784.

[240] T. Maksymyuk, J. Gazda, L. Han, and M. Jo, “Blockchain-Based Intelligent Network Management for 5G and Beyond,” in 2019 3rd Int. Conf. on Advanced Information and Communications Technologies (AICT), 2019, pp. 36–39.

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

[242] B. Mafakheri, T. Subramanya, L. Goratti, and R. Riggio, “Blockchainbased Infrastructure Sharing in 5G Small Cell Networks,” in 2018 14th International Conference on Network and Service Management (CNSM). IEEE, 2018, pp. 313–317.

[243] R. Sekaran, R. Patan, A. Raveendran, F. Al-Turjman, M. Ramachandran and L. Mostarda, “Survival Study on Blockchain Based 6G-Enabled Mobile Edge Computation for IoT Automation,” in IEEE Access, vol. 8, pp. 143453-143463, 2020, doi: 10.1109/ACCESS.2020.3013946.

[244] A. H. Khan et al., "Blockchain and 6G: The Future of Secure and Ubiquitous Communication," in IEEE Wireless Communications, vol. 29, no. 1, pp. 194-201, February 2022, doi: 10.1109/MWC.001.2100255.

[245] T. Sharma, S. K. Prasad and V. Sharma, "Research challenges of Blockchain in 6G Network," 2022 IEEE Delhi Section Conference (DELCON), New Delhi, India, 2022, pp. 1-7, doi: 10.1109/DELCON54057.2022.9753098.

[246] R. Belchior, B. Putz, G. Pernul, M. Correia, A. Vasconcelos and S. Guerreiro, "SSIBAC: Self-Sovereign Identity Based Access Control," 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Guangzhou, China, 2020, pp. 1935-1943, doi: 10.1109/TrustCom50675.2020.00264.

[247] M. S. Ferdous, F. Chowdhury and M. O. Alassafi, "In Search of Self-Sovereign Identity Leveraging Blockchain Technology," in IEEE Access, vol. 7, pp. 103059-103079, 2019, doi: 10.1109/ACCESS.2019.2931173.

[248] W3C, Decentralised Identifiers (DIDs) v1.0 Core architecture, data model and representations. [Available] https://www.w3.org/TR/did-core/

[249] W3C, Verifiable Credentials Data Model v1.1 Available at: https://www.w3.org/TR/vc-data-model/

[250] P. Porambage, G. Gür, D. P. M. Osorio, M. Liyanage, A. Gurtov and M. Ylianttila, "The Roadmap to 6G Security and Privacy," in IEEE Open Journal of the Communications Society, vol. 2, pp. 1094-1122, 2021, doi: 10.1109/OJCOMS.2021.3078081.

[251] A. Dabholkar and V. Saraswat. Ripping the fabric: Attacks and mitigations on hyperledger fabric. In V. S. Shankar Sriram, V. Subramaniyaswamy, N. Sasikaladevi, Leo Zhang, Lynn Batten, and Gang Li, editors, Applications and Techniques in Information Security, pages 300–311, Singapore, 2019. Springer Singapore

[252] C. Cordi. "Hyperledger Fabric Security Threats: What to Look For", Hyperledger Foundation Blog, 2021.

[253] N. Atzei, M. Bartoletti, & T. Cimoli (2017). A survey of attacks on ethereum smart contracts (sok). In Principles of Security and Trust: 6th International Conference, POST 2017, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2017, Uppsala, Sweden, April 22-29, 2017, Proceedings 6 (pp. 164-186). Springer Berlin Heidelberg.

[254] M. Wohrer and U. Zdun, "Smart contracts: security patterns in the ethereum ecosystem and solidity," 2018 International Workshop on Blockchain Oriented Software Engineering (IWBOSE), Campobasso, Italy, 2018, pp. 2-8, doi: 10.1109/IWBOSE.2018.8327565.

[255] J. Camenisch and A. Lysyanskaya. “A Signature Scheme with Efficient Protocols”. In Proceedings of the 3rd International Conference on Security in Communication Networks (SCN’02), pp 268–289, 2002

[256] M. H. Au, W. Susilo, & Y. Mu. “Constant-size dynamic k-TAA”. In Security and Cryptography for Networks: 5th International Conference, SCN 2006, Maiori, Italy, September 6-8, 2006. Proceedings 5 (pp. 111-125). Springer Berlin Heidelberg.

[257] T. Looker, O. Steele, BBS+ Signatures 2020, Draft CG Report, W3C Credentials CG, 2022. Available at : https://w3c-ccg.github.io/ldp-bbs2020/#the-bbs-signature-suite-2020.

[258] Hexa-X Consortium, “D1.2 Expanded 6G vision, use cases and societal values – including aspects of sustainability, security and spectrum,” April 2021. [Online]. Available: https://hexa-x.eu/wp-content/uploads/2022/04/Hexa-X_D1.2_Edited.pdf [Accessed March 2023]

[259] Hexa-X Consortium, “D1.3 Targets and requirements for 6G – initial E2E architecture,” February 2022. [Online]. Available: https://hexa-x.eu/wp-content/uploads/2022/03/Hexa-X_D1.3.pdf [Accessed March 2023]

[260] 5G Public Private Partnership, Test, Measurement and KPIs Validation Working Group, “White Paper: Beyond 5G/6G KPIs and Target Values,” 2022. [Online]. Available at: https://5g-ppp.eu/wp-content/uploads/2022/06/white_paper_b5g-6g-kpis-camera-ready.pdf [Accessed March 2023]

[261] Beyond 5G Promotion Consortium, White Paper Subcommittee, “Beyond 5G White Paper ~Message to the 2030s~,” March 2022. [Online]. Available: https://b5g.jp/w/wp-content/uploads/pdf/whitepaper_en_1-0.pdf [Accessed March 2023]

[262] Networld Europe, “Strategic Research and Innovation Agenda 2022, Technical Annex,” 2022. [Online]. Available at: https://bscw.5g-ppp.eu/pub/bscw.cgi/d516614/SRIA%202022%20Technical%20Annex%20Published.pdf [Accessed March 2023]

[263] Balle, Borja, Giovanni Cherubin, and Jamie Hayes. "Reconstructing training data with informed adversaries." 2022 IEEE Symposium on Security and Privacy (SP). IEEE, 2022.

[264] Ateniese, Giuseppe, et al. "Hacking smart machines with smarter ones: How to extract meaningful data from machine learning classifiers." International Journal of Security and Networks 10.3 (2015): 137-150.

[265] Nasr, Milad, Reza Shokri, and Amir Houmansadr. "Comprehensive privacy analysis of deep learning: Passive and active white-box inference attacks against centralized and federated learning." 2019 IEEE symposium on security and privacy (SP). IEEE, 2019.

[266] Jayaraman, Bargav, and David Evans. "Evaluating differentially private machine learning in practice." USENIX Security Symposium. 2019.

[267] Marsal Consortium, "Deliverable D5.1 Initial report on decentralized framework for confidentiality and hardware-accelerated security mechanisms", 2021. Available at : https://www.marsalproject.eu/wp-content/uploads/2022/09/MARSAL_D5.1_V1.0.pdf

[268] ISO/TC 307/JWG 4 Joint Working Group. "Blockchain and distributed ledger technologies and IT Security techniques." Final Report, ISO/TC 307/JWG 4 N18, International Organization for Standardization, September 2021, https://www.iso.org/standard/76039.html.

[269] Assured Consortium, "Deliverable D6.2 first demonstrators implementation report, 2022. [Available] https://www.project-assured.eu/deliverables/

[270] European Telecommunications Standards Institute,"Network Functions Virtualisation (NFV); Trust; Report on Attestation Technologies and Practices for Secure Deployments ", ETSI GR NFV-SEC 007, 2017. [Available] https://www.etsi.org/deliver/etsi_gr/NFV-SEC/001_099/007/01.01.01_60/gr_nfv-sec007v010101p.pdf

[271] Peter Kairouz. “Federated Learning & Privacy“ given at the Summer School on Privacy-Preserving Machine Learning at ITU Copenhagen and Aarhus University (Denmark) in 2022. Slides available at: https://medialib.cmcdn.dk/medialibrary/7B031F9C-64B5-43B7-B5AC-D0DF772C7975/3743CF16-8E32-ED11-84B6-00155D0B0940.pdf

[272] INSPIRE-5gplus “D5.3 Complete 5G security testing infrastructure implementation and final results” Version: v1.0 available at: https://www.inspire-5gplus.eu/wp-content/uploads/2022/12/i5-d5.3_complete-5g-security-testing-infrastructure-implementation-and-final-results_v1.0.pdf

Annex A: ENISA 5G TL Threats vs Assets

Threat Type	Threats	Potential Impact	Affected Assets
Nefarious Activity/Abuse of assets (NAA)	**Manipulation of network configuration/data forging** - Routing tables manipulation - Falsification of configuration data - DNS manipulation - Manipulation of access network and radio technology configuration data - Exploitation of misconfigured or poorly configured systems/networks - Registration of malicious network functions	- Information integrity - Information destruction - Service unavailability	- SDN, NFV, MANO - RAN, RAT - System configuration data - Network configuration data - Security configuration data - Business services
	Exploitation of software, hardware vulnerabilities - Zero-day exploits - Abuse of edge open application programming interfaces (APIs) - Application programming interface (API) exploitation	- Information integrity - Information destruction - Service unavailability	- SDN, NFV, MANO - RAN, RAT - MEC - API - Physical infrastructure - Business applications - Security controls - Cloud, virtualisation - Subscribers' data - Application data - Security data - Network data - Business services
	Denial of service (DoS) - Distributed denial of service (DDoS) - Flooding of core network components - Flooding of base stations - Amplification attacks - MAC layer attacks - Jamming of the network radio - Edge node overload - Authentication traffic spikes	- Service unavailability - Outage	- SDN, NFV - RAN, RAT - MEC - Cloud - Network services - Business services
	Remote access exploitation	- System integrity	- SDN, NFV, MANO - Cloud - Network services
	Malicious code/software - Injection attacks (SQL, XSS) - Virus - Malware	- Service unavailability - Information integrity - Information destruction - Other software asset	- Data network - Business applications - Security controls - Cloud, virtualisation

	- Rootkits - Rogueware - Worms/trojan - Botnet - Ransomware	integrity - Other software asset destruction	- Subscribers' data - Application data - Security data - Network data - Business services - Network services
	Abuse of remote access to the network	- Information integrity - System integrity	- SDN, NFV - RAN, RAT - Subscribers' data - Application data - Security data - Network data
	Abuse of information leakage - Theft and/or leakage from network traffic - Theft and/or leakage of data from cloud computing - Abuse on security data from audit tools - Theft/breach of security keys	- Information integrity - Information destruction - Information confidentiality	- Data storage/repository - Subscribers' data - Cryptographic keys - Monitoring data - User subscription profile data
	Abuse of authentication - Authentication traffic spikes - Abuse of user authentication/authorization data by third parties' personnel	- Information integrity - Information destruction - Service unavailability	- Network service - Subscribers' data - Application data - Security data - Network data
	Lawful interception function abuse	- Information integrity - Information destruction	- Subscribers' data - User subscription profile data
	Manipulation of hardware and software - Manipulation of hardware equipment - Manipulation of the network resources orchestrator - Memory scraping - MAC spoofing - Side channels attacks - Fake access network node - False or rogue MEC gateway - UICC format exploitation - User equipment compromising	- Service unavailability - Information integrity - Information destruction	- Cloud data center equipment - User equipment - Radio access/units - Light data centers - SDN, MANO, NF - RAN, RAT - Virtualization - Subscribers' data - Network services
	Data breach, leak, theft and manipulation of information	- Information integrity - Information destruction - Information confidentiality	- Subscribers' data - Subscriber geo locations - Financial data - Commercial data, IP - Configuration data - Service data

			- Network data
	Unauthorised activities/network intrusions - IMSI catching attacks - Lateral movement	- Information integrity - System integrity	- User equipment - Network services - Business services
	Identity/account or service fraud - Identity theft - Identity spoofing	- Service unavailability - Information destruction - Information integrity	- User subscription profile data - Subscribers' data
	Spectrum sensing	- Service unavailability	- RAT - Radio access units
	Compromised supply chain, vendor and service providers - Threat from third parties' personnel accessing MNO's facilities	- Service unavailability - Information integrity - Information destruction	- SDN, NFV, MANO - RAN, RAT - MEC - API - Physical infrastructure - Business applications - Security controls - Cloud, virtualisation - Network services - Business services
	Abuse of virtualization mechanisms - Network virtualization bypassing - Virtualized host abuse - Virtual machine manipulation - Data center threats - Abuse of cloud computational resources	- Service unavailability - Information integrity - Information destruction	- Virtualisation - SDN, NFV, MANO - Cloud - Network services - Business services
	Signalling threats - Signalling storms - Signalling fraud	- Service unavailability - Information integrity - Information destruction	- RAT - Radio access units - Protocols - Network services - Business services
Eavesdropping/ Interception/ Hijacking (EIH)	**Nation state espionage**	- Information integrity - Information confidentiality	- Subscribers' data - Subscriber geo locations
	Corporate espionage	- Information integrity - Information confidentiality	- Financial data - Commercial data - IP
	Traffic sniffing	- Information integrity - Information confidentiality	- Data traffic - Subscribers' data - Subscriber geo location
	Manipulation of network traffic, network reconnaissance and information gathering - Radio network traffic manipulation - Malicious diversion of traffic - Traffic redirecting - Abuse of roaming interconnections	- Information integrity - Information confidentiality	- Data traffic - Subscribers' data - Subscriber geo locations
	Man in the middle/ Session hijacking	- Information integrity - Information confidentiality	- Data traffic - Subscribers' data

			- Subscriber geo locations
	Interception of information	- Information integrity - Information confidentiality	- Data traffic - Subscribers' data - Subscriber geo locations
Physical Attacks (PA)	**Sabotage of network infrastructure (radio access, edge servers, etc.)**	- Service unavailability - Information destruction - Information integrity	- Radio access units - ICT equipment - Light data center - Cloud data center - Network services - Business services
	Vandalism of network infrastructure (radio access, edge servers, etc.)	- Service unavailability - Information destruction - Information integrity	- Radio access units - ICT equipment - Light data center - Cloud data center - Network services - Business services
	Theft of physical assets	- Service unavailability - Information destruction - Information integrity	- Radio access units - ICT equipment - Light data center - Cloud data center - Network services - Business services
	Terrorist attack against network infrastructure	- Service unavailability - Information destruction - Information integrity	- Radio access units - ICT equipment - Light data center - Cloud data center - Network services - Business services
	Fraud by MNO employees	- Service unavailability - Information destruction - Information integrity	- Radio access units - ICT equipment - Light data center - Cloud data center - Network services - Business services
	Unauthorised physical access to base stations in shared locations	- Service unavailability - Information destruction - Information integrity	- RAT - Radio access units - Network services - Business services
Unintentional Damages (accidental) (UD)	**Misconfigured or poorly configured systems/networks**	- Service unavailability - Information integrity	- Management processes - Policies - Legal - Human assets - SDN, NFV, MANO, API - RAN, RAT, MEC - Physical infrastructure - Business applications - Security controls - Cloud, virtualisation
	Inadequate designs and planning or lack of adaption - Outdated system or network from the lack of update or patch management	- Service unavailability - Information integrity	- Management processes - Policies

	- Errors from the lack of configuration change management - Poorly design network and system architecture		- Human assets - SDN, NFV, MANO - RAN, RAT - MEC - API - Physical infrastructure - Business applications - Security controls - Cloud, virtualisation
	Erroneous use or administration of the network, systems and devices	- Service unavailability - Information integrity	- Management processes - Policies - Human assets - SDN, NFV, MANO - RAN, RAT - MEC, UE, API - Physical infrastructure - Business applications - Security controls - Cloud, virtualization
	Information leakage/sharing due to human error	- Information integrity - Information confidentiality	- Data storage/repository - Management processes - Policies - Legal - Human assets - Subscribers' data - Application data - Security data - Network data
	Data loss from unintentional deletion	- Information integrity - Information confidentiality	- Management processes - Policies - Human assets - Subscribers' data - Application data - Security data - Network data
Failures or Malfunctions (FM)	**Failure of the network, devices or systems**	- Service unavailability - Information destruction - Information integrity	- Cloud data center - User equipment - RAT, Radio unit - Light data center - Network services - Business services
	Failure or disruption of communication link	- Service unavailability - Information destruction - Information integrity	- Cloud data center - Network services - Business services
	Failure or disruption of main power supply	- Service unavailability - Information destruction - Information integrity	- Cloud data center - Network services - Business services
	Failure or disruption from service providers (supply chain)	- Service unavailability - Information destruction - Information integrity	- Network services - Business services

	Malfunction of equipment (devices or systems)	- Service unavailability - Information destruction - Information integrity	- Radio access units - ICT equipment - Light data center - Cloud data center - Network services - Business services
Outages (OUT)	**Loss of resources** - Human resources - Physical resources	- Service unavailability - Information destruction - Information integrity	- Human assets - Legal - Network services - Business services
	Support services	- Service unavailability - Information destruction - Information integrity	- Human assets - Management processes - Policies - Legal - Network services - Business services
	Data network (access)	- Service unavailability - Information destruction - Information integrity	- Cloud data center - Network services - Business services
	Power supply	- Service unavailability - Information destruction - Information integrity	- Cloud data center - Network services - Business services
Disasters (DIS)	**Natural disasters** - Earthquakes - Landslides	- Service unavailability - Information destruction - Information integrity	- Radio access units - ICT equipment - Light data center - Cloud data center - Network services - Business services
	Environmental disaster - Floods, storms - Pollution, dust, corrosion - Fires, heavy winds - Unfavourable climatic conditions	- Service unavailability - Information destruction - Information integrity	- Radio access units - ICT equipment - Light data center - Cloud data center - Network services - Business services
Legal (LEG)	**Breach of service level agreement (SLA)**	- Service unavailability - Information destruction - Information integrity	- Network services - Business services
	Breach of legislation	- Service unavailability - Information destruction - Information integrity	- Network services - Business services
	Failure to meet contractual requirements and/or legislation	- Service unavailability - Information destruction - Information integrity	- Network services - Business services

Consortium

Space Hellas
www.space.gr

NCSR Demokritos
www.demokritos.gr

Telefonica I&D
www.telefonica.com

RHEA SYSTEM SA
www.rheagroup.com

INESC TEC
www.inesctec.pt

Infili Technologies PC
www.infili.com

UBITECH LTD
www.ubitech.eu

IQUADRAT R&D
www.ucm.es

ICCS
www.iccs.gr

FORSVARETS FORSKNINGSINSTITUTT
www.ffi.no

UNIVERSIDAD COMPLUTENSE DE MADRID
www.ucm.es

INSTITUTO POLITÉCNICO DO PORTO
www.ipp.pt

ERTICO ITS EUROPE
www.ertico.com

Contact Us
privateer-contact@
spacemaillist.eu

Co-funded by the European Union
6GSNS

PRIVATEER has received funding from the Smart Networks and Services Joint Undertaking (SNS JU) under the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101096110