Grant Agreement No.: 101096342
Call: HORIZON-JU-SNS-2022
Topic: HORIZON-JU-SNS-2022-STREAM-B-01-04
Type of action: HORIZON-JU-RIA

Holistic, omnipresent, resilient services
for future 6G wireless and computing ecosystems

D2.3 HORSE Landscape: Technologies, state of the art, AI policies and requirements (IT-2)

Revision: v.1.0

Work package	WP2
Task	Tasks 2.1, 2.2 & 2.3
Due date	30/09/2024
Submission date	15/11/2024
Deliverable lead	SUITE5
Version	1.0
Authors	Stefanos Venios (SUITE5), Andreas Petrou (SUITE5), Admela Jukan (TUBS), Iulisloi Zacarias (TUBS), Chukwuemeka Muonagor (TUBS), Panagiotis Gkonis (NKUA), Panagiotis Trakadas (NKUA), Nikolaos Nomikos (NKUA), Eva Rodriguez (UPC), Xavi Masip (UPC), Jordi Forne (UPC), Sofia Giannakidou (STS), Alexandros Dimos (8BELLS), Orazio Toscano (ETI), Alice Piemonti (MARTEL), Vito Cianchini (MARTEL), Jose Manuel Manjón (TID), Fabrizio Granelli (CNIT), Alessandro Carrega (CNIT), Paulo Paixão (EFACEC), Pedro Elísio (EFACEC), Manuel Angel Jimenez Quesada (ATOS), Leesa Joyce (HOLO), Anthony Pogo Medina (UMU), Emilio García de la Calera Molina (UMU)
Reviewers	Orazio Toscano (ETI), Iulisloi Zacarias (TUBS)

Abstract	*D2.3 HORSE Landscape: Technologies, state of the art, AI policies and requirements (IT-2)* is a public report that builds on the project's first iteration (IT-1) and updates the entire HORSE context, in view of IT-2 architectural design. It refreshes HORSE vision and background technologies and updates the understanding of HORSE research pillars: Cybersecurity, Networking and Artificial Intelligence. Furthermore, it updates and enriches the functional and non-functional requirements of HORSE and conveys a fresh view on the role that HORSE can play and the impact it could achieve in each of the project's Use Cases. This work will set in motion the definition of the updated HORSE architecture and ultimately steer the technical implementation of the HORSE project.
Keywords	Vision, State of the Art, Requirements, Policies, 6G, Artificial Intelligence, Cybersecurity, Networking, Data Management, Extender Reality (XR), Light Rail Transit (LRT)

DOCUMENT REVISION HISTORY

Version	Date	Description of change	List of contributor(s)
V0.1	10/06/2024	Defined Table of Contents	Stefanos Venios, Andreas Petrou (SUITE5)
V0.2	31/07/2024	Updates of functional and non-requirements for the HORSE modules	Stefanos Venios, Andreas Petrou (SUITE5), Admela Jukan, Iulisloi Zacarias, Chukwuemeka Muonagor (TUBS), Panagiotis Gkonis, Panagiotis Trakadas, Nikolaos Nomikos (NKUA), Eva Rodriguez, Xavi Masip, Jordi Forne (UPC), Sofia Giannakidou (STS), Alexandros Dimos (8BELLS), Orazio Toscano (ETI), Alice Piemonti, Vito Cianchini (MARTEL), Jose Manuel Manjón (TID), Fabrizio Granelli, Alessandro Carrega (CNIT), Manuel Angel Jimenez Quesada (ATOS)
V0.3	20/09/2024	Updates in HORSE Vision and State-of-the-art analysis	Admela Jukan, Iulisloi Zacarias, Chukwuemeka Muonagor (TUBS), Panagiotis Gkonis, Panagiotis Trakadas, Nikolaos Nomikos (NKUA), Eva Rodriguez, Xavi Masip, Jordi Forne (UPC), Orazio Toscano (ETI), Alice Piemonti, Vito Cianchini (MARTEL), Jose Manuel Manjón (TID), Manuel Angel Jimenez Quesada (ATOS), Leesa Joyce (HOLO)
V0.4	26/092024	Updates in AI data management procedures	Stefanos Venios, Andreas Petrou (SUITE5), Sofia Giannakidou (STS), Alexandros Dimos (8BELLS)

V0.5	31/10/2024	Updates in HORSE Use Cases descriptions	Paulo Paixão, Pedro Elísio (EFACEC), Leesa Joyce (HOLO), Anthony Pogo Medina (UMU), Emilio García de la Calera Molina (UMU)
V0.6	1/11/2024	Updates in Network Services & Threats	Fabrizio Granelli, Alessandro Carrega (CNIT)
V0.7	4/11/2024	Addition of new functional requirements, removal of functional requirements incl. justification, mapping of requirements to Use Cases	Stefanos Venios, Andreas Petrou (SUITE5), Admela Jukan, Iulisloi Zacarias, Chukwuemeka Muonagor (TUBS), Eva Rodriguez, Xavi Masip, Jordi Forne (UPC), Paulo Paixão, Pedro Elísio (EFACEC), Leesa Joyce (HOLO), Anthony Pogo Medina (UMU), Emilio García de la Calera Molina (UMU)
V0.9	12/11/2024	Version for internal peer review.	Stefanos Venios (SUITE5), Orazio Toscano (ETI), Iulisloi Zacarias (TUBS)
V1.0	15/11/2024	Final version for submission.	Stefanos Venios (SUITE5), Fabrizio Granelli (CNIT)

Disclaimer

Copyright notice

Project co-funded by the European Commission in the Horizon Europe Programme		
Nature of the deliverable:	R	
Dissemination Level		
PU	*Public, fully open, e.g. web*	**x**
SEN	*Sensitive, limited under the conditions of the Grant Agreement*	
Classified R-UE/ EU-R	*EU RESTRICTED under the Commission Decision No2015/ 444*	
Classified C-UE/ EU-C	*EU CONFIDENTIAL under the Commission Decision No2015/ 444*	
Classified S-UE/ EU-S	*EU SECRET under the Commission Decision No2015/ 444*	

* *R: Document, report (excluding the periodic and final reports)*
DEM: Demonstrator, pilot, prototype, plan designs
DEC: Websites, patents filing, press & media actions, videos, etc.
DATA: Data sets, microdata, etc
DMP: Data management plan
ETHICS: Deliverables related to ethics issues.
SECURITY: Deliverables related to security issues
OTHER: Software, technical diagram, algorithms, models, etc.

Executive summary

This document builds on the project's first iteration (IT-1) and updates the entire HORSE context, in view of IT-2 architectural design; from the project's vision and research pillars to the use cases, the functional and non-functional requirements, and the considered network services, threats and AI data management procedures.

After a brief introduction to outline the document purpose and structure, it refreshes HORSE vision and background technologies, verifying it conveys the message for the project mission and its underlying technologies in a clean and concise way.

The research pillars of HORSE, Cybersecurity, Networking and Artificial Intelligence, are updated next, taking into account the developments in the time period between the beginning of the project and the conclusion of its first phase.

In the security domain, the document explores the implications of 6G networks, including new technologies/architectures, physical layer security, privacy protection, and risks and threats. Threat identification, characterization, and modelling techniques such as anomaly detection and threat modelling are also examined. In the networking domain, the document addresses network exposure capabilities beyond 5G, energy efficiency, digital twin design, and the role of the physical layer in 6G networks. Furthermore, it explores AI-enabled solutions for security enhancement, intent-based networking, as well as generative AI.

The HORSE use cases section updates the descriptions of the two project Use Cases: Secure Smart LRT Systems (SS-LRT) and Remote Rendering to Power XR Industrial (R^2XRI). Most importantly, it conveys a fresh view on the role that HORSE can play in each Use Case and the impact it could achieve. Therefore, for each Use Case, updated information on the HORSE infrastructure, workflows and demonstration usage scenarios, is given.

The functional and non-functional requirements of HORSE are further updated and enriched, under the light of the experience gained by the HORSE project consortium partners, as well as the comments received during the mid-term review. The updated list of requirements will act as input to the second iteration of the platform architectural design, and depending on their priority, these requirements shall be developed in the project's second iteration (IT-2).

Additionally, the document updates the description of the 6G network services and threats that the HORSE project will consider, including API exposure, AI- and ML-enabled operation, AI data training and heterogeneity research areas.

Finally, the document crafts more the HORSE AI data management procedures considered in the project, with examples deriving from the demonstrations achieved during the first phase of the project.

The end goal of this document is to offer a thorough understanding of the landscape surrounding HORSE, enabling stakeholders, researchers, policymakers, and practitioners to make informed decisions and recommendations, ensuring the proper implementation of the project.

Table of Contents

DOCUMENT REVISION HISTORY **2**
Disclaimer **4**
Copyright notice **4**
Executive summary **5**
Table of Contents **6**
List of Figures **8**
List of Tables **9**
Abbreviations **10**
1. Introduction **13**
1.1. Purpose of this Document 13
1.2. Methodology 13
1.3. Document Structure 14
1.4. Relation to other Work Packages and Tasks 14
2. HORSE Vision and Background **15**
2.1. Vision 15
2.2. Underlying Technologies 15
3. HORSE Research Pillars and State-of-the-art Analysis **17**
3.1. Security 17
3.1.1. Security in the 6G world 17
3.1.1.1. Security implications of AI-ML architecture 17
3.1.2. Risks and threats 18
3.1.3. Threats identification, characterization, and modelling 19
3.1.3.1. Generative AI-Enhanced Threats 21
3.1.3.2. Emerging Threat Vectors with GenAI 21
3.1.3.3. Anomaly Detection Tailored for GenAI-Related Threats 21
3.2. Networking 22
3.2.1. Network exposure capabilities beyond 5G 22
3.2.2. Energy Efficiency 23
3.2.3. Digital Twin Design 24
3.2.4. Physical-Layer in 6G Networks 25
3.3. Artificial Intelligence 26
3.3.1. AI-enabled solutions for security enhancement in 6G and threat mitigation 26
3.3.2. Intent-based Networking 28
3.3.3. Generative AI 28
4. HORSE Use Cases **30**

4.1. HORSE Use Case 1 - Secure Smart LRT Systems (SS-LRT) 30
4.1.1. Demonstration: Usage Scenarios 30
4.2. HORSE Use Case 2 - Remote Rendering to Power XR Industrial (R^2XRI) 32
4.2.1. Demonstration: Usage Scenarios 32
4.2.1.1. The Necessity of Network Infrastructure for XR 33
4.2.1.2. How Network Quality Influences XR Performance and Experience 33
4.2.1.3. Security: Protecting Against Network Attacks 34
4.2.1.4. Validating HORSE Through XR Test Cases 34
5. HORSE Functional & Non-Functional Requirements 36
5.1. Mapping HORSE requirements to Use Cases for validation 46
6. HORSE Network Services and Threats 48
6.1. 6G Services considered in HORSE 48
6.1.1. API exposure 48
6.1.2. AI- and ML-enabled operation 48
6.1.3. AI data training 49
6.1.4. Heterogeneity 49
6.2. 6G threats considered in HORSE 50
6.2.1. Secure Smart LRT Systems Use Case 50
6.2.2. Remote Rendering to Power XR Industrial Use Case ($R^2$2XRI) 50
7. HORSE AI Data Management 51
7.1. Elasticsearch Database of the Smart Monitoring component 51
7.2. Data Management Procedures 52
7.3. 5G/6G Network Traffic Data 54
7.4. Human Interaction 55
8. Conclusions 57
References 58

List of Figures

Figure 1: Gen AI in the Cyber Threat Landscape 20
Figure 2: SS-LRT Use Case 30
Figure 3: Use Case 1 - Solution 31
Figure 4: Use Case 1 - Attack representation 31
Figure 5: Use Case 2 - Architecture 33
Figure 6: Use Case 2 - Example of 3D model with and without Stream enabled 34
Figure 7: Use Case 2 - Multi-User as Network stress test 35

List of Tables

Table 1: List of HORSE functional requirements 43
Table 2: List of HORSE non-functional requirements 46
Table 3: Mapping HORSE requirements to Use Cases for validation 47

Abbreviations

5GC	5G Core Network
AF	Application Function
AI	Artificial Intelligence
AMF	Access and Mobility Management Function
API	Application Programming Interface
AR	Augmented Reality
AUSF	Authentication Server Function
CAD	Computer Aided Design
CAPIF	Common API Framework
CFL	Collaborative Federated Learning
CPS	Cyber-Physical Systems
DAE	Deep Autoencoder
DDoS	Distributed Denial of Service
DL	Deep Learning
DNN	Deep Neural Network
DoS	Denial of Service
DRL	Deep Reinforcement Learning
DT	Digital Twin
Dx.x	Deliverable x.x
EE	Energy Efficiency
FDL	Federated Deep Learning
FL	Federated Learning
GAN	Generative Adversarial Network
GenAI	Generative Artificial Intelligence
GRU	Gated Recurrent Unit
IBN	Intent-Based Networking
IDS	Intrusion Detection Systems
IIT	Industrial Internet of Things
IoT	Internet of Things
IT	Information Technology

KPI	Key Performance Indicator
LLM	Large Language Model
LRT	Light Rail Transit
LSTM	Long-Short Term Memory
MIMO	Multiple-Input Multiple-Output
MITM	Man in the Middle
ML	Machine Learning
Mxx	Month xx
NDT	Network Digital Twin
NEF	Network Exposure Function
NF	Network Function
NFV	Network Function Virtualisation
NOMA	Non-Orthogonal Multiple Access
NSSF	Network Slice Selection Function
NWDAF	Network Data Analytics Function
OCC	Operational Command Centre
OT	Operational Technology
PCF	Policy Control Function
PLS	Physical Layer Security
RAG	Retrieval Augmented Generation
RAN	Radio Access Network
R^{2}XRI	Remote Rendering to Power XR Industrial
RBM	Restricted Boltzmann Machine
RL	Reinforcement Learning
RNN	Recurrent Neural Networks
SBA	Service-Based Architecture
SBI	Service-Based Interface
SDN	Software Defined Networking
SS-LRT	Secure Smart LRT Systems
TL	Transfer Learning
Tx.x	Task x.x
UAV	Unmanned Aerial Vehicle

V2X	Vehicle-to-Everything
VLC	Visible Light Communications
VM	Virtual Machine
VR	Virtual Reality
WPx	Work Package x
XR	Extended Reality

1. Introduction

1.1. Purpose of this Document

This document builds on the project's first iteration (IT-1) as described in the first version of "HORSE Landscape: Technologies, state of the art, AI policies and requirements" [15]) and updates the entire HORSE context, in view of IT-2 architectural design. Its purpose is to incorporate the experience of the project partners during the first 18 months of the project, the comments received by the reviewers during the mid-term review and the developments in the scientific landscape during the last year, in order to update the project's vision, the investigation and analysis of the technologies and their state of the art, the positioning of the Use Cases, the requirements and the AI data management relevant to HORSE. By consolidating information from various sources and leveraging the expertise of multiple partners, this document aims to inform and support the decision-making process, guiding the second architectural design phase of HORSE, to be documented in the upcoming deliverable D2.4. It offers a thorough understanding of the landscape surrounding HORSE, enabling stakeholders, researchers, policymakers, and practitioners to make informed decisions and recommendations, ensuring the proper implementation of the project.

1.2. Methodology

The development of this document has been a collaborative effort involving multiple partners. The methodology was based on the existing work presented in D2.1.

The methodology can be summarized as follows:

- **Requirements Gathering:** The partners collectively identified the areas of the document that needed updates and defined the requirements for each section. A brief literature review was conducted to identify existing research, reports, policies, and industry standards related to the contents of the document. This served as a foundation for the subsequent analysis.
- **Data Collection and Analysis:** The partners collaborated in gathering data from various sources, including academic research papers, industry publications, government regulations, and relevant online resources. In addition, the lessons learnt by the project partners during the first 18 months of the project and the comments received by the reviewers during the mid-term review were treated as valuable document input. The partners utilized their expertise and collective knowledge to systematically analyse the collected input and to work towards the categorization, synthesis, and comparison of the pertinent content.
- **Document Structure and Writing:** A structured outline for the document was developed based on the outcomes of the analysis.
- This ensured a logical flow of information and facilitated the presentation of information. The partners collaborated on writing the content for each section, drawing upon their respective skills and insights.
- **Review and Validation:** The draft document underwent several rounds of rigorous review by all partners. Feedback and suggestions were collected and incorporated, and revisions were made to enhance the document's quality and comprehensiveness. The final version of the document represents the collective knowledge, competence, and consensus of the partner consortium.

By following this methodology, the partners aim to provide a robust and reliable resource that informs stakeholders, researchers, policymakers, and practitioners about the current state of the HORSE project.

1.3. Document Structure

This document is structured into several sections to convey the collected information accurately and with clarity. The following is an overview of the document's structure:

- **Section 1: Introduction:** This section introduces the document, outlining its purpose, methodology, relation to other work packages and tasks, and the structure of the document itself.
- **Section 2: HORSE Vision and Background:** This section updates the consortium's collective understanding of the HORSE vision and the underlying technologies and conveys this in a structured way to the reader.
- **Section 3: HORSE Research Pillars and State-of-the-art Analysis:** This section reviews the three main research pillars of HORSE: Security, Networking, and AI, under the light of the experience gained by the HORSE project consortium partners, as well as the comments received during the mid-term review.
- **Section 4: HORSE Use Cases:** This section updates the understanding of the role that HORSE can play the two specific HORSE Use Cases: Secure Smart LRT Systems (SS-LRT) and Remote Rendering to Power XR Industrial (R^2XRI). For each Use Case, updated information on the HORSE infrastructure, workflows, demonstration usage scenarios, and test scenarios, is given.
- **Section 5: HORSE Functional & Non-Functional Requirements:** This section updates the list of requirements for the various HORSE modules. These requirements serve as guidelines for the second architectural design phase.
- **Section 6: HORSE Network Services and Threats:** This section updates the description of the 6G network services and threats that the HORSE project will consider.
- **Section 7: HORSE AI Policies:** In this section the AI data management policies related to the HORSE project are addressed.
- **Section 8: Conclusions:** The document concludes by summarizing the main findings, emphasizing the importance of the HORSE project, and providing an outlook for upcoming developments.

1.4. Relation to other Work Packages and Tasks

This deliverable is the 2nd iteration of the output of tasks *T2.1 – Market radar and baseline technologies identification, T2.2 – Overall requirements specification and identification and T2.3 – AI data collection strategy and procedures.* They all started in M01 and ended in M21. Sections 2 and 3 are associated with T2.1, Sections 4 and 5 with T2.2 and Sections 6 and 7 with T2.3. This deliverable feeds task *T2.4 – Architectural design,* which will produce an updated description of the architectural design, to be documented in deliverable D2.4. The deliverable at hand, in conjunction with deliverable D2.4, will constitute the final functional design of the HORSE platform, which is developed in WP3 and WP4, and integrated and validated in WP5.

2. HORSE Vision and Background

2.1. Vision

The consortium envisions HORSE as a robust and advanced infrastructure designed to foster the development of innovative services within 6G networks. The HORSE platform aims to be human-centric, open-source, green, and sustainable. It faces the significant challenge of operating 6G infrastructure for smart connectivity and service management, prioritizing effectiveness at the intersection of 6G connectivity, computing infrastructure management, and security.

Some of the key technologies used in 6G networks are artificial intelligence (AI), molecular communication, quantum communication, terahertz (THz) communication, and millimetre wave (mm-Wave) radio frequencies. These technologies offer enhanced speeds and new forms of communication that traditional technologies lack. Moreover, they will be primarily software-driven, meaning many functions will be managed by software rather than relying solely on hardware. These technologies will equip the network with new, intelligent, and innovative capabilities, enhancing the user experience, particularly in the context of mobility and resource volatility. Among these technologies, AI is recognized as a key component of 6G networks.

AI technology represents a promising solution that enhances security measures when integrated with 6G technology. In the HORSE project, we are leveraging AI to identify and mitigate security issues related to 6G technologies and architectures. Additionally, AI will play a crucial role in facilitating secure and reliable orchestration of 6G services. HORSE is managing services using high-level policies and proactive strategies, integrating them into a digital twin (DT) environment.

Furthermore, human-centric communication technology is essential for the development and utilization of future networks. This approach encompasses two key concepts: collective intelligence and sociotechnical design, which serve as the foundational pillars for future architectural design. By promoting user engagement, the human-centric approach can also foster trust in AI, as its actions become more explainable to users. In HORSE, we are developing an AI-assisted human-centric platform that ensures device connectivity, minimizes latency, optimizes resource and data utilization, and enhances security and trust capabilities for 6G-enabled smart devices.

The envisioned HORSE platform is being validated through highly innovative, high-performance, and representative scenarios, characterized by the distributed operation of the transport system and multi-user remote rendering in extended reality. These scenarios allow to evaluate the adaptability of the HORSE platform to specialized domains with specific constraints and specifications.

2.2. Underlying Technologies

HORSE is a complex platform designed to foster the development of innovative services within 6G networks. It integrates a wide range of technologies in the Cybersecurity, AI, and Networking research areas.

This section outlines the underlying technologies that will form the basis of the HORSE platform, including threat detection and prediction, impact analysis, proactive mitigation and prevention against threats and breaches, Network Function Virtualisation (NFV), intent-based networking (IBN), and AI-based technologies.

In the 6G era, **Service-Based Architectures (SBAs)** will play a vital role in service delivery. SBAs offer a flexible, modular framework that separates service logic from network infrastructure, allowing for rapid deployment and scalability of personalized services. This adaptability enables network operators to swiftly respond to changing user demands and supports diverse applications, making 6G networks highly flexible and dynamic [1].

Network Function Virtualization (NFV) separates network functions (NFs) from their underlying hardware, enabling them to operate on standard servers or in the cloud. This virtualization enhances flexibility and scalability when implementing network services. NFV enables operators to rapidly develop services and dynamically allocate resources in response to changing consumer demands [2], making it crucial for the successful delivery of 6G networks.

Digital Twins (DT) are virtual representations of real-world systems that enable continuous monitoring, simulation, and enhancement. They are expected to play a vital role in developing complex 6G network infrastructures by simulating components, ultimately improving efficiency and performance [3]. Additionally, they serve as sandbox environments for testing new network services. Specifically, in the HORSE platform, two DTs are considered, one for threat prediction, and the other for impact analysis.

Artificial Intelligence (AI) can enhance intrusion detection, prevention, and response to the complex cybersecurity needs of 6G networks more effectively than traditional measures. It identifies anomalies in network traffic, predicts potential attacks, and drives preventive actions. AI is also used to analyse data sets to detect intricate attack patterns that are challenging for human operators. However, challenges remain, such as the need for large training datasets and the risk of adversarial attacks. Overall, AI presents a promising solution for 6G network cybersecurity [4].

Generative AI (GenAI) especially through Large Language Models (LLMs), is playing a pivotal role in the automation of complex processes and improving decision-making. In the cybersecurity domain, GenAI can enhance threat detection and mitigation by processing large volumes of data and generating intelligent responses. LLMs are increasingly being considered in various cybersecurity areas, including vulnerability detection, malware analysis, phishing detection, and anomaly detection in network traffic. Their potential for automating security strategies makes them a promising solution for addressing cybersecurity challenges [5].

3. HORSE Research Pillars and State-of-the-art Analysis

HORSE, a highly complex research endeavour, harnesses a multitude of cutting-edge technologies sourced from three main research domains, specifically Cybersecurity, Networking and AI, to achieve its ambitious objectives. This interdisciplinary approach empowers HORSE to tackle intricate challenges at the intersection of these fields, opening new avenues for groundbreaking advancements. These main research areas were presented in a state-of-the-art analysis in deliverable D2.1 [15]; after the conclusion of the first phase of the project, the pertinent sections were reviewed in the light of the experience gained by the HORSE project consortium partners, as well as the comments received during the mid-term review. Developments from the past 18 months were taken into account, along with a continued focus on the work planned for the second half of the project.

3.1. Security

3.1.1. Security in the 6G world

As it exposed at D2.1 [15], 6G network will be closer to humans enabling unprecedent levels of integration across daily life. At this point security will be a core point to protect both individual privacy and societal stability. Besides the issues inherited from 5G and B5G there are new topics in the 6G security context:

- Trust modelling, trust policies and trust mechanisms should be defined and standardized since the 6G world is an extremely heterogeneous environment with multi-domain deployments and operators.
- Quantum computing, as discussed in D2.1, can be used to easily break current encryption systems. During last year NIST provided new research to help system administrator to transition to new standards as soon as possible [6] with a new encryption algorithm [7] that provide a new framework to resist future attacks by quantum computers. That type of algorithms could be to impact in the efficiency of the 6G and B5G network.
- The AI-ML architecture, due to its fundamental role in the new security aspects of 6G. It will be addressed in a subsequent subsection.

3.1.1.1. Security implications of AI-ML architecture

AI and ML have gone through groundbreaking developments in recent years. This new technology will be crucial in the 6G networks due to a deeper integration of emerging AI tools, which introduces new topics related to the security environment:

- Proposals for beyond 5G and 6G architectures in literature introduce AI-driven orchestration systems. Any vulnerability in these systems could lead to severe consequences, as they manage critical infrastructures. Some attacks related to AI-driven systems are:
  - Model Stealing: Attackers achieve information related to the AI model to identify its behaviour and its vulnerabilities.
  - Adversarial Attacks: implies data injected to deceive the AI models.
  - Data Poisoning: relies on influence in the AI decision during the training phases.

- AI-ML can provide components and architectures that detect and prevent attacks., This is one of the main research areas in which the HORSE project is involved and it is discussed in more details further through HORSE deliverables.
- On the other hand, there are AI-driven tools that attackers can use to plan and execute their attack. These tools are currently in research and development, and some of those related to network environment include:
  - Automated Vulnerability scanning and exploitation. This automates the discovery of system weaknesses, such as insecure configurations or unpatched software versions.
  - Botnet coordination. This tool allows attackers to deploy a smarter DDoS attack using orchestrators to make decisions independently during the attack, helping them avoid detection.

3.1.2. Risks and threats

6G networks promise unprecedented advancements in connectivity, speed, and data processing. However, as the technology's capabilities expand, so does the attack surface of the system, along with the potential security risks and threats.

At a high level, several macro-risks can be identified. Firstly, data privacy becomes a concern as the amount of personal data transferred and stored will increase exponentially with the anticipated rise in Internet of Things (IoT) devices, smart city infrastructures, and AI integrations. This data could be vulnerable to theft and misuse if not appropriately secured. Secondly, as network complexity increases, it presents more points of vulnerability for attackers to exploit. With 6G networks projected to be virtually ubiquitous, connecting almost everything, a single breach could lead to widespread system disruptions or infrastructure failure. Moreover, with 6G's reliance on AI for network optimization and management, malicious actors could use AI to conduct sophisticated, targeted attacks. This introduces a new level of risks and threats.

More specifically, the introduction of GenAI opens up additional security challenges. In recent years, GenAI has shown potential for both constructive applications and threats to cybersecurity. As highlighted in [8], this technology enables attackers to create sophisticated phishing schemes, malware, and malicious code that elevate the sophistication and targeting of cyberattacks. The risks go beyond simple attacks, as these AI-driven strategies allow intrusions that are difficult to detect and mitigate.

AI poisoning is another emerging threat in 6G networks. For example, in data poisoning, attackers can insert or modify training samples, potentially steering AI predictions toward their own objectives. In Federated Learning (FL) contexts, model poisoning enables attackers to control AI parameters, altering model outputs and affecting network decisions. Access to training datasets not only threatens model integrity but also exposes vast amounts of user data, thereby risking user privacy [9].

In conjunction with these AI-specific threats, the increased use of small cells for coverage in 6G networks could lead to physical tampering. Supply chain vulnerabilities could also provide an avenue for inserting malicious hardware or software into the 6G infrastructure. These aspects raise concerns regarding the security of networks [10], [11], [12]. Further risks and threats can be identified and organized based on different criteria. Technology-related risks and threats encompass specific risks associated with various technologies integrated into 6G networks. For example, AI-related risks include poisonous attacks, evasion attacks, model extraction, and model inversion attacks. Visible Light Communication (VLC) is vulnerable to eavesdropping and jamming. Terahertz technology faces access control attacks and eavesdropping. Blockchain is at risk of Sybil attacks, re-entrance attacks, and privacy attacks.

Quantum communication can be targeted through quantum cloning attacks and quantum collision attacks. Molecular communication faces flooding (DoS) attacks, jamming, desynchronization, and collision attacks.

The risks and threats can also be categorized based on specific architecture layers. Sensing layer risks include physical attacks, theft of information, attacks on visible light communications, and sniffing attacks. Edge layer attacks involve data poisoning, evasion attacks, and privacy infractions. Control layer attacks target Software Defined Network (SDN)

, cloud computing services, and ML models. Application layer attacks pose risks in intelligent network management, such as DoS and Man-in-the-Middle (MITM) attacks, and unauthorized access to systems through intent-based interfaces.

Furthermore, application-related risks and threats arise from specific applications in 6G networks. UAVs are susceptible to physical attacks, spoofing, eavesdropping, DoS, and hijacking attacks. Holographic applications face unsecured data transmission and privacy concerns. Extended reality is vulnerable to security issues related to sharing personal data, data leakage, and unauthorized access to confidential information. Connected autonomous vehicles are at risk of capturing sensor data, physical hijacking, falsifying cloud service data, and confidentiality threats. DTs can be tampered with or intercepted, compromising privacy, and IoT information can be altered, infringing upon system privacy. Cyber-physical systems (CPS) face unauthorized access, data breaches, manipulation of control systems, and privacy violations.

Lastly, open Radio Access Network (RAN) security risks involve insufficient isolation, privacy breaches, misconfiguration, supply chain risks, and increased opportunities for attackers. These risks and threats highlight the challenges that need to be addressed to ensure the security and resilience of 6G networks. Effective security measures, protocols, and standards must be developed and implemented to mitigate these risks and protect the integrity, privacy, and functionality of the network and its applications [13], [14].

3.1.3. Threats identification, characterization, and modelling

Following up D2.1 [15], the cybersecurity threat landscape continues to evolve, becoming increasingly complex. As such, efficient threat detection remains a critical priority but we can observe that referring to the two primary approaches recognized in the literature (nominally the Signature-Based approach, which is effective for known attacks but limited in scope, and the Statistic-Based approach, now frequently enhanced by Machine Learning (ML) techniques, allowing for the recognition of new and evolving threat patterns) something new is appearing.

In recent times, in fact, the emergence of GenAI has reshaped the cybersecurity landscape significantly. On the one hand, malicious actors have begun leveraging GenAI to create sophisticated cyber threats. For instance, GenAI can be used to generate highly convincing phishing attacks that are difficult for traditional defences to detect. Additionally, GenAI tools can automate the development of malware, making it more adaptable and harder to trace.

Conversely, cybersecurity professionals are also harnessing GenAI to bolster defence mechanisms. GenAI is being deployed to enhance threat detection processes, including the development of advanced anomaly detection systems that can identify unusual patterns indicative of a cybersecurity threat. Furthermore, GenAI has proven effective in countering phishing attacks by improving email filtering systems and developing advanced pattern recognition algorithms that can detect subtle signs of malicious content.

In summary, the impact of GenAI on the Cybersecurity Threat Taxonomy is multifaceted. It has expanded both the threat landscape with more sophisticated attack vectors, and it has

enhanced defensive measures through improved threat detection and response strategies. As the field progresses, the strategic integration of GenAI into cybersecurity practices will be essential for maintaining robust defence mechanisms in an increasingly digital world.

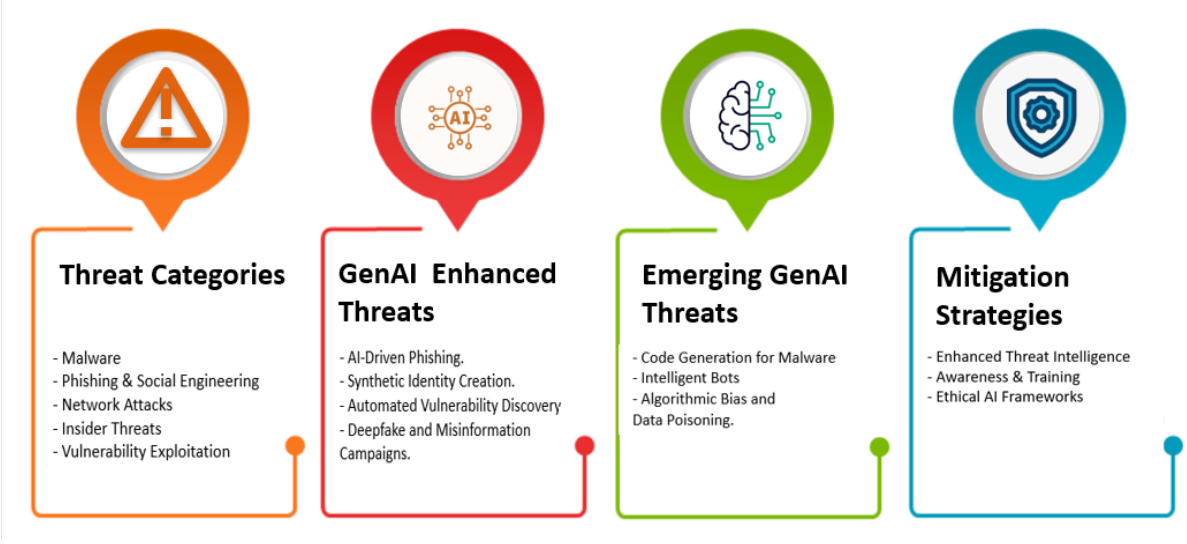

Figure 1: Gen AI in the Cyber Threat Landscape

Figure 1 briefly summarizes the:

- Traditional Threat Categories
  - Malware (e.g., ransomware, spyware)
  - Phishing & Social Engineering
  - Network Attacks (e.g., DDoS, Man-in-the-Middle)
  - Insider Threats
  - Vulnerability Exploitation (e.g., zero-day, misconfigurations)
- Generative AI-Enhanced Threats
  - AI-Driven Phishing: Tailored, highly convincing messages with GenAI-generated content
  - Synthetic Identity Creation: Deepfake profiles using AI-generated images and text for fraud and social engineering.
  - Automated Vulnerability Discovery: GenAI models to predict and exploit system vulnerabilities.
  - Deepfake and Misinformation Campaigns: Realistic audio, video, and images for social engineering at scale.
- Emerging Threat Vectors with GenAI
  - Code Generation for Malware: Using GenAI models to develop polymorphic malware.
  - Intelligent Bots: Chatbots powered by GenAI that impersonate real users for data extraction.
  - Algorithmic Bias and Data Poisoning: Attacking GenAI models to embed bias or malicious data.
- Mitigation Strategies
  - Enhanced Threat Intelligence: Incorporate AI monitoring tools to detect unusual patterns.
  - Awareness & Training: Educate on recognizing AI-enhanced social engineering.
  - Ethical AI Frameworks: Implement guidelines to counteract misuse in AI applications.

3.1.3.1. Generative AI-Enhanced Threats

With the advancement of GenAI, cyber threats have taken on new forms, presenting increasingly sophisticated challenges. One prominent area is AI-driven phishing, where tailored, compelling messages are crafted using GenAI-generated content. These messages can accurately mimic legitimate communication styles, making them difficult to detect and more effective at deceiving targets. This capability allows attackers to execute socially engineered attacks at scale, exploiting both personal and organizational vulnerabilities.

Another alarming evolution is in Synthetic Identity Creation. GenAI facilitates the creation of deepfake profiles, leveraging AI-generated images and text to construct realistic but fake identities. These synthetic identities are employed in fraudulent activities and social engineering scams, where they can infiltrate organizations, manipulate trust, and extract sensitive information. Such activities significantly complicate identity verification processes and pose a substantial threat to traditional security systems.

Beyond individual attack vectors, GenAI has been instrumental in Automated Vulnerability Discovery. GenAI models can predict undiscovered vulnerabilities and dynamically exploit them by analysing vast amounts of system data.

Additionally, deepfake and misinformation campaigns have emerged, where realistic audio, video, and images are produced for malicious purposes such as social engineering, propaganda, and defamation. These GenAI-driven misinformation efforts are capable of undermining trust in digital content, influencing public opinion, and destabilizing societal structures.

3.1.3.2. Emerging Threat Vectors with GenAI

The landscape of emerging threat vectors is expanding with GenAI, particularly in the realm of Code Generation for Malware. Attackers are utilizing GenAI models to develop polymorphic malware, which can alter its code to evade detection continuously. This capability not only enhances the malware's persistence within targeted systems but also complicates traditional methods of threat analysis and signature-based detection.

The rise of Intelligent Bots signifies another key development. GenAI-powered chatbots can impersonate real users, enabling attackers to extract sensitive information through seemingly legitimate conversations. These bots can adapt their responses in real-time, making them effective tools for spear-phishing campaigns and other forms of social engineering attacks. This kind of sophisticated automation allows for a broader reach and increased efficacy of data extraction efforts.

GenAI also introduces unique challenges through Algorithmic Bias and Data Poisoning. Adversaries can manipulate GenAI models by introducing biased or malicious data, which can skew the decision-making processes of AI systems. Data poisoning attacks compromise the integrity of training datasets, potentially leading to AI-driven systems making flawed or harmful decisions. These vulnerabilities underscore the need for robust AI governance and the development of defences against adversarial attacks targeting AI models directly.

3.1.3.3. Anomaly Detection Tailored for GenAI-Related Threats

In response to these evolving GenAI-related threats, anomaly detection systems must adapt by harnessing the power of AI themselves. Traditional anomaly detection relies on predefined rules, which prove inadequate against the dynamic and sophisticated nature of GenAI-

enhanced attacks. Modern approaches focus on ML models capable of identifying unusual patterns and deviations from the norm without prior knowledge of specific threats.

GenAI-augmented anomaly detection leverages unsupervised ML techniques, such as clustering and Deep Learning (DL), to detect subtle irregularities in massive datasets. These systems can identify anomalous behaviours indicative of GenAI-driven activities, like unexpected communication patterns or sudden changes in network traffic. By continuously learning from new data, these models can adapt to evolving threat landscapes, providing real-time detection and alerting capabilities.

Additionally, integrating explainable AI techniques into anomaly detection frameworks enhances transparency, allowing cybersecurity professionals to understand the reasoning behind detections. This is crucial for distinguishing between benign anomalies and actual threats. As GenAI continues to influence both the capabilities of adversaries and the defence strategies of cybersecurity teams, ongoing advancements in anomaly detection remain essential to ensuring robust and proactive security measures.

3.2. Networking

3.2.1. Network exposure capabilities beyond 5G

One of the new paradigms introduced by 5G and that offers an enormous capacity for innovation is its programmability through 5G Core Network (5GC). Specifically, exposing features and functions of the network through APIs to external entities (third parties), such as developers, to achieve a more secure and efficient access to network components while expanding the possibilities.

A key feature of 5GC is that the primarily service-based architecture (SBA) makes this network type inherently flexible [16]. This means that NFs that compose 5GC functionalities (AMF, PCF, AUSF, NSSF, etc.) can communicate with each other and access their services if authorized, since service-based interfaces (SBIs) are exposed.

The continuous evolution of the 5GC has led to the standardization of a flexible mechanism by 3GPP: the Network Exposure Function (NEF) [16]. Its primary mission is to securely expose network data and capabilities to third parties. The NEF acts as an intermediate point between the NFs in the network core and external applications. In other words, NEF enables external applications to consume data from the core NFs through centralized and secured entry points. These APIs are used, for example and among other things, for external Application Functions (AFs) to modify the behavior of the network. Which without proper monitoring and security features can result in a major security breach. In any case, there are clears benefits of network exposure through the NEF, for example, limiting the complexity of the underlying network, monetizing some network features, and controlled access for external AFs.

A key part of the NEF is the NEF Northbound interface, which is a RESTful API in charge of many procedures between the NEF and an external AF. Among these procedures we can find the securitization of communication. The NEF Northbound APIs also have a service-based approach, which allows activities such as subscriptions to services or notifications to take place between the NEF and external entities using the APIs. NEF Northbound APIs are based on Common API Framework (CAPIF) [17], whose objective is to unify and standardize the use of exposed 5G capabilities. One of the most interesting features of CAPIF, related to the possible security breach mentioned above, is the authorization of API invokers. This is a way of ensuring

that the entities using the network exposed functions are verified. Furthermore, the use of a unified framework such as CAPIF provides an abstraction layer which simplifies the heterogeneity of the network. Therefore, many applications do not need to be modified to use 5G capabilities.

The exposure of NFs and capabilities opens a very diverse range of scenarios both in the present and future, related, for example, to network slicing, ML, Edge Computing use cases, Vehicle-to-Everything (V2X), AR/VR (Augmented Reality / Virtual Reality) and, in short, any scenario that may have exposed capabilities of a NF in 5GC.

Another relevant 5G function is Network Data Analytics Function (NWDAF) [18], used for collecting data (KPIs and information about different network domains), and provide analytics-based statistics to 5G core functions. While this is a powerful mechanism to introduce AI/ML and automation control-loops in network management is also a risk, since a new point is exposed for various types of malicious attacks, and therefore the general security recommendations regarding 5G network elements should be applied here [19].

It is expected that this openness of 5G networks via the exposure functions, APIs for third party vertical applications and the general trend of using AI in network management will continue expanding more as part of 6G. Thus, it is critical to address security topics in the design of 6G architecture and not treat them as an afterthought, considering the potential vulnerabilities associated with exposure APIs, network data and the applicability of AI to network automation.

3.2.2. Energy Efficiency

The large number of interconnected devices on the internet (IoT) along with the ever-increasing demands for high data rates, seamless connectivity as well as the support of advanced services and applications necessitates a holistic network redesign where the optimization of various performance metric should be considered. In the new era of 6G networks, where a mass number of devices is connected, one such metric is energy efficiency (EE) [20]. To this end, the goal is to reduce the environmental footprint of the connected devices and leverage flexible network deployments.

In the 6G landscape, the network concept is constantly redefined, according to traffic conditions and other important metrics. To this end, data gathered from the connected devices are used to optimize various performance metrics, via the deployment of advanced ML algorithms. However, data collection and processing in a unique cloud server would not only result in a single point of failure, but also in a high computation load and energy footprint. Therefore, various efficient ML techniques have been proposed over the last years, in an effort to divide the computational load in the participating devices. Once such technique is FL [21], where local ML models are generated in each one of the participating nodes. Afterwards, once training per node is finalized, the local model parameters are sent to a master aggregation server for model update. Hence, not only computational load is balanced among the local devices, thus leveraging EE, but also privacy is enhanced as well, which is a crucial issue in 6G communications, since transmission of sensitive data does not take place.

In the same context (i.e., load balancing) other novel techniques include the decoupling of connected devices from specific access points (i.e., base stations – BSs in the cellular network terminology). To this end, the concept of cell-free resource allocation has emerged over the last decade, where a mobile terminal can be served by multiple access points according to its signal strength and overall interference [22]. Hence, traffic and signalling load is balanced among the active APs in a specific geographical area.

Finally, non-orthogonal multiple access (NOMA) can address resource limitations by serving multiple devices on the same spectral and temporal resources, thus reducing the need for complex resource utilization calculations [23]. NOMA enables resource sharing between users and exploits their channel power level differences.

3.2.3. Digital Twin Design

Network Digital Twins (NDTs) are CPS that simulate and model physical assets or processes in real time. These systems are becoming increasingly popular in industrial sectors such as manufacturing, healthcare, and transportation, as they can help optimize processes, reduce costs, and improve overall efficiency. One of the most significant trends in NDTs is the integration of ML and AI. By incorporating ML algorithms, DT networks can become more intelligent and autonomous, enabling them to make decisions and predictions based on real-time data.

NDT consist of creating a virtual model of a network infrastructure that can be used for monitoring, troubleshooting, and optimizing network performance. These DTs are typically created by collecting data from the network in real-time and using ML algorithms to build a predictive model of network behaviour.

One of the key advantages of using DTs for network management is their ability to provide real-time visibility into network performance. By monitoring network traffic and behaviour in real-time, DTs can help network operators identify and diagnose issues more quickly, allowing them to respond and resolve problems faster than they could with traditional methods.

Another advantage of DTs for network management is their ability to simulate and predict network behaviour. By building a predictive model of network behaviour, DTs can help network operators optimize network performance, identify potential issues before they occur, and even simulate the impact of network changes before they are implemented.

DTs can also be used to improve network security. By modelling network behaviour and identifying anomalies in real-time, DTs can help network operators detect and respond to cyber threats more quickly and effectively than traditional security measures.

Key challenges associated with DTs for computer networks include the complexity of network infrastructure and the need for large amounts of data to build an accurate predictive model. Additionally, DTs must be updated and maintained to reflect changes in the network infrastructure or configuration, which can be a time-consuming and resource- intensive process, either manual or automated.

As proposed in [80], there are five levels of DT, where each layer requires a greater degree of maturity and digital transformation, but also includes increased value. The five levels are:

- Descriptive Twin, which provides a live, editable version of design and construction data of the physical twin;
- Informative Twin, which provides additional operational modelling and sensory data;
- Predictive Twin, which leverages operational data for insights;
- Comprehensive Twin, which provides simulations for future “what-if” scenarios;
- Autonomous Twin, with the ability to learn and act on behalf of the users.

Recently, the usage of DTs was extended to mobile networks, and especially 5G and 6G networks. The main objective of such works is to enable the integration of AI/ML loops within the management process in order to increase autonomous behaviour and reaction to faults, as well as to improve and optimize the network performance.

At the moment, the topic is not yet completely mature in the scientific literature. However, some interesting and relevant works include:

- In [24], the authors describe at high level the usage of DT technology to integrate AI solutions within the network life cycle. The paper describes how DTs enable to learn, optimize and test the network during the design and development phase, how provide collective intelligence during operation, and how to support knowledge transfer during the expansion and extension of the infrastructure.
- In [25], the authors provide a holistic view on the usage of DTs in 6G, as they explore the applicability of the DT technology in the context of 6G communication systems by viewing it as a tool to make research, development, operation, and optimization of the next-generation communication systems highly efficient.
- [26], instead, focuses on the usage of DT technology in security scenarios. The paper presents the usage of a simplified DT (i.e. a cyber range) to augment cyber range environments with ML tools. The work focuses on how this scenario might work and the way in which it might be used to train new experts.

3.2.4. Physical-Layer in 6G Networks

The 6G mobile communication networks should satisfy strict requirements related to reliability, latency, and security. Simultaneously, they should also provide a significant improvement in coverage, data transfer rates, user experience, and network capacity. As a result, the key performance indicators (KPIs) that will be adopted are expected to be 10 to 100 times better than those employed in 5G.

Over the last years, various advanced physical layer techniques have emerged to support the diverse 6G landscape. The use of a mass number of transmit antennas has been investigated as a potential solution. This concept is also known as massive multiple input multiple output (m-MIMO) and can leverage mass user connectivity as well as the support of advanced services and applications via the generation of highly directional beams as well as user separation [27]. However, in an effort to reduce transmission complexity and leverage energy efficiency, which is another key aspect of 6G networks, in practical wireless orientations fewer active RF chains are utilized compared to the total number of active antennas. This concept is also known as hybrid beamforming [28].

In the same context, due to the scarcity of spectrum resources, another key challenging approach is the use of non-orthogonal resources for signal transmission and reception. This concept is also known as non-orthogonal multiple access (NOMA) [29]. To this end, mobile nodes with the highest signal quality are selected for spectrum sharing.

6G networks are expected to be deployed over much higher frequencies compared to 4G/5G networks, not only due to spectrum scarcity in lower bandwidth regions but also due to the need to support higher data rates. Hence, millimetre wave (mmWave) transmission is an active area of research over the last years. In combination with m-MIMO techniques, thousands of antenna arrays can be deployed per access point [30].

Finally, another recent architectural development in the context of 6G networks is the use of cell-free m-MIMO configurations. In this case, ultra dense deployments per service area are supported [31]. Hence, a mobile user can be served simultaneously by multiple access points, thus leveraging user diversity and signal reception according to channel conditions.

3.3. Artificial Intelligence

3.3.1. AI-enabled solutions for security enhancement in 6G and threat mitigation

AI plays a critical role in 6G, not only in the design and optimization of protocols and operations, but also in the design of early detection of threats and anomalies. AI benefits 6G security systems, but the alliance between 6G and AI is a double edge-sword as it can also become a target of attacks.

Unlike 5G networks, where security solutions across all devices and base stations are configured with universal settings for certain types of attacks, it is apparent that such an approach cannot be applied in 6G networks. Intrusion Detection Systems (IDS) have been extensively used; however, they have been shown to fail in detecting complex attacks. Cybersecurity attacks in 6G networks are dynamic, polymorphic and sophisticated, using previously unseen custom code, able to communicate with external command and control entities to update their functionality. To this end, a smart support system is required for predicting attacks, detecting threats and defining proactive actions, prior to implementing mitigation strategies. This will require the evaluation of the impact of the attack, the criticality and resilience of the infrastructure compromised and the cost of the proactive actions and effective mitigation.

An extensive review of security and privacy issues of 6G networks in the physical, connection, and service layers is presented in [32]. It identifies new threat vectors, different from 5G, such as threats in the physical layer, and security issues in distributed AI. In [33], the authors have proposed an optimisation framework to address the identified challenges in 6G networks. The proposed framework optimizes security scheme selection and configurations to balance the security-energy trade-off in various scenarios. In [34], the authors analyse various potential new threats caused by the introduction of new technologies related to the usage of open-source tools and frameworks for 6G network deployment and present possible mitigation strategies to address these threats.

AI started to be used by security solutions [35] to overcome their limitations in the detection of complex and zero-day attacks. Initially, signature-based and anomaly-based techniques were used for the detection of attacks however these classical approaches acks due to the automatic feature engineering, have a low detection rate, and are not efficient in detecting small variants of existing attacks. Consequently, ML techniques were adopted due to the increasing complexity of hacking incidents, zero-day attacks, and unknown malware. ML based security solutions have been successfully developed on the infrastructure level (intrusion and anomaly detection), software level (malware, virus and botnet detection) and privacy level (personal information).

5G networks use different ML techniques to achieve dynamic and robust security mechanisms [36]. As a drawback, application of ML increases the risks of security attacks and privacy leakages. More specifically, use of AI has become new security threats and increase the attack surface in future wireless technology. DT [40] To detect cyberattacks in future wireless technology different ML, and DL based intrusion detection methods will be used [41]. Moreover, distributed learning [37], Deep Reinforcement Learning (DRL) [38], and FL [39] models have proven their ability in the detection of complex and zero-day attacks in distributed environments.

Several surveys in the literature have analysed the usage of AI by security applications proving that they are suitable for 6G security enhancement. In the physical layer, AI can improve the performance of the detection engines using DRL [44] to enhance randomness in physical layer

phase-modulated key generation and to enhance physical layer authentication [45]. Channel estimation is a significant issue in 6G wireless communication and is vulnerable to adversarial attacks. These adversarial attacks are associated with the incorporated AI functionality in 6G wireless communication systems/networks. In [46], the authors have proposed a deep autoencoder (DAE) based 6G channel estimation for detecting and preventing adversarial attacks. The simulation result shows that the proposed solution effectively detects and mitigates the attacks, enhancing the security in 6G networks that are vulnerable to AI-related threats. Moreover, Deep Neural Network (DNN) can also be utilized in layer physical layer security (PLS) to assist in securing wireless systems to counter the spoofing attack and Reinforcement Learning (RL) can also be employed in authentication-related security issues against the eavesdropping attack [47]. Furthermore, in unmanned vehicle communications, generative adversarial networks (GANs) can provide a countermeasure for defending against jamming attacks.

At the network layer AI is considered to enhance security solutions performance in the prediction of network attacks [46], filtering malicious traffic and making intelligent recommendation for network changes. Finally, in the service layer, AI is a favoured technique in different aspects, such as access behaviour modelling [47], or in biometric authentication [48].

DL methods can provide considerable data security support to the 6G end-to-end system, which includes cross-layer optimization such as optimizing the channel coding, synchronization, and estimations [49]. Distributed solutions focus more on the edge and end-to-end solutions while securing the 6G networks. The edge DL solutions are not capable of handling all types of attacks. A meta-learning approach is proposed to handle the mentioned issue. It adaptively changes the ML model running on a device to improve the performance and accuracy of the model. In [50], authors have utilized the meta-learning algorithm to identify the Wi-Fi impersonation attack. In cyber physical systems (CPS), IDSs are developed by using Federated Deep Learning (FDL) algorithm [51]. The proposed models support the multiple industrial CPS while preserving the privacy of the system. Both meta-learning and FL are used to detect cyberattacks in the 6G networks, but these approaches are not mature enough to guarantee privacy of the physical device [52].

In [39], two staged FL-based approaches have been employed for the detection of anomalies in B5G networks. The first stage considered a small portion of threats using an ML classifier. In the second stage, a more complex model is employed for the detection of anomalies that were unable to detect in the first stage. In a recent work [54], a Collaborative Federated Learning (CFL) mechanism has been utilized in conjunction with DRL based approach for the detection of DDoS attacks. The CFL helps in updating the model parameters for the detection of attack closer to the device to enhance the recognition speed whereas the DRL-based mechanism aims to minimize the errors through the training, resulting in optimized decision-making based on the learning experience. For the DDoS attack detection scenario, Gated Recurrent Unit (GRU), a kind of recurrent neural network has been considered which employs the current/past information of traffic patterns in attack prediction. The evaluation results show the fast response time recognition and significant improvement in attack detection accuracy.

Integration of AI/ML can be used as a double sword. On one hand, AI can be used to improve security solutions, while on the other, the use of centralized data poses serious privacy issues. Additionally, AI and ML-based optimization techniques can enhance time-series and statistical methods, enabling systems to operate effectively in non-normal conditions and better defend against system-generating attacks. For instance, [55] explores the use of GANs to simulate intrusions and malware for improving its detection. While in [56] Transfer Learning (TL) is used to improve the detection of zero-day attacks.

Like the integration of AI/ML with the 6G networks, the integration of IT (Information Technology), OT (Operational Technology), and IIT (Industrial Internet of Things) has also experienced different types of threats. In [53], the authors have identified twenty-three different threats related to the integration of IT, OT, and IIT with the 6G networks. The study has also provided a review of different DL models including Restricted Boltzmann Machine (RBM), and Recurrent Neural Network (RNN) incorporated with long short-term memory (LSTM) for the detection of malware and ransomware attacks.

3.3.2. Intent-based Networking

IBN[57] is an advanced networking paradigm that automates network administration and operations. It converts high-level corporate goals or user intentions into policies that are dynamically distributed throughout the network architecture. IBN platforms leverage AI and ML to continuously monitor network circumstances, implement security policies, and automatically alter configurations to keep the desired state. IBN streamlines network administration by abstracting technical difficulties, allowing operators to focus on business goals rather than hardware configurations.

One of IBN's key features is the ability to verify that the network's current state is consistent with the planned policies and objectives. This verification is carried out by continuous monitoring and real-time feedback loops. The network employs telemetry data and analytics to detect differences between expected and actual conditions, allowing automated repair steps to be conducted as needed. Additionally, IBN can dynamically adjust to changes in traffic patterns or security issues, providing increased resilience and adaptability. This proactive strategy allows for faster response times and assures compliance with security and performance standards.

IBN can also operate with security architectures, such as Zero Trust models, to provide safe environments. Intent-based segmentation enables networks to dynamically assess and alter trust levels depending on user and device behaviour guaranteeing tight control over access. The use of intent-based management and Zero Trust principles improves overall security by constantly validating access and limiting lateral movement within the network. This makes IBN particularly helpful in remote, cloud, and IoT scenarios, where traditional perimeter-based security methods are ineffective.

3.3.3. Generative AI

GenAI, particularly through LLMs, is transforming industries by automating complex processes and enhancing decision-making capabilities. In cybersecurity, GenAI has the potential to revolutionize threat detection, vulnerability analysis, and mitigation by processing vast amounts of data and generating intelligent responses.

LLMs are increasingly applied in various cybersecurity domains, including vulnerability detection, malware analysis, phishing detection, and anomaly detection in network traffic [67]. LLMs have shown considerable promise in addressing cybersecurity challenges offering a promising approach to automating security mitigation strategies, especially when dealing with specific network attacks such as phishing, Distributed Denial of Service (DDoS), and malware propagation. The strength of LLMs lies in their ability to analyse large datasets and extract meaningful patterns. For instance, LLMs like GPT-3, GPT-4, and specialized models have shown great promise in vulnerability detection and secure code generation, enabling faster response times and more accurate threat management [71].

As LLMs advance, they have the potential to significantly impact both attack detection and the automation of defensive responses. These models can analyse large volumes of threat data to create tailored solutions for different types of attacks. This allows for the automatic identification of network threats and the generation of corresponding mitigation strategies, resulting in a dynamic and continuously evolving database that strengthens cybersecurity. Their ability to detect threats, propose countermeasures, and update attack-mitigation databases in real time has proven successful, particularly in providing alerts and recommendations for incidents like malware infections or unauthorized access [72].

Zhang et al. [68] further highlight the application of LLMs in various cybersecurity tasks, including secure code generation, vulnerability detection, and anomaly analysis, demonstrating their ability to reduce manual effort while improving accuracy and response times. Additionally, efforts like the CyberMetric dataset provide benchmarks for evaluating the general knowledge of LLMs in cybersecurity, showing their proficiency in answering complex questions and proposing mitigation strategies [69].

Moreover, by utilizing Retrieval-Augmented Generation (RAG), LLMs can continuously adapt to emerging threats and mitigation techniques, strengthening system resilience. RAG is a method that enhances the capabilities of LLMs by combining their ability to generate text with real-time retrieval of external information. Traditional LLMs, such as GPT models, rely solely on the data they were trained on, which can become outdated or limited in scope. RAG addresses this limitation by allowing the model to query external sources, such as databases, documents, or websites, while generating responses. This gives the model access to the most current and relevant information available, rather than just relying on static knowledge. In the context of cybersecurity, RAG significantly enhances the adaptability of LLMs. When faced with an emerging threat or a new type of attack, an LLM using RAG can retrieve the latest security data, such as vulnerability reports or mitigation strategies, from up-to-date external resources. This enables the model to generate solutions that are both relevant and timely, ensuring that the mitigation techniques it proposes are aligned with the current threat landscape. By continuously integrating fresh information into its responses, RAG-equipped LLMs can provide more accurate recommendations and improve the overall resilience of cybersecurity systems.

Despite their potential advantages, LLMs face several challenges, particularly related to security risks. Studies indicate that LLMs are susceptible to adversarial prompts and attacks, such as prompt injection, which can compromise the integrity of generated mitigations [70]. Thus, ongoing research is needed to ensure that LLM-generated responses are secure and robust, preventing malicious actors from exploiting these automated systems. Moreover, there is ongoing research on improving the interpretability and explainability of LLMs. Understanding how these models generate responses is crucial to ensure the trustworthiness of the mitigations they propose. Future efforts aim to make LLMs more transparent and robust, enabling their broader application in automating cybersecurity defences [71].

4. HORSE Use Cases

In this section, the HORSE pilots are illustrated in the form of use cases in the two domains selected by the project. Since the description of the use cases, the problem statement for each one and the pertinent usage scenarios have been elaborated in deliverable D2.1 [15] and have not significantly changed since then, in the current deliverable the section focuses more on the integration of the use case solutions with the HORSE platform, the usage scenarios and in particular the testing strategies.

4.1. HORSE Use Case 1 - Secure Smart LRT Systems (SS-LRT)

As described in D5.1 [75] and in previous HORSE documentation, the first use case (SS-LRT) is based on the operation of a Light Rail Transit (LRT) system and the consortium is using as reference environment, the solutions of real scenarios performed in Dublin/LUAS (Ireland) and Bergen (Norway) Metro's, by EFACEC.

Figure 2 illustrates the integration of a Metro Solution with the HORSE platform, showing the stations/tram stops and vehicles communication with the Operational Command Centre (OCC). This is the reference architecture of Use Case 1.

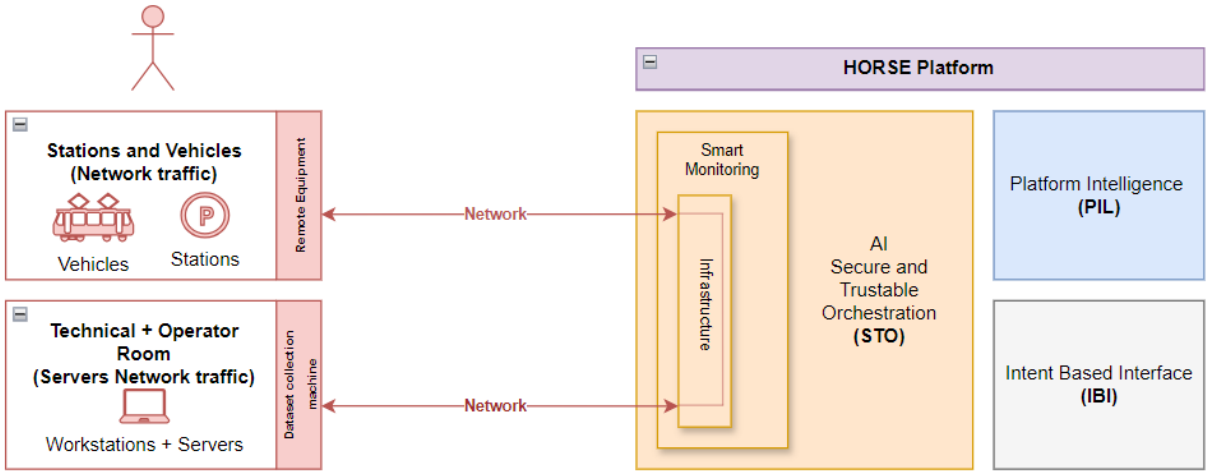

Figure 2: SS-LRT Use Case

4.1.1. Demonstration: Usage Scenarios

For the HORSE demonstration and validation purposes, a representative laboratory scenario was defined, involving the connectivity and integration of three testbeds: i) UMU, ii) UPC, and iii) EFACEC. At UMU testbed an emulation of the tram stops and vehicles will be deployed using VM capabilities and a video camera will be used to simulate the video streaming of a real tram stop. This scenario will use the 5G network supported by the UMU testbed and will be connected to the UPC testbed, where the HORSE platform will be deployed. The UPC will be connected to EFACEC laboratory (EFACEC Oracle Cloud) where a simulation of an OCC will be deployed. Therefore, this environment assures the interconnection of vehicles and tram stops with an OCC, using a 5G network and allows the integration of the HORSE platform for demonstration the HORSE benefits, in particular in the presence of cybersecurity threats.

Figure 3 illustrates the reference solution for the Use Case 1, showing the integration of the three laboratory environments.

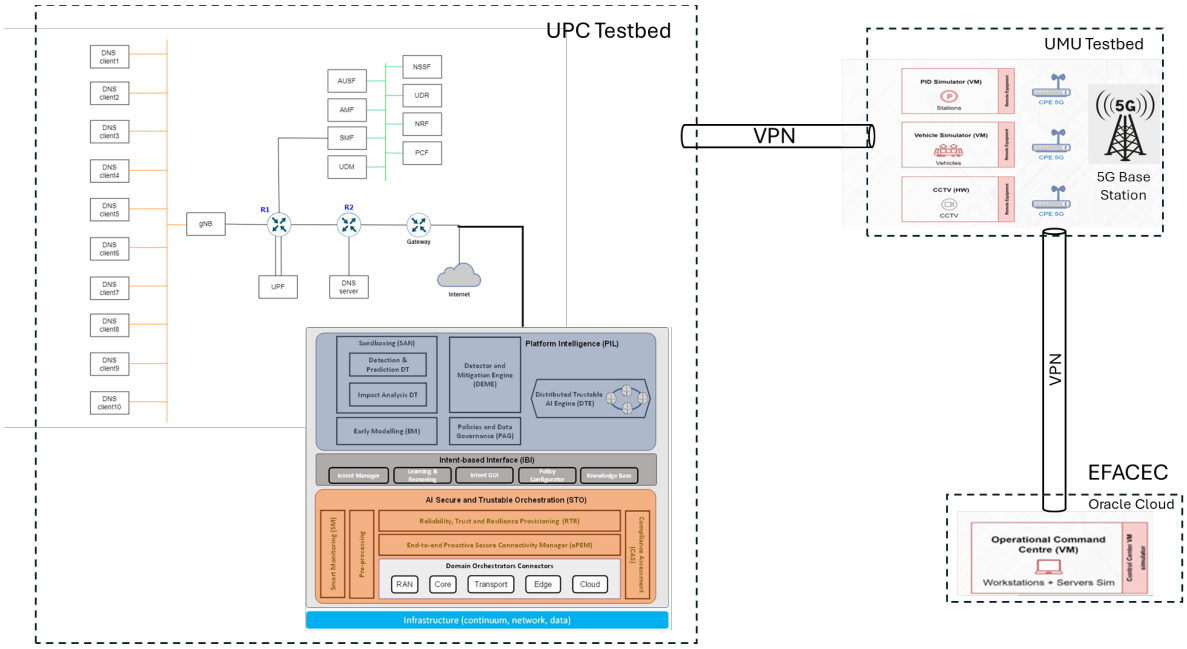

Figure 3: Use Case 1 - Solution

Several test procedures will use this architecture to validate the HORSE platform behaviour in the presence of cyber-attacks and Figure 4 represents some capabilities of the HORSE related to: i) attack detection, ii) processing, iii) performance (metrics) and mitigation (actions).

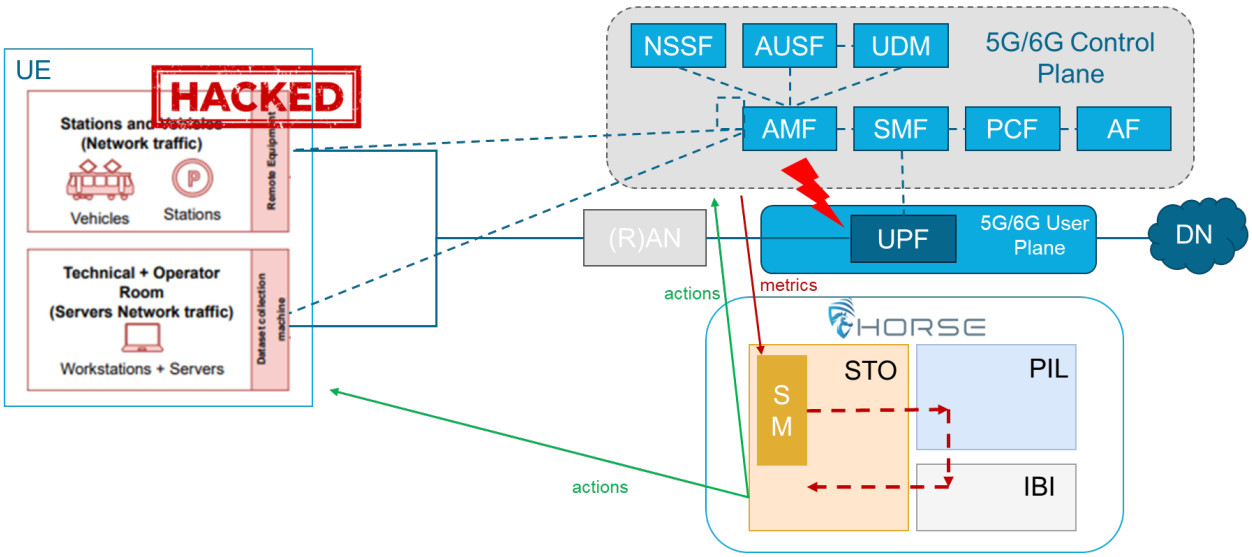

Figure 4: Use Case 1 - Attack representation

4.2. HORSE Use Case 2 - Remote Rendering to Power XR Industrial (R^2XRI)

The second use case of this HORSE project (Remote Rendering to Power XR Industrial) will focus on remote application rendering in the Extended Reality (XR) industrial sector. The use of XR technologies has become commonplace in many industrial verticals, who aim to leverage the various beneficial properties of XR to enhance workflow processes. Among such enhancements, some of the key benefits are immersive training measures, remote support, and product design. An ongoing challenge in industrial XR is in the accommodation of the continued growth of these technologies and their associated business demands with appropriate network infrastructure and connectives.

This use case will utilize the HORSE platform to assist in meeting these network needs. The XR application *Hololight SPACE (SPACE)* by partner HOLO provides end-users with the ability to engage in multi-user virtual fast-prototyping. Fast-prototyping involves the collaborative display and interaction with a computer-aided-design (CAD) file virtually. Incorporated into AR 3S is a remote rendering and application streaming functionality, imparted by the Remote Application Rendering SDK called Hololight STREAM (STREAM). Remote rendering and streaming provide high resolution and quality XR experiences by bypassing device processing limitations. This remote rendering ability is critically dependent on low latency, high throughput, and secure network connectivity. The various functionalities and attributes of the SPACE application will be enhanced in this use case by leveraging the HORSE platform, which will aid in validating the components of the platform itself.

As described in D2.1, this UC will mainly focus on 4 sub cases:

- Rendering of XR in a local network
- Fast-prototyping sessions in multi-player mode
- Multi-user experience
- Industrial Metaverse and XR devices

4.2.1. Demonstration: Usage Scenarios

A robust network infrastructure is foundational for supporting extended reality (XR) applications. As industries worldwide increasingly integrate XR solutions to enhance workflows —whether for immersive training, remote support, or advanced product design— the true potential of XR hinges on the capabilities and quality of the underlying network. HORSE is developing an advanced infrastructure that addresses the demands of next-generation XR applications. Figure 5 shows how HORSE is planning on providing this infrastructure to the XR solution.

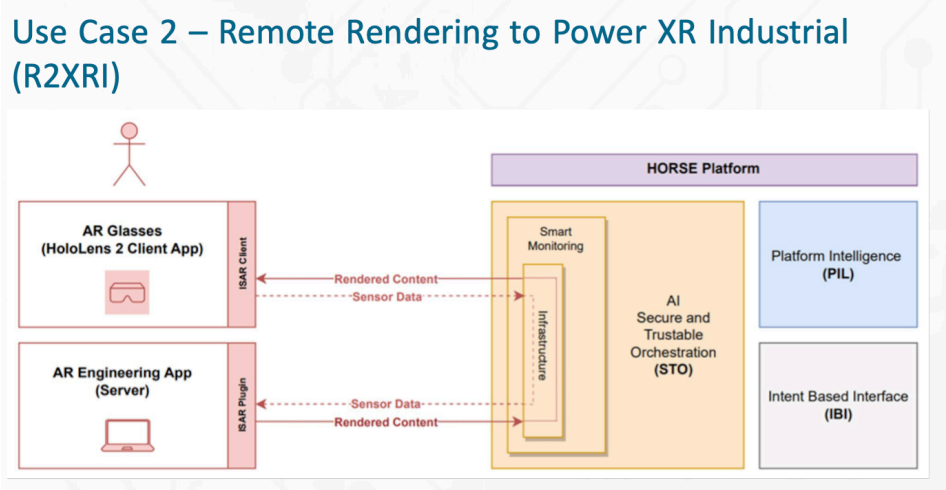

Figure 5: Use Case 2 - Architecture

4.2.1.1. The Necessity of Network Infrastructure for XR

The use of XR in industries is growing; from complex 3D model visualizations to collaborative DTs, the applications are boundless. To contextualize the demand, a study by PwC projects that by 2030, XR technology will contribute over $1.5 trillion to the global economy [79]. These are contingent on high-quality, high-performing networks. A lagging or insecure network can compromise both the functionality and experience of XR, undermining its utility in real-world industrial settings. Yet, the limitations of current networks are evident, with inadequate infrastructure often resulting in high latency, limited bandwidth, and security vulnerabilities [78].

4.2.1.2. How Network Quality Influences XR Performance and Experience

A strong network infrastructure supports the delivery of high-resolution graphics and smooth, uninterrupted interactions. The demand for this is especially pronounced in XR applications where 3D CAD files and DTs require high-resolution visuals, often involving millions of polygons. For industrial applications, clarity in design and accuracy are paramount for decision-making, risk assessment, and quality assurance.

Hololight's product, SPACE, exemplifies the need for high-quality network. As an advanced XR application for industries, it facilitates the visualization of 3D CAD data, enables multi-user collaboration, and supports complex tasks like prototyping and layout planning. It achieves this through the integration of Hololight STREAM which enables remote rendering of applications. The communication between remote server and the client installed on the smart glasses is carried out through a TCP/IP based WiFi connection. Without a network capable of supporting large data transfers with minimal latency, the performance of SPACE would degrade, resulting in poor image quality, delays in interactivity, and ultimately, a suboptimal experience.

Figure 6: Use Case 2 - Example of 3D model with and without Stream enabled

4.2.1.3. Security: Protecting Against Network Attacks

Network quality, however, is not solely defined by bandwidth or latency; security is equally critical. As networks expand and connect more devices, they become increasingly vulnerable to attacks. Cyber threats are diverse, with ransomware attacks and data-related accounting for the majority. Malware, DDoS attacks, and phishing are also prevalent. In industrial XR applications, where valuable data is transmitted and real-time operations depend on connectivity, these threats can disrupt workflows, compromise data, and impact user safety.

The DDoS threat involves overwhelming a network by flooding it with traffic from multiple sources, making it inaccessible. For XR applications, which rely on high data throughput, this could render the solution unusable. By cutting off access, attackers can prevent users from loading essential applications, participating in collaborative sessions, or visualizing critical 3D data. The impact is profound in scenarios like fast prototyping, where designers across locations work together, or in industrial metaverses where multiple users engage in collaborative tasks like factory layout planning.

4.2.1.4. Validating HORSE Through XR Test Cases

To ensure its infrastructure meets these stringent demands, HORSE employs a series of test cases using Hololight's SPACE and STREAM technologies, which allow the platform to assess network quality, reliability, and security in realistic conditions.

1. **Single-User, High-Load Test**: In this scenario, one user runs Hololight SPACE over a local network and loads a large 3D object. This test assesses the network's ability to handle heavy data loads without sacrificing quality. HORSE network infrastructure is validated by running this test on both AR and VR devices, as each device type imposes unique demands.
2. **Cross-Location Collaboration**: Another test involves users located at different sites connecting over the HORSE network to collaborate on a fast-prototyping session in SPACE. This tests the platform's capability to support high-quality, low-latency communication across distances—a key factor for industries where design teams are distributed.
3. **Multi-User, High-Bandwidth Usage**: This test simulates a high-demand scenario in which several users with both AR and VR headsets operate within the same network. This stresses the network's bandwidth, assessing how resolution and experience quality are impacted under load. HORSE's infrastructure can thus gauge the threshold for maintaining performance, which is crucial for scenarios involving multi-user industrial metaverses.

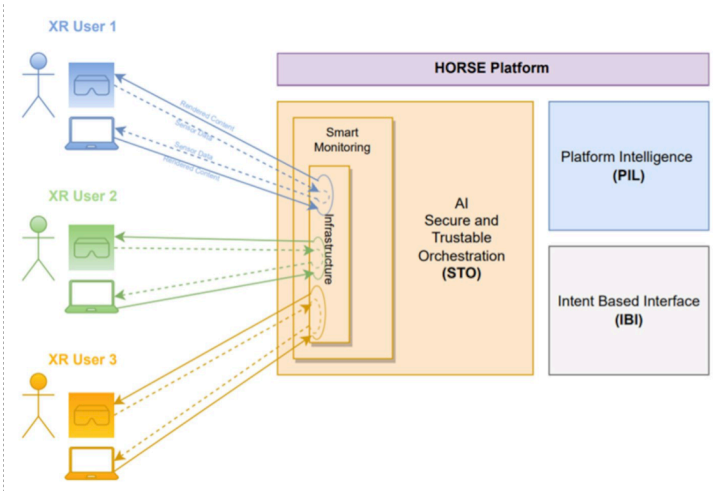

Figure 7: Use Case 2 - Multi-User as Network stress test

4. **Security Under Attack**: Given the high incidence of DoS/DDoS attacks in network environments, HORSE's test suite includes simulations of these types of attacks. The HORSE infrastructure's capabilities are tested here to ensure that network overloads are prevented, maintaining connectivity for essential XR applications. This resilience is especially vital for industries.

5. HORSE Functional & Non-Functional Requirements

This section provides the updated list of functional requirements for the various HORSE modules. Depending on their priority, these requirements shall be developed in the project's second iteration (IT-2). Table 1 below includes both the requirements proposed and already covered in the project's first iteration (IT-1) (addressing the HORSE use cases as described in the first version of HORSE Landscape: Technologies, state of the art, AI policies and requirements [15]), and new requirements introduced after the conclusion of IT-1.

In the table below, the "REQ ID" and the "Name" columns identify the requirement, while the "Description" column provides a more detailed explanation of the requirement. The keywords used in the "Priority" column are to be interpreted as described in RFC 2119 [59]. The "HORSE Module" column links the requirement to the module in the HORSE architecture responsible for implementing the requirement or the group of modules (e.g., PIL, STO). In order to track the project development, a column with the name "Status" was added to briefly report the development status of the requirement (covered, partially covered, or pending for IT-2).

Taking into consideration, the integration of the HORSE platform in the selected testbeds, at the end of this section, some considerations are elaborated, concerning the validation of the HORSE requirements. For a better understanding, a dedicated table is presented, identifying the relationship between the requirements and the Use Case to be demonstrated and validated.

Grant Agreement No.: 101096342
Call: HORIZON-JU-SNS-2022
Topic: HORIZON-JU-SNS-2022-STREAM-B-01-04
Type of action: HORIZON-JU-RIA

REQ ID	Name	Description	Priority	HORSE Module	Status
REQ-F-01	Multi-device connectivity monitoring	The HORSE platform must monitor the connectivity of devices connected to the managed network	MUST	Smart Monitoring	Covered
REQ-F-02	Multi-device protection	The HORSE platform must monitor the cybersecurity, including authentication, authorization, threat detection and secure connectivity, of the devices on extreme edge connected to the monitored network	MUST	Smart Monitoring, DEME	Pending for IT-2
REQ-F-03	Auditing of messages	The HORSE platform could offer auditing capabilities per subsystem	COULD	IBI, PIL, STO	Pending for IT-2
REQ-F-04	Auditing of device connections	The HORSE platform should produce auditing logs of devices connecting to the network managed by the platform	SHOULD	Smart Monitoring	Covered
REQ-F-05	Unauthorised device attempt detection	The HORSE platform must be able to detect when an unauthorized device attempts to connect to network and stop it from harming the HORSE platform	MUST	Smart Monitoring	Pending for IT-2
REQ-F-06	Detection of connection error on devices	The HORSE platform must detect connection errors of authorized devices trying to join the HORSE network / slice	MUST	Smart Monitoring	Pending for IT-2
REQ-F-07	Network Performance monitoring	The HORSE platform must ensure efficient monitoring mechanisms to timely identify network performance degradation regarding reliability, latency, and bandwidth	MUST	Smart Monitoring	Covered
REQ-F-08	Authentication support	The HORSE platform should be able to supervise different authentication and authorization mechanisms (Ie: OAuth2.0, DIDs, digital signatures)	SHOULD	All HORSE modules	Covered
REQ-F-09	Threat detection	The HORSE platform must be able to detect potential threats from external entities	MUST	DEME	Covered
REQ-F-10	Data integrity	The HORSE platform should be able to verify the integrity of information exchanged between different HORSE modules	SHOULD	All HORSE modules	Pending for IT-2
REQ-F-11	Notification	The HORSE platform must be able to notify the network operator about actions enforced on detected threats or foreseen threats	MUST	IBI, ePEM, RTR, DOC	Partially covered
REQ-F-12	Detection of attacks	The HORSE platform should detect attacks (such as DDoS attacks) on the network	SHOULD	DEME	Covered
REQ-F-13	Mitigation of attacks	The HORSE platform should propose network and system reconfigurations to mitigate attacks	SHOULD	IBI, DTE	Covered

REQ ID	Name	Description	Priority	HORSE Module	Status
REQ-F-14	Prediction of attacks	The HORSE platform must implement a methodology to predict an attack	MUST	DEME	Covered
REQ-F-15	Policy enforcement	The HORSE platforms should be able to enforce reconfiguration of the infrastructure in case of threat or attack detection	SHOULD	RTR, ePEM, DOC	Covered
REQ-F-16	Sandboxing of reconfiguration	The HORSE platform should be able to test and evaluate new configurations before deploying them to the infrastructure	SHOULD	IBI, IA-DT, EM	Covered
REQ-F-17	Persistence of information	The HORSE platform must save the intents entered by the user thought the Intent GUI in a persistent manner	MUST	IBI	Covered
REQ-F-18	Reporting of Intent-based decisions	The HORSE platform should report to the network administrator the decisions taken by the intent-based module	SHOULD	IBI	Covered
REQ-F-19	Anomaly detection	The HORSE platform must provide the appropriate mechanisms for anomaly detection in the transmitted messages	MUST	DEME	Covered
REQ-F-20	Attack modelling	The HORSE platform must be able to model attacks.	MUST	EM, PEM	Covered
REQ-F-21	Attacks impact modelling	The HORSE platform should model the impact of attacks in a SAN scenario.	SHOULD	EM	Pending for IT-2
~~REQ-F-22~~	~~Awareness of slices~~	~~The HORSE platform must be aware of slices in the networks (level of isolation, shared elements)~~	~~MUST~~	~~Slice Manager~~	Removed (justification included)
REQ-F-23	Access management	The user must be able to define and then the HORSE platform must enforce access policies in real time and ensure that access to the collected data assets in only granted to the authorised entities (users or components)	MUST	PAG	Partially covered
~~REQ-F-24~~	~~Secure interaction with the exposure functions of the network~~	~~The HORSE platform should be able to securely exchange data and commands from/to the network~~	~~SHOULD~~	~~RAN, CORE~~	Removed (justification included)

REQ ID	Name	Description	Priority	HORSE Module	Status
~~REQ-F-25~~	~~Granularity of the access~~	~~The HORSE platform could be able to support different roles in accessing the system~~	~~COULD~~	~~PAG~~	Removed (justification included)
REQ-F-26	Multi-tier orchestration	The HORSE platform should be able to manage services in a multi-tier environment, comprising cloud, edge and far edge	SHOULD	SM, RTR, ePEM, DOC	Covered
REQ-F-27	Notification of provisioning	The HORSE platform must notify the user about reconfiguration of the network to mitigate or avoid an attack	MUST	IBI, PEM, DOC, RTR	Partially covered
REQ-F-28	Real-time monitoring of attacks	The HORSE platform must continuously monitor the network for possible attacks and notify the user about them	MUST	PEM	Partially covered
REQ-F-29	Policies definition	The HORSE platform should provide a way to define policies and action to be performed in the network when certain conditions are met	SHOULD	IBI, RTR, PEM, DOC	Covered
~~REQ-F-30~~	~~Configuration of security level per slice~~	~~The HORSE platform must support configuration of security level in a per slice granularity~~	~~MUST~~	~~ePEM~~	Removed (justification included)
REQ-F-31	Use of anonymized data for AI training	The HORSE platform should use anonymized data to train AI model to detect threats and attacks	SHOULD	DTE	Covered
REQ-F-32	AI-based policies definition	The HORSE platform should be able to define set of optimum policies using AI/ML models to guarantee the system security against potential attacks	SHOULD	DTE	Partially covered
REQ-F-33	Reproducibility and repeatability of certain behaviours of digital twin in the network	The HORSE Digital Twin should be able to consistently repeat specific experiments, and to incorporate controlled variations to experiments execution as requested by its users.	SHOULD	SAN	Covered
REQ-F-34	Different granularity of control plane functions for Digital twin	The HORSE Digital Twin should be capable of deploying different network functions to test them independently or to model whole functionality sets or planes as a single entity, according to specific experiment.	SHOULD	SAN	Covered
REQ-F-35	Data anonymization	The HORSE platform must execute data anonymization operations on collected data assets	MUST	PAG	Partially covered

REQ ID	Name	Description	Priority	HORSE Module	Status
REQ-F-36	Data encryption	The HORSE platform must support end-to-end data encryption for data in transit	MUST	PAG	Pending for IT-2
REQ-F-37	Observability	The HORSE platform could allow the user to monitor the status (successful or failed execution) and view an incident summary of all AI pipelines	COULD	PAG, DTE	Pending for IT-2
REQ-F-38	Data retention	The user should be able to define and then the HORSE platform should execute data retention operations (e.g., automated deletion after a certain due date) on collected data assets	SHOULD	PAG	Partially covered
REQ-F-39	Data ingestion 1	The HORSE platform must allow the ingestion of data at rest (for example, from a file or from an API)	MUST	Smart Monitoring, Pre-Processing	Covered
REQ-F-40	Data ingestion 2	The HORSE platform must allow the ingestion of real-time data (for example, streaming data)	MUST	Smart Monitoring, Pre-Processing	Covered
REQ-F-41	Data pre-processing	The user must be able to define data pre-processing rules (for handling outliers, for handling missing data values, etc.) on the data assets and the HORSE platform must pre-process the collected data assets according to these rules	MUST	Smart Monitoring, Pre-Processing	Covered
REQ-F-42	Network and service status information	The PIL must be able to periodically gather information about the status of the network and running services	MUST	PIL	Pending for IT-2
REQ-F-43	Threat Detection Time	The Horse platform must be able to provide early attack detection within three ROPs (Note: The ROP period with which monitoring data are collected from the network is dimensioned according the network size. A typical value is in the order of some minutes)	MUST	DEME	Partially covered
REQ-F-44	Threat Detection Rate	The detection rate, i.e., the number of successfully detected attacks over the total, should be above 90%, considering the application of ML and the SoA benchmarks	SHOULD	DEME	Pending for IT-2
REQ-F-45	Monitoring the latency between network endpoints	The SM should be able to provide the IBI at any time the average latency between two network end-points	SHOULD	Smart Monitoring	Pending for IT-2

REQ ID	Name	Description	Priority	HORSE Module	Status
REQ-F-46	Monitoring the throughput between network endpoints	The SM should be able to provide the IBI at any time the average throughput between two network end-points	SHOULD	Smart Monitoring	Pending for IT-2
REQ-F-47	Monitoring of packet loss between two network endpoints	The SM should be able to provide the IBI how reliable is a network connection between two network endpoints in a scale from 0 to 1.	SHOULD	Smart Monitoring	Pending for IT-2
REQ-F-48	Visual information of intent's lifecycle	The IBI should be able to show the lifecycle of received intents and its execution	SHOULD	IBI	Pending for IT-2
REQ-F-49	Learning and reasoning about human input	When a decision is escalated to human operators, the IBI should be able to learn the decision taken from the operator to apply the same reasoning when same situation repeats	SHOULD	IBI	Pending for IT-2
REQ-F-50	Store attacks/mitigations	The HORSE platform must be capable of storing detailed records of known attacks and their corresponding mitigation strategies within the Knowledge Base	MUST	KB	Pending for IT-2
REQ-F-51	Access to Attacks-Mitigations information	The HORSE platform must enable its components to access the Knowledge Base (KB) to retrieve attacks and mitigations data via REST-API	MUST	KB	Pending for IT-2
REQ-F-52	Generation of mitigation strategies with GenAI	The HORSE platform should leverage advanced generative AI techniques to automatically generate new mitigation strategies for identified attacks, enhancing the content of the Knowledge Base	SHOULD	KB	Pending for IT-2
REQ-F-53	Prioritize mitigation actions	The HORSE platform should provide mechanisms for ranking, thus prioritizing mitigation actions based on their severity and impact.	SHOULD	KB	Pending for IT-2

REQ ID	Name	Description	Priority	HORSE Module	Status
REQ-F-54	Location awareness	The HORSE platform should have means to determine the location of UE in the network and share this information through a centralized API	SHOULD	LOCATION API	Pending for IT-2
REQ-F-55	Network status visualization	The HORSE platform could show the status of the network, including the status of the detected or predicted attacks or anomalies and the status of the mitigations and preventive actions.	COULD	Dashboard	Pending for IT-2
REQ-F-56	Decentralized ML training	The HORSE platform should support decentralized training of he involved ML models	SHOULD	DTE	Pending for IT-2
REQ-F-57	ML models repository	The HORSE platform should support dynamic update of various ML models stored in the corresponding repository	SHOULD	DTE	Covered
REQ-F-58	Intents	The HORSE platform should cater for different types of intent depending on short- and long-term goals (mitigation and prevention intents)	SHOULD	IBI, DTE	Covered
REQ-F-59	Monitoring of packet flows through networked interfaces	The SM must provide the SAN data flows in pcap format to enable the analysis and replica of flows between the Physical and the Digital Twin of the Network.	MUST	Smart Monitoring	Pending for IT-2
REQ-F-60	Policy Collection	The CAS must collect policies from the policy configurator using REST APIs	MUST	CAS	Pending for IT-2
REQ-F-61	Compliance Verification	The CAS must assess collected policies against compliance criteria defined by 3GPP and ENISA standards	MUST	CAS	Pending for IT-2

REQ ID	Name	Description	Priority	HORSE Module	Status
REQ-F-62	Flagging Non-Compliant Policies	The CAS must flag policies that do not meet compliance standards for review	MUST	CAS	Pending for IT-2
REQ-F-63	Reporting	The CAS should generate detailed compliance reports	SHOULD	CAS	Pending for IT-2

Table 1: List of HORSE functional requirements

It is worth mentioning that some requirements were removed and should no longer be considered in IT-2 of the project while other requirements were updated. This change reflects the HORSE Project partners' consensus and addresses the reviewers' comments after the conclusion of the first phase of the project. This especially applies to requirements regarding the use and awareness of slices in the network under consideration, as well as the central user management for the HORSE platform. Although these requirements were initially considered, REQ-F-24 and REQ-F-25 as optional, REQ-F-22 and REQ-F-30 as mandatory in the first round of requirements elicitation, the consortium is proposing their removal for IT-2. The reasons advocating in favour of this proposal are mainly the use and exploitation of Network Slicing in current 5G networks and beyond versus the current phase of the project and the available systems [60].

Currently, it is possible to find in the specialized literature multiple works related to a centralized view of network slicing creation (at least for 5G networks) that tackle security topics such as network isolation and deployment of slices, most of them related to the network and application (cloud) layer. However, most of the studies and implementations lack extensions for RAN. In the meantime, 3GPP focus on slicing is steered towards slicing security and verticals support [61], [62], [63], which at the moment are in Rel.18 as study items.

Regarding the impact of removing these requirements from the elicited requirements of HORSE, we believe that the project outcomes are not hindered or diminished. If not else, it also helps focus more on further developing our solutions based on our design. In addition, REQ-F-21 has been revised to also address the impact of attacks on the targeted 6G components. This assessment, along with the mitigation impact, will provide a comprehensive view of the cyberattacks within the threat model. Following, we justify the update or removal of each requirement from the HORSE Project.

REQ-F-21

The description of this requirement was updated to reflect the objectives of IT-2 and align with the achievement of the project objectives. The impact of attacks on the different 6G components within a SAN scenario could be modelled. This modelling will provide helpful information on how 6G components can be affected by potential threats. The EM component is responsible for providing all the information required by the SAN to perform successfully. Consequently, it will integrate this information into the established threat model. As a result of these considerations, REQ F-21 has been updated accordingly.

REQ-F-22

The solutions developed in the project can infer the slice awareness indirectly assuming that through smart monitoring slice relevance could be detected. However, the peering of HORSE framework with 5G specific to network slicing functions or orchestrators will not be approached. In the current consortium the offered solutions and testbeds available for the project, the slicing mechanisms are mostly related to cloud and the network resources rather than the RAN. As such the consortium prefers to steer the efforts towards the implementation of other more impactful function requirements.

REQ-F-24

HORSE modules are constantly interacting with the network elements. Such communication should always adopt up-to-date security solutions, otherwise risking compromising the control of the entire network. However, different mechanisms are already in place to provide security solutions for network exposure data and control, such as the security mechanisms adopted by the 3GPP NEF [76] and OpenCAPIF [77] framework. Although HORSE is concerned about keeping the network safe, HORSE modules are complementary to the mentioned ones, not replacing but communicating with NEF and other functions. Therefore, the adoption of security mechanisms at the RAN and CORE interaction level is more related to the engineering and implementation of the communication between modules. The removal of REQ-F-24, thus, does

not mean that HORSE modules will ignore any security mechanism for securely communicating with the network. However, it will allow the partners to focus on developing and researching the primary function provided by each HORSE module, tackling the communication with other modules as a supporting task.

REQ-F-25

The magnitude of different components trying to bring together in this project, distances from the concept of a coherent platform with rigid central user management. In addition, the IBI module has been assigned other roles and functionality and cannot be considered as a central Dashboard for the whole project, acting as an entry point for each and every component. The idea of supporting different roles (e.g., user, administrator, manager etc.) centrally has been dropped in favour of per-component user management.

REQ-F-30

For the project objectives it is enough to demonstrate security solutions that can work for either one slice or for the total of the slices used (i.e. the whole 5G network). In this view, the removal of this requirement will not affect at all the efforts and the approach of the project wrt 6G security.

The next table includes the list of non-functional requirements. Each non-functional requirement is identified by its requirement id (REQ ID) and name. The column "Description" is used to detail the non-functional requirement, while the "Priority" column is to be interpreted as described in RFC 2119 [59].

REQ ID	Name	Description	Priority
REQ-NF-01	Geographic dispersion support	The HORSE platform must consider the geographic dispersion of elements and devices connecting to the network.	MUST
REQ-NF-02	Scalability	The HORSE platform should support expansion and scalability of the systems.	SHOULD
REQ-NF-03	Centralized data collection	The HORSE platform should collect data about the network performance using a centralized endpoint	SHOULD
REQ-NF-04	User friendliness	The HORSE platform should offer intuitive user-friendly interfaces	SHOULD
REQ-NF-05	Consistent interfaces	The HORSE platform should offer consistent interfaces among its different modules	SHOULD
REQ-NF-06	Decentralized management	The HORSE platform should support decentralized management of system modules (not all modules hosted in the same datacentre)	SHOULD
REQ-NF-07	Installability of the platform	The HORSE platform should be installable in servers running at the cloud or at servers running at the edge or the network (e.g., on premises servers)	SHOULD
REQ-NF-08	Platform support	The HORSE platform components must support installation on the Linux platform	MUST
REQ-NF-09	Web access	The components of the HORSE platform should be accessible via web technologies	SHOULD
REQ-NF-10	Support of lightweight virtualization	The HORSE platform should be based on containerized software blocks in order to support service mobility in a timely manner	SHOULD
REQ-NF-11	Compliance to legal legislation	The HORSE platform must comply with the legal framework with respect to information dissemination	MUST
REQ-NF-12	Service mobility	The HORSE Platform must support device and service mobility.	SHOULD
REQ-NF-13		The IA methods employed by the HORSE platform must adhere to ethical principles and values	MUST

REQ ID	Name	Description	Priority
REQ-NF-14	Context awareness	The HORSE platform must have access to status information about network traffic, network status and services	MUST

Table 2: List of HORSE non-functional requirements

5.1. Mapping HORSE requirements to Use Cases for validation

Taking advantage of the testbeds, the HORSE modules, and the use case deployments, the IT-2 verification and validation will be performed continuously. The details regarding performance, KPI measurements, and technical validation will be considered. Additionally, these environments will allow the validation of the requirements. Table 3 identifies the main HORSE requirements to be validated using the final integrated HORSE version and the corresponding use cases.

REQ ID	Name	Use Case Validation
REQ-F-05 - OK	Unauthorised device attempt detection	UC1, UC2
REQ-F-06	Detection of connection error on devices	UC1, UC2
REQ-F-07	Network Performance monitoring	UC1, UC2
REQ-F-09	Threat detection	UC1
REQ-F-11	Notification	UC1
REQ-F-12	Detection of attacks	UC1, UC2
REQ-F-13	Mitigation of attacks	UC1, UC2
REQ-F-14	Prediction of attacks	UC1, UC2
REQ-F-15	Policy enforcement	UC1, UC2
REQ-F-17	Persistence of information	UC1
REQ-F-27	Notification of provisioning	UC1
REQ-F-28	Real-time monitoring of attacks	UC1
REQ-F-45	Monitoring the latency between network endpoints	UC1
REQ-F-46	Monitoring the throughput between network endpoints	UC1

REQ ID	Name	Use Case Validation
REQ-NF-14	Context awareness	UC1

Table 3: Mapping HORSE requirements to Use Cases for validation

6. HORSE Network Services and Threats

This section updates the description of the 6G network services and threats that the HORSE project will consider. The 6G network services requirements will be defined in the API exposure, AI- and ML-enabled operation, AI data training and heterogeneity research areas, while the HORSE 6G network threats will include DoS, data tampering and network congestion.

6.1. 6G Services considered in HORSE

In the HORSE project, 6G network services will cover at least the following four areas: (i) API exposure, (ii) AI- and ML-enabled operation, (iii) AI data training, and (iv) heterogeneity.

6.1.1. API exposure

APIs exposure at the edge is ever gaining importance in 5G networks motivated by the need to enrich existing services with improved security and performance, as well as to enable the development of new ones. Indeed, highly demanding networked services (e.g., those requiring low latency or supported by massive IoT deployments) may benefit from 5G network capabilities, including for example high performance, efficient data management (collection, processing, ingestion), or proper device location, to offer high levels of quality of service, even for extremely demanding services.

The 5GPP architecture working group in the "The 6G Architecture Landscape European perspective" white paper [64], pointed out API exposure as a key research area, being a fundamental component in the global architecture to support and facilitate applications to interact with the network.

6.1.2. AI- and ML-enabled operation

AI and ML represent one of the key technologies to enable to exploit the softwarisation process started from 5G, that will be at the center of the 6G network architecture. Concepts such as O-RAN, network automation, DTs require to different degrees the introduction of ML or AI solutions.

As we edge closer to the era of 6G, the integration of ML and AI in mobile networks is poised to revolutionize the way we connect and communicate. Unlike its predecessors, 6G is expected to be not just an evolution, but a transformation, leveraging AI and ML to achieve unprecedented levels of efficiency, adaptability, and intelligence.

- Dynamic Resource Management: AI and ML algorithms enable real-time analysis and prediction of network conditions, allowing for dynamic allocation of resources. This ensures optimal performance even in highly congested areas or during peak usage times, effectively minimizing latency and maximizing throughput.
- Enhanced Security: In the 6G landscape, security threats will be more sophisticated. AI-driven security solutions can detect and mitigate potential threats by analyzing patterns and predicting malicious activities, ensuring a secure and resilient network.

- Network Optimization: AI and ML can be used to optimize network parameters autonomously, adjusting to varying conditions without human intervention. This includes tasks like optimizing signal strength, reducing energy consumption, and improving coverage in remote areas.
- Personalized User Experience: By leveraging user data, AI can create personalized experiences for users. This could range from tailoring network services to individual needs to providing highly personalized content delivery, enhancing user satisfaction and engagement.
- Support for Emerging Technologies: 6G networks will support a myriad of emerging technologies such as AR, VR, and IoT. AI and ML will play a crucial role in managing the data traffic and ensuring seamless interaction between these technologies and the network.
- Intelligent Automation: AI-driven automation will simplify network management and maintenance. From predictive maintenance that prevents failures before they occur to automated troubleshooting and repair, these technologies will significantly reduce operational costs and improve network reliability.

6.1.3. AI data training

The ever-growing need for data to be used to generate and train AI models is nowadays a key driver in research 5G/6G is not blind to. Many of the well described challenges 6G must face in the coming years may be addressed by developing AI-assisted solutions. When dealing with security provisioning AI data training will undoubtedly play a key role in defining predictive models that may notably contribute to design proactive and more automated security strategies. However, although many aspects related to how data is collected, ingested, stored and preserved yet remain as challenges, it is with no doubt that the development of customized AI training models for 5G/6G network scenarios would contribute to the design of novel services, where security will become a key pillar fostering the creation of novel services or even business models.

6.1.4. Heterogeneity

Unlike the relatively uniform architecture of previous generations, 6G networks will consist of a diverse array of infrastructure components, each playing a unique role in ensuring seamless connectivity and optimal performance.

- Diverse Access Technologies: 6G will integrate multiple access technologies, including millimeter-wave, terahertz communication, and even satellite communication. This diversity allows for more flexible and resilient connectivity, catering to different use cases and geographical conditions.
- Multi-Tier Network Architecture: 6G networks will adopt a multi-tier architecture, comprising macrocells, microcells, picocells, and femtocells. This heterogeneous structure ensures comprehensive coverage, enhanced capacity, and improved user experiences, especially in dense urban environments and remote areas.
- Integration of Edge and Cloud Computing: To handle the massive data traffic and low-latency requirements of 6G applications, the network infrastructure will seamlessly integrate edge and cloud computing resources. Edge nodes will process data closer to the user, reducing latency, while cloud servers will provide vast computational power for more complex tasks.

- IoT and Smart Infrastructure: The proliferation of IoT devices will be a significant aspect of 6G networks. These networks will need to accommodate a wide variety of connected devices, from low-power sensors to high-bandwidth AR/VR systems. This heterogeneity in devices necessitates a flexible and adaptive infrastructure.
- SDN and NFV: 6G will extensively utilize SDN and NFV to create a more dynamic and programmable network. These technologies enable the network to adapt in real-time to changing conditions and demands, allowing for efficient management of diverse infrastructure components.
- Energy Efficiency and Sustainable Design: With the integration of various technologies and components, 6G networks will emphasize EE and sustainability. This includes the deployment of green base stations, renewable energy sources, and intelligent energy management systems to minimize the environmental impact of the network.

6.2. 6G threats considered in HORSE

HORSE identifies possible threats for the two use cases included in the project in order to set a clear specification of requirements, a complete set of functionalities as well as the required needs for preliminary testing and validating the outcome of the project. It must be noted here that HORSE will address different threats related to 6G, that include both commonly known attacks (such as DoS, DDoS, or similar) as well as novel attacks potentially emerging from the implementation of the 6G services described in the previous section.

6.2.1. Secure Smart LRT Systems Use Case

The threats HORSE considers to be addressed in the Secure Smart LRT Systems Use Case, are Denial of Service (DoS) and data tampering. The rationale behind this assessment is motivated by the previous work done by ENISA in the last Threat Landscape Report [58] for the transport sector, identifying these two treats as two of the main threats targeting the railway sector. Indeed, most of the last year's attacks in the railway sector targeted their IT systems causing disruptions in passenger services, display boards, surveillance systems, etc.

6.2.2. Remote Rendering to Power XR Industrial Use Case ($R^2$2XRI)

The Remote Rendering to Power XR Industrial Use Case ($R^2$2XRI) aims to leverage the resilience and security functionalities to be provided by the HORSE project. These functionalities will ensure an unhindered data exchange flow during XR experiences which allows maintained operational efficiency in the industrial setting. To assess the efficacy of the envisioned security functionalities, a dedicated network threat will be simulated during the execution of this use case. Usage of the XR technologies here consists of a XR application hosted on a server which sends application streams to XR devices (e.g., HoloLens 2 AR glasses) and in return receives back sensor data. The reciprocal data exchange between XR device and XR application requires quality connectivity to ensure timely packet flow and permissive levels of transmission to avoid congestion. The latter of can be highly detrimental for end-users, as visualization and interaction with XR content is significantly impacted if network connectivity is highly congested and can even cease altogether. The simulated network threat in this use case will saturate the XR network connectivity to drive a low bit rate for data exchange. This threat scenario will be used to assess the extent to which HORSE can respond and effectively resolve such an attack within the context of XR experiences.

7. HORSE AI Data Management

7.1. Elasticsearch Database of the Smart Monitoring component

The Smart Monitoring component leverages the Elasticsearch database to provide robust real-time data analysis, storage, and retrieval capabilities essential for comprehensive monitoring. Elasticsearch, known for its distributed nature and powerful full-text search capabilities, underpins the data-driven operations of this component by enabling seamless ingestion, indexing, and querying of vast amounts of log and monitoring data.

Advantages of Using Elasticsearch in Smart Monitoring:

- Scalability and Performance:

Elasticsearch's distributed architecture allows the Smart Monitoring component to handle large volumes of data efficiently. The architecture ensures high availability and quick access to information even under heavy load conditions. Its ability to scale horizontally by adding more nodes helps maintain optimal performance as data volumes grow. This scalability ensures that even as the monitored environment expands, Elasticsearch remains reliable and responsive.

- Real-Time Data Analysis:

The component uses Elasticsearch to ingest and analyse data in near real-time. This is critical for identifying patterns, detecting anomalies, and generating alerts based on predefined rules, which supports proactive incident management and system health checks. Elasticsearch's efficient data processing pipeline ensures minimal latency, making real-time analysis seamless, which is essential for immediate response and mitigation of potential issues.

- Advanced Querying and Filtering:

Elasticsearch provides a robust querying language that enables complex search and aggregation operations. The Smart Monitoring component benefits from this to perform detailed data analysis, allowing users to filter data across multiple dimensions and gain insights through customizable dashboards. The use of both structured and unstructured data querying supports diverse analytical needs, from simple searches to complex, multi-parameter data examinations.

- Indexing and Data Storage:

All data ingested by the Smart Monitoring component is indexed in Elasticsearch, ensuring that data is stored efficiently and can be retrieved rapidly. The structure and mapping of the indices are designed to support optimal query performance and data retrieval. Elasticsearch’s index lifecycle management (ILM) policies are utilized to manage data retention and ensure efficient storage practices, balancing long-term data retention needs with storage capacity.

- Support for PCAP Analysis:

For real-time network monitoring, the component utilizes Elasticsearch to store metadata derived from PCAP (packet capture) files. This enables deep packet inspection results to be indexed and analysed, providing visibility into network traffic patterns and potential threats. The indexed data supports correlations between network events, aiding in root cause analysis and security incident investigations. This capability ensures detailed and actionable network intelligence.

- Data Enrichment and Processing:

Elasticsearch works seamlessly with components like Logstash and Beats for data enrichment and pre-processing before indexing. This integration allows Smart Monitoring to parse, transform, and enrich raw data to provide more contextually relevant insights. The processed data can include additional fields, tags, or metadata that enhance searchability and analysis. This enrichment process adds significant value by ensuring that data is more informative and actionable.

7.2. Data Management Procedures

The provision of harmonized, interoperable, and consistent datasets is critical to enable data providers to better understand their data and perform analytics tasks by combining datasets from different sources in an easier manner. Data Management procedures provide:

- **Mapping of the ingested data to a respective HORSE data model:** Pre-Processing aligns the ingested data to a common HORSE data model to enhance their interoperability. Part of the mapping process is performed in a semi-automated way, where the data provider can set subscriptions to act as data streams. These subscriptions specify the data source, the destination of these data, a time interval on how often to read from the data source as well as rules on how to read from the said data source. Data exchange will take place automatically through the subscription. Since the raw data are stored within the Elasticsearch database, the subscription retrieves this data by issuing queries to the database. These queries effectively represent the subscription rules, which define the specific characteristics each query seeks. For instance, if the subscription monitors network traffic to detect potential attacks on the Network Time Protocol (NTP) service, the queries will search for packet indices that exhibit NTP-related features. After each query is executed, the retrieved data are then forwarded via restful API to the desired data destination.

  As a second step, the data provider is allowed to review the subscriptions through a user-friendly interface and decide whether these subscriptions will be maintained, modified or deleted. The data provider can modify a subscription by updating the data source, the time interval and the query rules. In case this subscription is no longer needed, it can simply be discarded.

- **Data pre-processing:** Data Management ensures the data quality of the available assets, which is of crucial role for ML models since it impacts the accuracy and generalizability of the model. Errors in data can be due to various factors. They can be the results of imperfections in the data acquisition system or deliberate attacks aiming to poison the data. Both types of errors can harm the performance of the current model and specific measures should be taken in each case due to the structural differences between them. For minimising imperfections in the data acquisition system, possible techniques include:

  - Data profiling and statistical checks: Analyse statistical properties and data distribution to locate distribution drifts related to erroneous samples.
  - Outlier detection: Utilize outlier detection algorithms to identify anomalies errors in the data.
  - Domain specific rules (including human expert knowledge): Ingest prior knowledge in the form of filters to exclude datapoints not complying to this knowledge.

Another possible type of harmful data is input generated by adversarial attacks. Data management should exclude such data, before ML training, in order to create robust and secure AI models. In adversarial attacks, the attacker forces the model to produce incorrect outputs by slightly perturbating the input in such a way (often unnoticeable by humans) that elicits misclassification of the model. Another form of adversarial attack is data poisoning, where the attacker manipulates the input data used in ML training in order to decrease the performance of the model, shift the classification outcome of a specific sample to the wrong class, increase training time, etc. [65]

Data management uses the following mitigation methods to tackle these threats [66]:

- Adversarial training: synthetic/adversarial samples are created from the original dataset to be used also in training. Therefore, using augmented data, the model's resilience is increased.
- Input validation and filtering: validation checks are performed on the input to identify unexpected patterns and abnormalities. Flagged adversarial examples are then discarded based on specific criteria and thresholds.
- Pre-processing techniques: a simple process the involves normalizing the inputs prior to feeding the ML model like normalization, dimensionality reduction or feature scaling.

The aforementioned requirements are crucial for ensuring a robust and error-free data exchange mechanism. The primary feature of the Pre-Processing stage that addresses these requirements is the implementation of query rules. To mitigate the risk of data tampering through adversarial attacks, queries can filter traffic based on a diverse array of packet features. These features may include source and destination IP addresses, which can help prevent the ingestion of traffic from unknown or potentially spoofed IP addresses. Packet size is yet another valuable metric that can be extracted from the packets to determine if they are of a suspicious nature. Essentially, the queries can extract and apply filtering to any monitored packet feature.

Having established that Pre-Processing can extract all requisite features from the raw data, it is imperative to emphasize its modularity. This modularity facilitates the implementation of additional data verification procedures to minimize imperfections through the application of the aforementioned techniques. The consortium should reach a consensus on specific data profiles or outlier detection algorithms and measures to ensure data quality. It is important that the selected solution dies not hinders Pre-Processing's data gathering operations. These algorithms can be applied as a final filtering stage before transmitting the data to its intended destination.

- **Generation of data handling status messages:** Data Management is designed with observability in mind. This allows for constant and efficient monitoring of the data pipelines' execution. By doing so, we can timely detect potential problems. This is achieved by identifying any deviations from their corresponding configuration. The system also communicates the status of its data management processes. Additionally, any errors encountered are reported through various feedback messages. For example, it can indicate the number of "rows" in the data that were dropped due to inconsistent data types.
- **Data retention and disposal:** Data Management allows the data provider to assess whether collected data is needed and decide whether it should be deleted or further retained. In order to do so in a compliant manner, the data provider should examine the different policies to which the usage of the data and the access to it adhere to. In conjunction with the aforementioned, the actions required by the legislation should be taken into account (e.g., GDPR clauses, or legislation regarding data retention for

auditing purposes), and the most optimal methods for the retention or erasure of these datasets should be suggested.

- **Storage of data:** Once the data are appropriately ingested and handled, the processed data along with the processed sample are forwarded to the storage component.
- **Storage of assets' metadata:** Along with the processed data assets, the accompanying metadata are also forwarded to the storage component, creating the appropriate links between the stored data and their metadata information.

7.3. 5G/6G Network Traffic Data

The Pre-Processing module, in addition to serving as HORSE's network data distributor for the AI modules, will also store this information in structured datasets, which may be used for future AI model training.

Given the large volume of data in network traffic, much of which may not be of immediate interest except for specific segments, the Pre-Processing module is ideally suited for generating HORSE's datasets. With its ability to search for specific metrics within traffic packets (e.g., the number of NTP packets), it can efficiently store relevant values for later use.

After the Pre-Processing module has extracted and forwarded the values to HORSE's AI modules, it will create comprehensive data structures and store them in the Smart Monitoring Elasticsearch database. It is understood that a dedicated index will be allocated for these datasets. By "comprehensive data structures," we refer to commonly used formats for time series data, such as CSV or JSON files; however, the final choice of format will also depend on the ease of storage within the Elasticsearch database.

For better understanding we present a piece of the extracted number of NTP and DNS packets forwarded to the DEME. This was produced as part of the demo for the mid-term review. In the table below we see the number of NTP and DNS packets during an NTP attack, we can see that by the surge of NTP packets. The traffic snapshots are taken every two minutes.

	NTP	DNS
Snapshot 1:	34	34
Snapshot 2:	34	33
Snapshot 3:	33	33
Snapshot 4:	35	33
Snapshot 5:	38	35
Snapshot 6:	47	33

Snapshot 7:	62	33
Snapshot 8:	75	35
Snapshot 9:	80	34
Snapshot 10:	77	33
Snapshot 11:	61	35
Snapshot 12:	49	34
Snapshot 13:	39	33
Snapshot 14:	35	34

7.4. Human Interaction

Intent-based networks originated from the desire for network automation whose end-goal would be networks that would need zero intervention from humans, instead the specific desires of the so-called humans could be implemented in the network as intents [73]. However, another school of thought [74] believes that knowledge learned by machines cannot win human domain knowledge at all times for a bundle of reasons, and for that cause a human being placed in the loop is essential, hence the concept Human-in-the-loop (HITL).

HITL is a paradigm in science that refers to the involvement of human intervention in automated or machine processes. It doesn't include the human activities done during or by initiating the so-called processes, but only the tasks performed by humans while the processes run which interfere with or determine the course of the processes. HITL concept is an extensive area of research that covers the intersection of computer science, cognitive science, and psychology [74].

There are several methods and tools used to implement the concept of HITL in automated systems. HITL can be implemented with the use of user interfaces, APIs, communication tools, etc. In the HORSE IBI module, the HITL functionality will be implemented through a graphical user interface which also doubles as the IBI dashboard. An alert is sent by the IBI to the dashboard whenever there is a decision that requires human intervention, the network administrator decides by selecting the appropriate decision on the dashboard to be implemented by the IBI. The decision for which human intervention is needed is determining the suitable policies to mitigate or prevent particular threats. Two components – Policy

Configurator and Learning and Reasoning Component already do this, but every now and then contribution from human domain knowledge is necessary to avoid over-reliance on machines and allow for improvement in the decision process or update of policies based on knowledge advancement. The network administrator still reserves the right to ignore the alert and allow the machine to take the decision after a given timeframe has elapsed.

8. Conclusions

In this deliverable, we have presented an updated overview of the HORSE landscape, which focuses on the development of Holistic, Omnipresent, Resilient Services for future 6G Wireless and Computing Ecosystems. Building on the project's first iteration (IT-1) we have updated the HORSE context.

The description of the HORSE vision and background technologies has been updated, in order to convey our ideas for the project mission and its underlying technologies in a clean and concise way.

Within the realm of security, we have examined the implications of the 6G world and discussed risks and threats that need to be addressed. Furthermore, we have emphasized the importance of threat identification, characterization, and modelling to enhance security measures in the 6G ecosystem.

Networking capabilities are a crucial aspect of the HORSE project, and we have delved into several key areas within this domain. Our analysis has explored network exposure capabilities beyond 5G, focusing on EE and the design of DTs. Additionally, we have highlighted the significance of the physical layer in 6G networks to ensure robust and reliable connectivity.

Artificial Intelligence (AI) plays a pivotal role in shaping the future of wireless and computing ecosystems. Therefore, we have investigated AI-enabled solutions for enhancing security in 6G and mitigating threats. Moreover, IBN has emerged as a promising approach to optimize network operations and improve overall efficiency. In the same manner, we considered the advancements in GenAI and the solutions it could bring to the HORSE platform.

To demonstrate the practical implications, the HORSE project is implementing two use cases: Secure Smart LRT Systems (SS-LRT), showcases the application of HORSE infrastructure in ensuring the security and smooth operation of smart public transportation systems; Remote Rendering to Power XR Industrial (R^2XRI) focuses on extended reality (XR) and highlights the benefits of rendering XR content in local networks, enabling fast prototyping sessions, multi-user experiences, and industrial applications. Both Use Cases have been updated, in particular with regards to the role that HORSE can play in each one, with the help of updated information on the HORSE infrastructure, workflows and demonstration usage scenarios.

In view of the second architectural design phase of HORSE, to be documented in the upcoming deliverable D2.4, we have updated and enriched the functional and non-functional requirements of HORSE, taking also into account the experience gained by the HORSE project consortium partners, and the comments received during the mid-term review. These requirements shall be developed in the project's second iteration (IT-2) depending on their priority and shall ensure the development of holistic and resilient services.

Furthermore, we updated the description of the 6G network services and threats that the HORSE project will consider, including API exposure, AI- and ML-enabled operation, AI data training and heterogeneity research areas, in an effort to bring fresh ideas and incorporate them into the course of this 3-year long project.

This work will set in motion the definition of the updated HORSE architecture and ultimately steer the technical implementation of the HORSE project. The insights gained from the first half of the project will serve as valuable references for the development of cutting-edge technologies and policies that align with the goals of the project.

References

[1] Taleb, T., et al. (2022). 6G system architecture: A service of services vision. *ITU journal on future and evolving technologies*, *3*(3), 710-743.

[2] Zhang, X., & Zhu, Q. (2023). AI-enabled network-functions virtualization and software-defined architectures for customized statistical QoS over 6G massive MIMO mobile wireless networks. IEEE Network, 37(2), 30-37.

[3] Masaracchia, A., et al. (2022). Digital twin for 6G: Taxonomy, research challenges, and the road ahead. IEEE Open Journal of the Communications Society, 3, 2137-2150.

[4] Jawad, A. T., et al. (2023). A comprehensive survey on 6G and beyond: Enabling technologies, opportunities of machine learning and challenges. Computer Networks, 110085.

[5] Ferrag, M. A., et al. (2023). Generative AI for cyber threat-hunting in 6G-enabled IoT networks. In 2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW) (pp. 16-25). IEEE.

[6] NIST Releases First 3 Finalized Post-Quantum Encryption Standards, https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards, accessed 30 October 2024.

[7] Announcing Issuance of Federal Information Processing Standards (FIPS) FIPS 203, Module-Lattice-Based Key-Encapsulation Mechanism Standard, FIPS 204, Module-Lattice-Based Digital Signature Standard, and FIPS 205, Stateless Hash-Based Digital Signature Standard, https://www.federalregister.gov/documents/2024/08/14/2024-17956/announcing-issuance-of-federal-information-processing-standards-fips-fips-203-module-lattice-based, accessed 30 October 2024.

[8] Gupta, M., Akiri, C., Aryal, K., Parker, E. and Praharaj, L., 2023. From chatgpt to threatgpt: Impact of generative ai in cybersecurity and privacy. IEEE Access.

[9] Oprea, A. and Vassilev, A., 2023. Adversarial machine learning: A taxonomy and terminology of attacks and mitigations (No. NIST Artificial Intelligence (AI) 100-2 E2023 (Withdrawn)). National Institute of Standards and Technology.

[10] S. A. Abdel Hakeem, H. H. Hussein, and H. Kim, “Security requirements and challenges of 6G technologies and applications,” *Sensors*, vol. 22, no. 5, p. 1969, 2022.

[11] P. Porambage, G. Gür, D. P. M. Osorio, M. Livanage, and M. Ylianttila, “6G security challenges and potential solutions,” in *2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)*, IEEE, 2021, pp. 622–627.

[12] M. Wang, T. Zhu, T. Zhang, J. Zhang, S. Yu, and W. Zhou, “Security and privacy in 6G networks: New areas and new challenges,” *Digit. Commun. Netw.*, vol. 6, no. 3, pp. 281–291, 2020.

[13] M. Liyanage, A. Braeken, S. Shahabuddin, and P. Ranaweera, “Open RAN security: Challenges and opportunities,” *J. Netw. Comput. Appl.*, vol. 214, p. 103621, 2023.

[14] “Cybersecurity of Open Radio Access Networks | Shaping Europe’s digital future,” May 11, 2022. https://digital-strategy.ec.europa.eu/en/library/cybersecurity-open-radio-access-networks (accessed Jun. 25, 2023).

[15] HORSE Project (2023a). Deliverable D2.1 “HORSE Landscape: Technologies, State of the Art, AI Policies and Requirements”.

[16] "Network programmability in 5G: an invisible goldmine for service providers and industry." https://www.ericsson.com/en/blog/2019/1/network-programmability---in-5g-an-invisible-goldmine-for-service-providers-and-industry (accessed Jun. 25, 2023).

[17] "'NetApp: Opening up 5G and beyond networks' White Paper," *EVOLVED-5G*, Dec. 14, 2022. https://evolved-5g.eu/2022/12/14/netapp-opening-up-5g-and-beyond-networks-white-paper/ (accessed Jun. 25, 2023).

[18] "NWDAF: Automating the 5G network with machine learning and data analytics." https://inform.tmforum.org (accessed Jun. 25, 2023).

[19] "ETSI TS 133 521 V17.1.0 (2022-05) - 5G; 5G Security Assurance Specification (SCAS);Network Data Analytics Function (NWDAF) (3GPP TS 33.521 version 17.1.0 Release 17)," *iTeh Standards*. https://standards.iteh.ai/catalog/standards/etsi/2c528851-5a69-4889-a4e5-5dc31b138bac/etsi-ts-133-521-v17-1-0-2022-05 (accessed Jun. 25, 2023).

[20] N. Hu, Z. Tian, X. Du and M. Guizani, "An Energy-Efficient In-Network Computing Paradigm for 6G," in *IEEE Transactions on Green Communications and Networking*, vol. 5, no. 4, pp. 1722-1733, Dec. 2021, doi: 10.1109/TGCN.2021.3099804.

[21] T. Li, A. K. Sahu, A. Talwalkar and V. Smith, "Federated Learning: Challenges, Methods, and Future Directions," in *IEEE Signal Processing Magazine*, vol. 37, no. 3, pp. 50-60, May 2020, doi: 10.1109/MSP.2020.2975749.

[22] P. K. Gkonis, S. Lavdas, G. Vardoulias, P. Trakadas, L. Sarakis and K. Papadopoulos, "System Level Performance Assessment of Large-Scale Cell-Free Massive MIMO Orientations With Cooperative Beamforming," in *IEEE Access*, vol. 12, pp. 92073-92086, 2024, doi: 10.1109/ACCESS.2024.3422349.

[23] V. Özduran, N. Nomikos, E. Soleimani-Nasab, I. S. Ansari and P. Trakadas, "Relay-Aided Uplink NOMA Under Non-Orthogonal CCI and Imperfect SIC in 6G Networks," in *IEEE Open Journal of Vehicular Technology*, vol. 5, pp. 658-680, 2024, doi: 10.1109/OJVT.2024.3392951.

[24] H. Ahmadi, A. Nag, Z. Khar, K. Sayrafian, and S. Rahardja, "Networked twins and twins of networks: An overview on the relationship between digital twins and 6G," *IEEE Commun. Stand. Mag.*, vol. 5, no. 4, pp. 154–160, 2021.

[25] N. P. Kuruvatti, M. A. Habibi, S. Partani, B. Han, A. Fellan, and H. D. Schotten, "Empowering 6G Communication Systems With Digital Twin Technology: A Comprehensive Survey," *IEEE Access*, 2022.

[26] S. Vakaruk, A. Mozo, A. Pastor, and D. R. López, "A digital twin network for security training in 5G industrial environments," in *2021 IEEE 1st International Conference on Digital Twins and Parallel Intelligence (DTPI)*, IEEE, 2021, pp. 395–398.

[27] B. M. Lee, "Massive MIMO for Massive Industrial Internet of Things Networks : Operation, Performance, and Challenges," in *IEEE Transactions on Cognitive Communications and Networking*, doi: 10.1109/TCCN.2024.3392739.

[28] X. Zhai, X. Chen, J. Xu and D. W. Kwan Ng, "Hybrid Beamforming for Massive MIMO Over-the-Air Computation," in *IEEE Transactions on Communications*, vol. 69, no. 4, pp. 2737-2751, April 2021, doi: 10.1109/TCOMM.2021.3051397.

[29] V. Özduran, N. Nomikos, E. Soleimani-Nasab, I. S. Ansari and P. Trakadas, "Relay-Aided Uplink NOMA Under Non-Orthogonal CCI and Imperfect SIC in 6G Networks," in *IEEE Open Journal of Vehicular Technology*, vol. 5, pp. 658-680, 2024, doi: 10.1109/OJVT.2024.3392951.

[30] J. Bang, H. Chung, J. Hong, H. Seo, J. Choi and S. Kim, "Millimeter-Wave Communications: Recent Developments and Challenges of Hardware and Beam Management Algorithms," in IEEE Communications Magazine, vol. 59, no. 8, pp. 86-92, August 2021, doi: 10.1109/MCOM.001.2001010.

[31] P. K. Gkonis, S. Lavdas, G. Vardoulias, P. Trakadas, L. Sarakis and K. Papadopoulos, "System Level Performance Assessment of Large-Scale Cell-Free Massive MIMO Orientations With Cooperative Beamforming," in IEEE Access, vol. 12, pp. 92073-92086, 2024, doi: 10.1109/ACCESS.2024.3422349.

[32] V.-L. Nguyen, P.-C. Lin, B.-C. Cheng, R.-H. Hwang, and Y.-D. Lin, "Security and privacy for 6G: A survey on prospective technologies and challenges," *IEEE Commun. Surv. Tutor.*, vol. 23, no. 4, pp. 2384–2428, 2021.

[33] S. Shen, C. Yu, K. Zhang, J. Ni, and S. Ci, "Adaptive and dynamic security in AI-empowered 6G: From an energy efficiency perspective," *IEEE Commun. Stand. Mag.*, vol. 5, no. 3, pp. 80–88, 2021.

[34] D. Je, J. Jung, and S. Choi, "Toward 6G security: technology trends, threats, and solutions," *IEEE Commun. Stand. Mag.*, vol. 5, no. 3, pp. 64–71, 2021.

[35] E. Rodriguez, B. Otero, N. Gutierrez, and R. Canal, "A survey of deep learning techniques for cybersecurity in mobile networks," *IEEE Commun. Surv. Tutor.*, vol. 23, no. 3, pp. 1920–1955, 2021.

[36] A. Afaq, N. Haider, M. Z. Baig, K. S. Khan, M. Imran, and I. Razzak, "Machine learning for 5G security: Architecture, recent advances, and challenges," *Ad Hoc Netw.*, vol. 123, p. 102667, 2021.

[37] O. Jullian, B. Otero, E. Rodriguez, N. Gutierrez, H. Antona, and R. Canal, "Deep-Learning Based Detection for Cyber-Attacks in IoT Networks: A Distributed Attack Detection Framework," *J. Netw. Syst. Manag.*, vol. 31, no. 2, p. 33, 2023.

[38] H. Sedjelmaci, "Attacks detection approach based on a reinforcement learning process to secure 5g wireless network," in *2020 IEEE International Conference on Communications Workshops (ICC Workshops)*, IEEE, 2020, pp. 1–6.

[39] S. Jayasinghe, Y. Siriwardhana, P. Porambage, M. Liyanage, and M. Ylianttila, "Federated learning based anomaly detection as an enabler for securing network and service management automation in beyond 5g networks," in *2022 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)*, IEEE, 2022, pp. 345–350.

[40] S. Kim, K.-J. Park, and C. Lu, "A survey on network security for cyber–physical systems: From threats to resilient design," *IEEE Commun. Surv. Tutor.*, vol. 24, no. 3, pp. 1534–1573, 2022.

[41] S. Dong, Y. Xia, and T. Peng, "Network abnormal traffic detection model based on semi-supervised deep reinforcement learning," *IEEE Trans. Netw. Serv. Manag.*, vol. 18, no. 4, pp. 4197–4212, 2021.

[42] A. Alotaibi and A. Barnawi, "Securing massive IoT in 6G: Recent solutions, architectures, future directions," *Internet Things*, p. 100715, 2023.

[43] D. Sirohi, N. Kumar, P. S. Rana, S. Tanwar, R. Iqbal, and M. Hijjii, "Federated learning for 6G-enabled secure communication systems: a comprehensive survey," *Artif. Intell. Rev.*, pp. 1–93, 2023.

[44] N. Ebrahimi, H.-S. Kim, and D. Blaauw, "Physical layer secret key generation using joint interference and phase shift keying modulation," *IEEE Trans. Microw. Theory Tech.*, vol. 69, no. 5, pp. 2673–2685, 2021.

[45] N. Xie, Z. Li, and H. Tan, “A survey of physical-layer authentication in wireless communications,” *IEEE Commun. Surv. Tutor.*, vol. 23, no. 1, pp. 282–310, 2020.

[46] Oleiwi, Haider W., Doaa N. Mhawi, and H. S. Al-Raweshidy. "A Secure Deep Autoencoder-based 6G Channel Estimation to Detect/Mitigate Adversarial Attacks." *2023 5th Global Power, Energy and Communication Conference (GPECOM)*. IEEE, 2023.

[47] Li, Weiwei, et al. "When Industrial Radio Security Meets AI: Opportunities and Challenges." *IEEE Transactions on Industrial Informatics* (2024).

[48] T. Edwards and M. S. Hossain, “Effectiveness of deep learning on serial fusion based biometric systems,” *IEEE Trans. Artif. Intell.*, vol. 2, no. 1, pp. 28–41, 2021.

[49] Y. Al-Eryani and E. Hossain, “The D-OMA method for massive multiple access in 6G: Performance, security, and challenges,” *IEEE Veh. Technol. Mag.*, vol. 14, no. 3, pp. 92–99, 2019.

[50] T. Li, Z. Hong, L. Liu, Z. Wen, and L. Yu, “Meta-WF: Meta-Learning-Based Few-Shot Wireless Impersonation Detection for Wi-Fi Networks,” *IEEE Commun. Lett.*, vol. 25, no. 11, pp. 3585–3589, 2021.

[51] B. Li, Y. Wu, J. Song, R. Lu, T. Li, and L. Zhao, “DeepFed: Federated deep learning for intrusion detection in industrial cyber–physical systems,” *IEEE Trans. Ind. Inform.*, vol. 17, no. 8, pp. 5615–5624, 2020.

[52] I. A. Ridhawi, S. Otoum, and M. Aloqaily, “Decentralized Zero-Trust Framework for Digital Twin-based 6G,” *ArXiv Prepr. ArXiv230203107*, 2023.

[53] M. A. Rahman and M. S. Hossain, “A deep learning assisted software defined security architecture for 6G wireless networks: IIoT perspective,” *IEEE Wirel. Commun.*, vol. 29, no. 2, pp. 52–59, 2022.

[54] Kianpisheh, Somayeh, and Tarik Taleb. "Collaborative Federated Learning for 6G With a Deep Reinforcement Learning Based Controlling Mechanism: A DDoS Attack Detection Scenario." *IEEE Transactions on Network and Service Management* (2024).

[55] I. K. Dutta, B. Ghosh, A. Carlson, M. Totaro, and M. Bayoumi, “Generative adversarial networks in security: a survey,” in *2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, IEEE, 2020, pp. 0399–0405.

[56] E. Rodríguez *et al.*, “Transfer-Learning-Based Intrusion Detection Framework in IoT Networks,” *Sensors*, vol. 22, no. 15, p. 5621, 2022.

[57] A. Clemm, L. Ciavaglia, L. Granville, and J. Tantsura, “RFC 9315 Intent-Based Networking-Concepts and Definitions,” 2022.

[58] “ENISA Transport Threat Landscape — ENISA.” https://www.enisa.europa.eu/publications/enisa-transport-threat-landscape (accessed Jun. 25, 2023).

[59] S. Bradner, “RFC2119: Key words for use in RFCs to Indicate Requirement Levels.” RFC Editor, 1997.

[60] Slawomir Kuklinski, Lechoslaw Tomaszewski, Robert Kolakowski, Prosper Chemouil. 6G-LEGO: A framework for 6G network slices. Journal of Communications and Networks, 2021, Journal of Communications and Networks, 23 (6), pp.442 - 453. 10.23919/JCN.2021.000025 . hal-03443008.

[61] 3GPP. "Study on enhanced security for network slicing phase 3". TR 33.886 V18.1.0 (2023-09).

[62] 3GPP. "Security Assurance Specification (SCAS) for the Network Slice-Specific Authentication and Authorization Function (NSSAAF) network product class". TS 33.326. V18.0.0 (2023-06).

[63] Peter Schmitt. "Rel-18 Stage3 - Completion in TSG CT". 3GPP Highlights. Jun 2024. Available at: https://www.3gpp.org/newsletter-issue-08-jun-2024.

[64]"'6G Architecture Landscape – European perspective' White paper." https://5g-ppp.eu/6g-architecture-landscape-european-perspective-white-paper/ (accessed Jun. 25, 2023).

[65]J. Lin, L. Dang, M. Rahouti, and K. Xiong, "Ml attack models: Adversarial attacks and data poisoning attacks," *ArXiv Prepr. ArXiv211202797*, 2021.

[66]"Mitigations Against Adversarial Attacks," *F-Secure Blog*, Jul. 11, 2019. https://blog.f-secure.com/mitigations-against-adversarial-attacks/ (accessed Jun. 25, 2023).

[67] Ferrag, M. A., Alwahedi, F., Battah, A., Cherif, B., Mechri, A., & Tihanyi, N. (2024). Generative AI and Large Language Models for Cybersecurity. arXiv preprint arXiv:2405.12750v1.

[68] Zhang, J., Bu, H., Wen, H., Chen, Y., Li, L., & Zhu, H. (2024). When LLMs Meet Cybersecurity: A Systematic Literature Review. arXiv preprint arXiv:2405.03644v1.

[69] Tihanyi, N., Ferrag, M. A., Jain, R., Bisztray, T., & Debbah, M. (2024). CyberMetric: A Benchmark Dataset for Evaluating LLMs in Cybersecurity Knowledge. arXiv preprint arXiv:2402.07688v2. Divakaran, D. M., & Peddinti, S. T. (2024). LLMs for Cyber Security: New Opportunities. arXiv preprint arXiv:2404.11338v1.

[70] Divakaran, D. M., & Peddinti, S. T. (2024). LLMs for Cyber Security: New Opportunities. arXiv preprint arXiv:2404.11338v1.

[71] Xu, H., Wang, S., Li, N., Wang, K., Zhao, Y., Chen, K., et al. (2024). Large Language Models for Cyber Security: A Systematic Literature Review. arXiv preprint arXiv:2405.04760v3.

[72] Nourmohammadzadeh, F., Hajizadeh, M., Majd, M., Najafi, P., Cheng, F., & Meinel, C. (2024). Large Language Models in Cybersecurity: State-of-the-Art. arXiv preprint arXiv:2402.00891v1.

[73] Clemm, A. (2021). Intent-Based Network Management. In: Toy, M. (eds) Future Networks, Services and Management. Springer, Cham. https://doi.org/10.1007/978-3-030-81961-3_14.

[74] X. Wu, L. Xiao, Y. Sun, J. Zhang, T. Ma, L. He. A survey of human-in-the-loop for machine learning. Future Generat. Comput. Syst., 135 (2022), pp. 364-381.

[75] HORSE Project (2024a). Deliverable D5.1 "HORSE demonstration scenario".

[76] 3GPP, "5G Security Assurance Specification (SCAS) for the Network Exposure Function (NEF) network product class", Technical Specification TS33.519 version 16.2.0 (accessed Nov. 04, 2024).

[77] ETSI, "ETSI Software Development Group OpenCAPIF". https://ocf.etsi.org/documentation/latest (accessed Nov. 04, 2024)

[78] F. Alriksson, D. H. Kang, C. Phillips, J. L. Pradas and A. Zaidi, "XR and 5G: Extended reality at scale with time-critical communication," in Ericsson Technology Review, vol. 2021, no. 8, pp. 2-13, August 2021, doi: 10.23919/ETR.2021.9904681

[79] Virtual and augmented reality could deliver a $1.5 trillion boost to the global economy by 2030 – PwC, https://www.pwc.com/th/en/press-room/press-release/2020/press-release-29-01-20-en.html, accessed 30 October 2024

[80] Autodesk, Demystifying Digital Twin, https://f.hubspotusercontent40.net/hubfs/4545544/AEC%20Demystifying%20Digital%20Twin%20(EN).pdf, accessed 30 October 2024