RIGOUROUS

Funded by
the European Union

RIGOUROUS -
secuRe desIGn and deplOyment of trUsthwoRthy cOntinUum computing 6G Services

Deliverable 2.2

RIGOUROUS USE-CASES

Title	RIGOUROUS Use Cases
Document description	This deliverable reports the specifications of the RIGOUROUS project's use cases and the validation scenarios as well as the use cases functional requirements.
Nature	Public
Task	T2.2
Status	F: Final
WP	WP2
Lead Partner	ICT-FI
Partners Involved	UMU, ORO, LNVO, WINGS, ONE, OULU, ITAV
Date	21/12/2023

Revision history	Author	Delivery date	Summary of changes and comments
Version 01	**ICT-FI**	27/02/2023	Creation of Table of Content Initial description of Use Cases
Version 02	**ORG**	05/07/2023	Updates to Section 3 - ORO Use-Case
Version 03	**ALL**	28/11/2023	Preparation of an internal version of the document
Version 04	**UMU, ONE**	04/12/2023	Internal review comments received
Version 05	**ALL**	15/12/2023	Internal review comments addressed
Final Version	**ICT-FI & OULU, UMU**	19/12/2023	Final version was prepared and submitted to Coordinator and final revision by UMU

Disclaimer:

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

CONTENTS

LIST OF ABBREVIATIONS AND ACRONYMS

Abbreviation	Explanation/ Definition
IoT	Internet of Things
AI	Artificial Intelligence
PPDR	Public Protection and Disaster Relief
DDoS	Distributed Denial-of-Service
VNFs	Virtual Network Function
PNFs	Physical Network Functions
UAT	User Acceptance Test
B2B	business-to-business
NG Firewalls	Next-generation firewall
IDS	Intrusion detection systems (IDS)
IPS	Intrusion prevention systems (IPS)
IoTSCP	IOT-based Smart City Platform
VR	Video on Demand
GPS	Global Positioning System
RTMP	Real-Time Messaging Protocol
WebRTC	Web Real-Time Communication
UUID	Universal Unique Identifier
EaaS	Encryption as a Service
TLS	Transport Layer Security
EDoS	Economic denial of sustainability
MTD	Moving Target Defense
ML	Machine Learning

API	Application programming interface
QoS	Quality of service
HMDs	Head-Mounted Displays
BYOD	Bring Your Own Device
FL	Federated learning
TRA	Threat Risk assessor

LIST OF FIGURES

LIST OF TABLES

1 Executive Summary

This document represents the outcome of our research in Task 2.2. We adopted a comprehensive approach to achieve several objectives. In the area of defining and refining the use cases of RIGOROUS, we aimed to establish a clear and precise understanding of the practical applications of the project. We then shifted our focus to conducting an in-depth analysis of the security threat landscape related to the project's use cases. This involved identifying and organizing potential threats into coherent scenarios, providing a comprehensive view of the security challenges faced. Within each scenario, we explored the major security challenges in detail, aiming to gain a nuanced understanding of the security aspects inherent in the project.

Effectively, the document provides a detailed review of the following four distinct use cases, each offering high-level descriptions and associated security threat scenarios.

- Use Case I - RIGOUROUS Platform Validation: Focused on validating the RIGOUROUS platform's capability to enhance the flexibility of telecommunication infrastructures, this use case centers around the Orange 5G Romania lab. Addressing the transformative challenges of 6G, it employs a DevSecOps approach to integrate security seamlessly into the development lifecycle. Specifically addressing "Protecting 6G Services against Cyber Threats," it assesses performance through three threat scenarios, confirming the platform's effectiveness in identifying, responding to, and mitigating complex cyber threats to vital 6G infrastructure.
- Use Case II - IoT-Based Smart City Platform: This use case revolves around a cloud-native IoT platform designed for smart city applications. Leveraging docker-based micro-services and Kubernetes, it manages diverse IoT data from gateways, supposedly spread across the city, supporting various communication technologies and devices. Security threat scenarios, including unauthorized communications and economical denial of service, are meticulously examined, emphasizing correlations with critical assets.
- Use Case III - Utilities Management and Security (WINGS): This in-depth examination focuses on facilities management with a specific emphasis on data security. Threat scenarios encompass data security, DDOS attacks, code, and data injection, along with challenges posed by outdated systems. Asset correlations are highlighted to provide a comprehensive understanding.
- Use Case IV - Public Protection and Disaster Relief (PPDR): Detailing scenarios involving PPDR scene and team provisioning, potential intrusions, and disclosure of device vulnerabilities. This case highlights the correlations between assets and critical elements that are at risk. Regarding this use case, and Use Case II, after a thorough investigation comparing the technologies and key principles used in the design of the two use case, this document recommends their merge.

At the end of the deliverable, a mapping between the use cases and the RIGOUROUS's high-level architecture, on one hand, and the project's assets on another hand is provided. The RIGOUROUS project's identified use cases create a strategic framework to address evolving telecommunications and security challenges, with each pivotal in shaping the project's comprehensive approach. The intention behind this deliverable is to extend its influence beyond the immediate scope by providing Guidance for WP3-4 Research. Derived from our findings, this guidance informs and directs the research efforts of WP3-4, ensuring a cohesive and synergistic progression. In essence, this deliverable not only encapsulates the outcomes of our research in T2.2 but also serves as a roadmap, guiding subsequent research endeavors within WP3-4.

2 INTRODUCTION

This deliverable introduces the use cases of the RIGOUROUS project, detailing their corresponding threat scenarios and providing some insights on the respective mitigation strategies. The content presented is a culmination of the efforts undertaken in Task 2.2, closely coordinated with other tasks within WP2 and across various Work Packages.

The initial use case concentrates on safeguarding 6G-enabled services from cyber threats, outlining three specific scenarios. The first scenario explores unauthorized access to the 5G/6G infrastructure, addressing both insider threats (privilege abuse) and external threats (exploitation of software vulnerabilities or erroneous configurations). To counteract these risks, RIGOUROUS components are deployed on the underlying OS components of the OSM platform. These components conduct audits, monitor login attempts, correlate timestamps and IP sources, and have the capability to block unauthorized activities. The second scenario involves an adversary utilizing commercially available tools to target live hosts in ORO MEC, aiming to create a threat profile of one of ORO's B2B customers. RIGOUROUS is designed to detect scanning technology signatures and enumeration attempts, responding with an IDS/IPS service to block such activities. The third scenario considers a distributed denial-of-service (DDoS) attack on system components, where RIGOUROUS is expected to detect ongoing attacks and trigger changes within the 5G Orchestrator to enhance infrastructure resilience through automated response orchestration and mitigation.

Transitioning to the second use case, which centers around the IoT-based Smart City Platform, three scenarios and their corresponding mitigation approaches are delineated. The first scenario involves an economical denial of service, with the proposed mitigation approach encompassing an AI-based EDoS detection and mitigation. The second scenario focuses on preventing unlawful access to IoT data violating data privacy, and leveraging an Encryption as a Service platform for cryptographic services to IoT gateways. The third scenario deals with unlawful access/communication to/with IoT gateways, the platform's micro-services, and APIs. Mitigation approaches include secure remote access to IoT gateways through fast authentication, securing service APIs, and ensuring secure communications among micro-services, even across multiple cloud domains. The two last scenarios may relate to all use cases of the project.

In response to the increasing prevalence of mobile networks and cloud adoption in the utilities sector, WINGS introduces the ARTEMIS platform, an end-to-end solution for proactive utility management. ARTEMIS integrates IoT, cloud, AI, and visualization, ensuring secure connectivity through the Smart Gateway. Addressing security concerns, the third use case focuses on the European Gas Network's resilience and protection against cyberattacks, offering a comprehensive and proactive defense against potential threats in the utilities sector.

The fourth use case centers on a PPDR (Public Protection and Disaster Relief) IoT Situational Awareness platform, featuring various scenarios. The suggested mitigation approaches include authentication and authorization for different assets and components within the Command-and-Control Centre, monitoring communications to detect abnormal activities, and implementing appropriate measures when a rogue element attempts to interact with the system or decommission an untrusted device.

Table 2-1 illustrates the alignment between the project objectives and each threat scenario within each project use case. These tables underscore the comprehensive validation potential of the envisioned use cases and associated threat scenarios, showcasing their effectiveness in validating all project objectives.

Table 2-1 Relevance of the use case threat scenarios to the project objectives.

UC1				
	Threat Scenarios			
	Threat Scenario 1: unauthorized access	Threat Scenario 2: Information Gathering about Services and Devices communicating through the Internet.	Threat Scenario 3: A service exposed through an EDGE component of ORO 6G Facility is targeted and attacked	RIGOUROUS Objectives
Relevance to Project Objectives	1 2 5	1 2 3 4 5	1 2 3 4 5	1- Holistic Smart Service framework for securing the IoT-Edge-Cloud continuum lifecycle management
				2- Human-Centric DevSecOps
				3- Model-based and AI-driven Automated Security Orchestration, Trust Management, and deployment
				4- Advanced AI-driven Anomaly Detection, decision, and Mitigation Strategies
				5- Demonstration of a Set of Industrially Relevant Use Cases in Operational Environments

UC2				
	Threat Scenarios			
	Threat Scenario 1: Unlawful access to IoT gateways, platform's APIs, and IoT data violating data privacy	Threat Scenario 2: Unauthorized communications to micro-services of an IoT smart city platform	Threat Scenario 3: Economical Denial of Service and Adversary AI attacks	RIGOUROUS Objectives
Relevance to Project Objectives	1 2 5	1 3	1 2 3 4 5	1- Holistic Smart Service framework for securing the IoT-Edge-Cloud continuum lifecycle management
				2- Human-Centric DevSecOps
				3- Model-based and AI-driven Automated Security Orchestration, Trust Management, and deployment

				4- Advanced AI-driven Anomaly Detection, decision, and Mitigation Strategies
				5- Demonstration of a Set of Industrially Relevant Use Cases in Operational Environments

UC3

	Threat Scenarios			RIGOUROUS Objectives
	Threat Scenario 1: **Data Security - Unauthorized access / Threat Scenario 2: Distributed Denial of Service (DDoS) attacks**	**Threat Scenario 3:Code and data injection attacks**	**Threat Scenario 3:** **Outdated systems**	
Relevance to Project Objectives	**4**	**1** **2** **4**	**2** **3**	1- **Holistic Smart Service framework for securing the IoT-Edge-Cloud continuum lifecycle management**
				2- **Human-Centric DevSecOps**
				3- **Model-based and AI-driven Automated Security Orchestration, Trust Management, and deployment**
				4- **Advanced AI-driven Anomaly Detection, decision, and Mitigation Strategies**
				5- **Demonstration of a Set of Industrially Relevant Use Cases in Operational Environments**

UC4

	Threat Scenarios			RIGOUROUS Objectives
	Threat Scenario 1: PPDR scene and teams provisioning	**Threat Scenario 2: Intrusion into system to access privileged information or cause disruption of services**	**Threat Scenario 3: Disclosure of device vulnerability or unlawful appropriation of a device**	
Releva nce to Projec	**1** **2**	**1** **2**	**2** **4**	1- **Holistic Smart Service framework for securing the IoT-Edge-**

	3 **4** **5**	**3** **4** **5**	**5**		**Cloud continuum lifecycle management**
					2- **Human-Centric DevSecOps**
					3- **Model-based and AI-driven Automated Security Orchestration, Trust Management, and deployment**
					4- **Advanced AI-driven Anomaly Detection, decision, and Mitigation Strategies**
					5- **Demonstration of a Set of Industrially Relevant Use Cases in Operational Environments**

This deliverable concludes with a mapping between the use cases and the RIGOUROUS's high-level architecture, connecting them to the project's assets. Identified use cases form a strategic framework, addressing evolving telecommunications and security challenges. Beyond its immediate scope, this deliverable guides WP3-4 Research, informing and directing ongoing efforts, and serves as a roadmap for subsequent research endeavors within WP3-4. In essence, it not only encapsulates the outcomes of T2.2 research but also functions as a guiding document for the project's future research activities.

3 Use Case I

3.1. Use Case‘s High Level Description

6G will pave the way for new services in telecom infrastructures, an essential aspect for future networks implementation, aiming to support 6G vertical use cases in different sectors such as Health, Automotive, Manufacturing, Media, Energy, Public safety and cover the 6G service types including Internet of Things (IoT), EDGE computing or Fog and Cloud Computing [1].

6G requires impressive network transformation, from dedicated network functions to software network functions, new physical infrastructure deployment, the network virtualisation concepts and new 6G functions. The network transformation from dedicated network functions to software virtualised implementations may open a series of security issues, from physical infrastructure - Physical Network Functions (PNFs), virtualised infrastructure and virtualisation implementation - Network Function Virtualisation (NFV) / Virtual Network Function (VNFs), 6G network functions (Service Based Architecture), 6G Management and Orchestration (MANO), control, and data plane, that may be exposed to several cyber security attacks [2,3].

The Use-Case to be piloted will validate the capacity and capabilities of the platform to increase the resilience of the Telecommunication infrastructures by protecting against threats to services offered by Orange Romania. Orange Romania use case will be run in Orange 5G LAB (https://5glab.orange.ro). Orange 5G lab is described as a complete 5G/6G testing area network infrastructure.

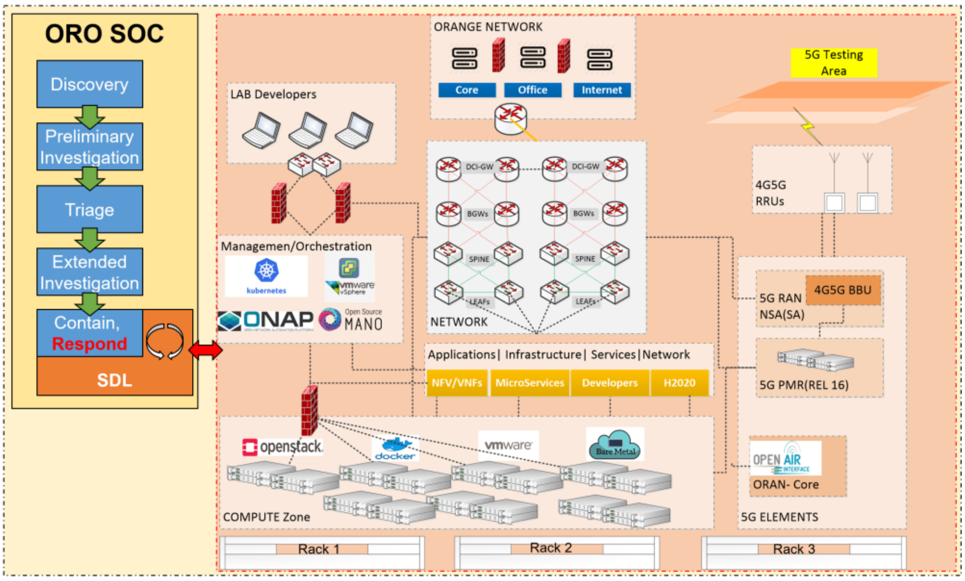

Figure 3-1 Orange 5G Lab High-Level Architecture

The Use-Case to be piloted will validate the capacity and capabilities of the platform to increase the resilience of the Telecommunication infrastructures by protecting against threats to services offered by Orange Romania. Orange Romania use case will be run in Orange 5G LAB (https://5glab.orange.ro). Orange 5G lab is described as a complete 5G/6G testing area network infrastructure for several use cases (IoT) and it is suitable to be exposed as a 5G/6G infrastructure running security threats. The 5G lab includes the 5G/6G network components and functions, as described in Figure 3–1.

The ORO 5GLab Testbed automates the integration of Security in each phase of the development and engineering life-cycles, from initial design through integration, deployment, testing and validation. This DevSecOps approach to innovation and development processes, enables ORO to interface the RIGOUROUS Operations Planes, to existing Security Operations Center architecture, processes and tools and presents ORO with the opportunity to enhance the in-life security design, deployment, testing and validation for new 5G and 6G Services and Network Applications.

The Protection of 6G Services against Cyber Threats Use-Case, piloted by ORO relies on 3 threat scenarios developed to validate the RIGOUROUS platform capabilities of detection, response, and mitigation of complex cyber threats to relevant 6G infrastructures.

3.2. Security Threat Scenarios

3.2.1. Threat Scenario 1

A first threat scenario envisions unauthorized access to the 6G Infrastructure through privilege abuse, by an inside actor and by an outside actor, through the exploitation of software vulnerabilities or erroneous configurations in the 6G Facility infrastructures.

3.2.1.1. Threat Scenario Description

The threat scenario assumes that the access to ORO's 6G Facility is monitored and protected through State-Of-The-Art deployments of security measures and operational best-practices. There are, thus, two distinct approaches of the attackers to access the 6G Facility, each approach utilizing different vectors of attack and a different set of vulnerabilities and exploits.

3.2.1.1.1 By Authentication Abuse:

An ORO employee with access to administrative credentials to several ORO Facility endpoints of OS MANO logs in from an endpoint other than the terminal they usually log in from and performs an action that changes the parameters of a VNF (Virtual Network Function), in this scenario a Web Server hosting a B2B Customer's Web Portal, that is deployed in production, disrupting service availability and integrity. Furthermore, this ORO employee deploys a back-door type service on one of the endpoints, allowing remote and external incoming connections.

In a subsequent event, an external adversary gains access to the endpoint previously compromised through the deployment of a back-door and succeeds to move laterally through the 5G Facility components and gains access to 5G Control Plane subsystems, specifically - but not limited to - the Hyper-visor components of the virtual infrastructure. They succeed in disrupting service continuity by migrating containers in production to a User Acceptance Test (UAT) environment. The virtualisation components affected by this attack are using Kubernetes for automatic deployment, sizing, and management of the containers, atop OpenStack deployments.

3.2.1.1.2 By Exploiting Software Vulnerabilities and Erroneous Configurations, Supply-Chain Attack:

In this threat scenario, an adversary working for a third-party supplier of ORO, with knowledge of the architecture and security posture of OROs Facilities, leverages their knowledge to exploit a vulnerability in the authentication feature exposed through an API of OS MANO. This adversary, who was previously involved in the deployment of various software components in OROs Facility, has specific knowledge on the vulnerabilities in certain services used in OS MANO and knowingly withholds this knowledge from ORO, only to use a specifically crafted exploit, later, providing them with administrative access to the OS MANO components. By gaining access, they proceed to modify configurations of OS MANO and installs rootkit-class malicious software on the underlying OSs hosting OS MANO, providing them with undiscriminating access to parts of the 5G Facility and proceeds to move laterally through the network, affecting services' availability and ex-filtrating confidential information stored in one Database instance used by a B2B Customer.

3.2.1.2. Mitigation Approach and Relevant Tools

In the Unauthorised Access Scenario, RIGOUROUS components are deployed on the underlying OS Components of the OSM platform and have the capability to audit and monitor login attempts to OSM's interfaces, via a proxy-similar deployment.

The RIGOUROUS components should have the ability to correlate timestamps and IP Sources to known behaviour and flag as suspicious any behaviour in authentication, above or below the baseline (i.e. - 'known behaviour'). Furthermore, the RIGOUROUS components should be able to block the unauthorized activities.

The detection mechanisms envisioned in this thread scenario relies on either RIGOUROUS-developed agent to be deployed on Linux targets hosting OSM components AND/OR on open-source available EDR-type agents such as OSSEC (HTTPS://WWW.OSSEC.NET/).

The agents will have the capability to provide, at minimum:

- Log-based Intrusion Detection
- Rootkit Detection
- Malware Detection
- Active Response
- Compliance Auditing
- File Integrity Monitoring
- System Inventory

RIGOUROUS's SOAR (Security, Orchestration, Automation, Response) cognitive loops should integrate threat data from these agents and further orchestrate the mitigation actions by integration with the State-Of-The-Art Security mechanisms available in ORO's Facility AND/OR RIGOUROUS-developed components.

Furthermore, RIGOUROUS should interface with ORO's existing Security Operations Center architecture, to enhance the alerting, prioritization and mitigation activities of the SOC Analysts. By enabling ORO's DevSecOps paradigm during the in-live (RUN) phase of the SDL, RIGOUROUS will contribute to improving the proactive and reactive security postures of ORO's SOC by accelerating the security vulnerabilities patching DevSecOps-process, as part of the SDL. (Figure 3-2: The DevSecOps Mitigation Approach).

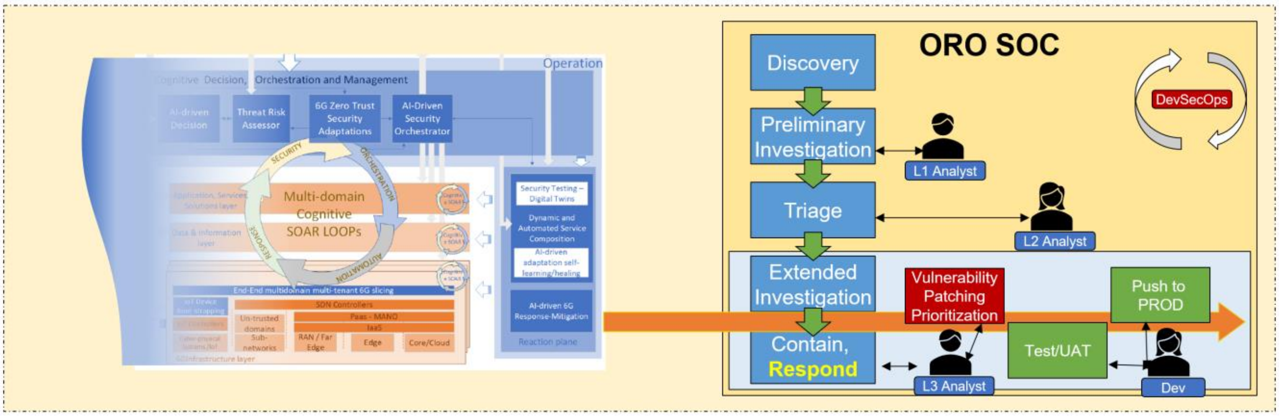
Operation
Cognitive Decision, Orchestration and Management
AI-driven Decision
Threat Risk Assessor
6G Zero Trust Security Adaptations
AI-Driven Security Orchestrator
SECURITY
ORCHESTRATION
AUTOMATION
RESPONSE
Application, Services Solutions layer
Data & information layer
Multi-domain Cognitive SOAR LOOPs
End-End multidomain multi-tenant 6G slicing
SON Controllers
Paas - MANO
IaaS
Un-trusted domains
Sub-networks
RAN / Far Edge
Edge
Core/Cloud
6G infrastructure layer
Security Testing – Digital Twins
Dynamic and Automated Service Composition
AI-driven adaptation self-learning/healing
AI-driven 6G Response-Mitigation
Reaction plane
ORO SOC
Discovery
Preliminary Investigation
Triage
Extended Investigation
Contain, Respond
L1 Analyst
L2 Analyst
L3 Analyst
DevSecOps
Vulnerability Patching Prioritization
Push to PROD
Test/UAT
Dev

Figure 3-2 ORO Use-Case Scenario 1 DevSecOps Mitigation Approach

In this scenario, L1 and L2 SOC Analysts will receive alerts triggered by RIGOUROUS, relevant to the exploitation attempts of an (previously) unknown vulnerability, in ORO's Testbed Environment. Through the preliminary investigation and triage processes, the Analysts validates the incident and the apparent cause, and escalates to the L3 Analysts, as they prioritize the patching of the vulnerability, in the Vulnerability Management Process.

By the means of an Agile Process, a Developer initiates the User Accepting Testing (UAT) Process and finalizes the push to production of the previously patched service.
By integrating RIGOUROUS in the DevSecOps processess of ORO's SOC, the mitigation loops, including containment and response to threats, will enable the SOC Analysts to improve the patching prioritization activities, part of the vulnerability management processes.

3.2.1.3. KPI and KVI

Table 3-1 The details of KPI and KVI

KPI	Description
KPI-13	Increase of accuracy in anomaly detection to exceed > 95%
KPI-14	Time to detection to reach real-time detection of order of milliseconds.
KPI-16	Number of kinds of Cyberattacks detected through AI > 10.
KPI-22	Target mitigation time against cyber-attacks, including all the stages of the complete SOAR cognitive loop (SOTA: 480 minutes; RIGOUROUS:<1min).
KPI-6	AI-powered Orchestration of four (04) kinds of resources, namely: services, devices, virtual network functions, and physical network functions.
KPI-11	OPEX reduction by at least 15% / Year in detection, decision, and mitigation.

3.2.1.4. Relevance to RIGOUROUS Objectives and Technical Tasks

Objective 2: Human-Centric DevSecOps - Scenario 1 of Use Case 1 will validate the implementation of the human-in-the-loop approach to the security and privacy models, as well as to the processes in place for Operational Cyber Security.

Objective 3: Model-based and AI-driven Automated Security Orchestration, Trust Management, and deployment - This scenario will leverage the Model-Based SOAR capabilities of RIGOUROUS to orchestrate automated mitigation against the threats simulated in the two threat conditions.

Objective 5 - Demonstration of a Set of Industrially Relevant Use Cases in Operational Environments - This Scenario will demonstrate the capabilities of RIGOUROUS to support mitigation of authentication abuse cybersecurity threats, to a telecommunications provider test-bed, replicating commercial-level services.

3.2.2. Threat Scenario 2

The second scenario refers to Information Gathering about Services and Devices communicating through the Internet. The perpetrators act as B2B customers and locate vulnerabilities in the MEC and access the network without authorization. The system should be able to detect these attempts and mitigate the impact.

3.2.2.1. Threat Scenario Description

In this scenario, an adversary using commercially available and open-source tools, while using a set of specific procedures, targets the live hosts in ORO MEC to identify live ports, and services, to discover vulnerabilities and threats in the network, and to discover and identify Operating systems and the architecture of the target systems. The adversary's goal is to create a threat profile of ORO's 5G Facility.

The attacker performs unauthorized audits ''scans" of the address space used by a B2B Customer of ORO for their Devices and Services communicating through the Internet, they assess existing vulnerabilities and misconfiguration in software, to be further used in orchestrating a cyber-attack. The attacker uses various scanning tools (freely available for download) on public IP ranges of ORO, assigned to the B2B Customer specific services, such as web servers hosting APIs, Web Portals, and custom services used by the IoT devices connected directly to the Internet.

The information gathered through this process can be further used to effectively evaluate the threat perimeter of ORO's Facility and their B2B Customers' and choose the relevant tactics, techniques and procedures needed to compromise the Facility's security.

3.2.2.2. Mitigation Approach and Relevant Tools

RIGOUROUS should have the ability to detect scanning technology signatures and enumeration attempts and respond by enabling and IDS/IPS service on the targeted part of the network, with the capability to block the scanning and enumeration attempts.

The detection can be achieved by correlating data coming from the AI-driven anomaly detection, decision, composition, and mitigation components to be developed in RIGOUROUS, to data coming from existing State-of-The-Art security technologies available in ORO's Facility (such as NG Firewalls).

The mitigation is expected to be achieved by using the SOAR cognitive loop capabilities in configuring and deploying an IDS/IPS capability to ORO's Facility, thus effectively blocking the scanning and enumeration attempts.

By enabling an automated response and orchestration capability to the Intrusion Detection and Prevention capabilities of ORO's Networks, RIGOUROUS will contribute to the overall agility of ORO's Security Operations processes and Network Operations Processes. (Figure 3-3: ORO Use-Case Scenario 2 - DevSecOps Mitigation Approach).

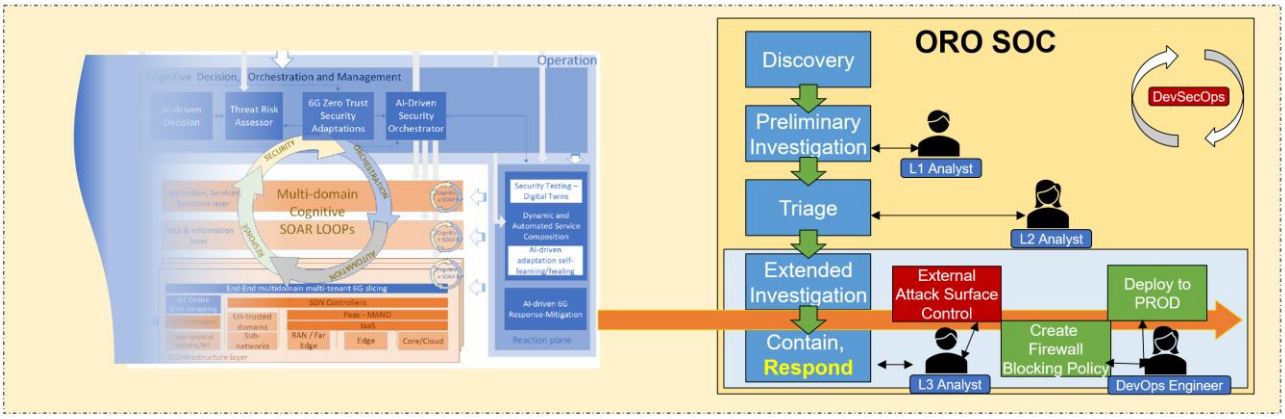
Operation
Cognitive Decision, Orchestration and Management
AI-driven Decision
Threat Risk Assessor
6G Zero Trust Security Adaptations
AI-Driven Security Orchestrator
SECURITY
ORCHESTRATION
AUTOMATION
RESPONSE
Application, Services, Solutions layer
Data & Information layer
Multi-domain Cognitive SOAR LOOPs
End-End multidomain multi-tenant 6G slicing
SDN Controllers
Un-trusted domains
Sub-networks
Paas - MANO
IaaS
RAN / Far Edge
Edge
Core/Cloud
6G Infrastructure layer
Security Testing – Digital Twins
Dynamic and Automated Service Composition
AI-driven adaptation self-learning/healing
AI-driven 6G Response-Mitigation
Reaction plane
ORO SOC
Discovery
Preliminary Investigation
Triage
Extended Investigation
Contain, Respond
L1 Analyst
L2 Analyst
L3 Analyst
DevOps Engineer
DevSecOps
External Attack Surface Control
Create Firewall Blocking Policy
Deploy to PROD

Figure 3-3 ORO Use-Case Scenario 2 DevSecOps Mitigation Approach

In this scenario, the L1 and L2 analysts will make use of the RIGOUROUS detection and mitigation capabilities, to validate the threat scenario associated with the Information Gathering Attempts of the external threat actors, and escalate to the L3 Analysts for in-life mitigation.

The L3 Analysts initiates the External Attack Surface Mitigation/Control processes, by isolating the root cause of the incident, enabling the DevOps Engineers to develop and implement a persistent fix (by deployment of a firewall policy restricting access to the exposed ports).

3.2.2.3. KPI and KVI

Table 3-2 The details of KPI and KVI

KPI	Description
KPI-23	Early-stage Security Threat Warning time optimization by at least 15 minutes for each detection compared to SoTA
KPI-20	Decrease mitigation reaction time by at least 30 minutes compared to SoTA.
KPI-30	Demonstration of the RIGOUROUS main innovations in the four key use cases using conditions based real operational environments.
KPI-5	Increased accuracy in orchestration.

3.2.2.4. Relevance to RIGOUROUS Objectives and Technical Tasks

Objective 4: **Advanced AI-driven Anomaly Detection, Risk Assessment and Mitigation Strategies** leveraging Anomaly Detection capabilities across ORO Network Layers, within a continuous risk assessment loop, enables an increase in response and mitigation capabilities against cyber threats.

Objective 5 - Demonstration of a Set of Industrially Relevant Use Cases in Operational Environments - This Scenario will demonstrate the capabilities of RIGOUROUS to support mitigation of information gathering malicious activities, to a telecommunications provider test-bed, replicating commercial-level services.

3.2.3. Threat Scenario 3

The third scenario refers to an Abnormal Traffic / Distributed Denial of Service attack targeting System Components. In this instance, a heavy-load DDoS attack takes place. The RIGOUROUS platform needs to detect the attack, isolate the impacted instances and transfer the traffic to unaffected instances.

3.2.3.1. Threat Scenario Description

In this scenario, a service exposed through an EDGE component of ORO 6G Facility is targeted and attacked with a heavy load of unsolicited traffic coming from distributed, heterogeneous sources (both IT and IoT Systems).

The likely threat actor is using a bot-net-as-a-service to target ORO's Facility internet-facing interfaces. The service that becomes unavailable to its intended consumers is a B2B Customer Web Portal, running on top of a web server hosted in ORO's Facility.

Although the application is decomposed and supported through micro-services, with fast replication capabilities and resilience-by-design deployment, the unwanted traffic is generated from a potent botnet and the attackers successfully target subsequent iterations of the service, on different EDGE interfaces.

3.2.3.2. Mitigation Approach and Relevant Tools

In the case of the Abnormal traffic load (DDoS) scenario, RIGOUROUS should have the ability to detect the ongoing attack and trigger a change, within the 5G Orchestrators in the ORO 5G Facility, to isolate the affected instances and immediately instantiate a migration of the VMs, hosting an instance of the components of the authentication services affected by the DDoS traffic, to a functional compute node, effectively improving the resilience of the 5G infrastructure by automated response orchestration and automated mitigation.

3.2.3.3. KPI and KVI

Table 3-3 The details of KPI and KVI

KPI	Description
KPI-19	Reduce the allowed malicious scale-up operations due to EDoS attacks to be < 5%

KPI-8	Number of AI Algorithms devised for 6G orchestration >3
KPI-9	Number of concurrent end-to-end slices supported >= 2048

3.2.3.4. Relevance to RIGOUROUS Objectives and Technical Tasks

Objective 3: Model-driven Automated Deployment & Security Orchestration at Operations by delivering automated response and recovery mechanisms, the application of this objective to UC#1 will enable the mitigation of impact and the assurance of resilience against DDoS Threats

Objective 5 - Demonstration of a Set of Industrially Relevant Use Cases in Operational Environments - This Scenario will demonstrate the capabilities of RIGOUROUS to support mitigation of Distributed Denial of Service Attacks, to a telecommunications provider test-bed, replicating commercial-level services.

3.2.4. Correlation to assets

For all threat scenario it is necessary to employ assets providing cognitive security, decision-making, orchestration, and management services, such as the AI-driven Decision Making and AI-Driven Algorithm for Risk Management and Mitigation provision in order to enable comprehensive cybersecurity threat assessment. The AI-driven Response Mitigation asset undergoes rigorous testing to ensure its effectiveness in countering potential threats. The process includes simulating cyber threat scenarios and evaluating its response capabilities. The risk management function will be deployed on a state-of-the-art 5G/IoT platform, ensuring seamless integration with the infrastructure.

In terms of orchestration and slice management, ORO will integrate the UMU Security Orchestration and use the AI Security Orchestrator to combine multiple models that could improve the overall robustness and decision making. In Scenario 3, the Orchestrator can be used to react against the DDoS attack by enforcing mitigation action to isolate the attacker and in scenario 2 of UC, the orchestrator can be used to enforce the slicing as mitigation mechanism. For the third threat scenario, where a DDoS is considered, ORO will integrate UWSs Slice Manager and Slice Control Agent in our current MANO capabilities, enabling fast slice control and replication of services to unaffected parts of ORO's testbed infrastructure.

For the information gathering threat scenario, UWS's Topology Inventory Agent will be integrated with ORO's testbed, to collect information on the Network devices, including virtual machines, containers, and physical nodes). The agent will then output updated information such as hardware and software properties and configurations, to various other consumers, including ORO's SoTA Monitoring and Detection stack (IDS/IPS, Firewalls, SIEMs, etc.).

By integrating UWS's Network Flow Monitoring and Network Self-Protection software assets, ORO aims to achieve enforcement of active security policies, and the mitigation of cyber attacks in the data plane components of the testbed Infrastructure, in all three threat scenarios. The Network flow monitoring asset will enhance ORO's SoTA IDS capabilities, and provide the RIGOUROUS framework of assets, with granular threat information in ORO's 5G/6G context.

UWS' Network Self-Healing software assets will enable ORO to orchestrate mitigation actions on intrusion detections, by integrating the asset in the management plane of ORO's testbed, with input data received from the Topology Inventory Agent and the Network Flow Monitor. This asset's integration will reinforce ORO's existing IDS/IPS mechanisms.

By integrating LNVO's Trust Evaluation and Trust Enabler Service Framework to ORO's testbed, the piloting of the three threat scenarios will be enhanced with continuous security and trust evaluation capabilities, with the assets acting as a detection mechanism for malicious behaviour of insider attackers, in our 6G facility, and as a mitigation mechanism against lateral movement of malicious actors. This functionality will be mapped to the outcomes of Scenario 1.

4 USE CASE II - IOT-BASED SMART CITY PLATFORM

4.1. Use Case's High Level Description

Emerging IoT platforms for smart city applications are built in a cloud native manner, and that is to leverage the potential of edge computing, and also to achieve scalability and cost-efficiency. The backend system of cloud-native IoT platforms may consist of docker-based micro-services, built modularly and orchestrated through tools such as Kubernetes. These micro-services could be deployed on a single edge cloud domain or multiple edge/cloud domains with different administrators. Communications among these micro-services could consequently occur within the same edge cloud domain or across multiple edge cloud domains. Furthermore, these micro-services could be sharing the resources of the same physical servers/infrastructure with the services of other tenants.

The IoT-based Smart City Platform (IoTSCP) combines video processing and virtual reality to facilitate the composition of Video on Demand (in a VR style). It processes videos from multiple cameras on the platform, enabling the display of different locations in a VR scene and dynamic switching between perspectives. The platform also includes privilege management, information security, and service middleware components (Figure 4-1). Users can participate in live VR broadcasts or access historical VR videos with an IoT-based smart city platform device. The IoTSCP platform's backend system consumes and exposes diverse IoT data generated by gateways or devices that may be spread across urban areas. These devices, stationed on static fixtures like light poles or placed on mobile objects such as vehicles, utilize a cellular technology, namely 4G/5G, or non-cellular options, such as WIFI. Gateways, varying in processing power from micro-computers like Raspberry PI to high-capacity GPUs like Jetson Xavier or TX2, can be equipped with various devices such as legacy and 360° cameras, sensors, and GPS devices. Remotely controlled by different entities, the platform aims to establish a microservice-based video service system supporting tasks such as receiving, uploading, managing, integrating, producing virtual reality, live and historical display, and sensor data processing (e.g., GPS, temperature, and humidity).

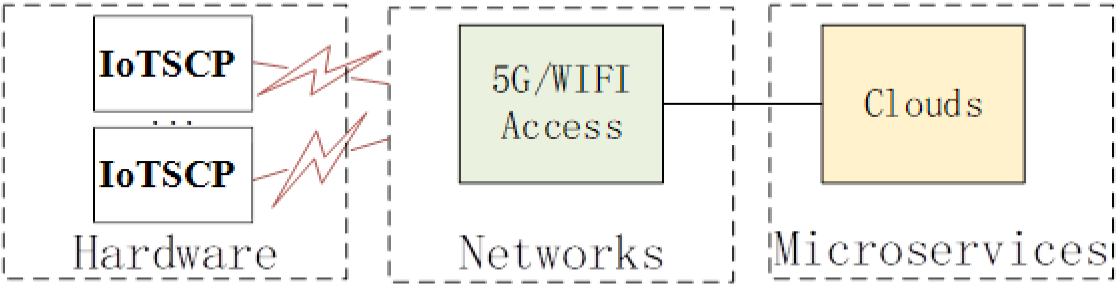

Figure 4-1 Basic framework of the envisioned IoTSCP platform.

The IoTSCP platform comprises two key components (Figure 4-2): hardware and microservices. The hardware, known as IoTSCP devices, is custom smart hardware fundamental to the platform's services. The cloud encompasses six microservices categories — video streaming, video on demand, web applications, messaging, authentication, and business logic. All microservices are configurable through Kubernetes (k8s), enabling web and mobile app development. Interfaces between IoTSCP and the cloud involve video streaming using RTMP/WebRTC protocols and non-video interactions via a self-defined MQTT protocol.

The IoTSCP platform utilizes custom protocols for encapsulating, decapsulating, and forwarding interprocess data, which are classified into five distinct categories: device status, alarms, camera configuration, switching, and sensor information. These messages enable the IoTSCP devices to communicate and exchange data with the cloud, facilitating various non-video interactions and functions. Pushing the converted and merged video stream to the designated server with the corresponding security code ID is known as "Push the stream to the clouds". The Video on Demand (VoD) service mainly processes historical videos from the IoTSCP platform, and it works similarly to platforms such as YouTube. When a user clicks on a GPS point on the map to play a historical video, the VoD service handles the appropriate starting point in the stored video and delivers the video for web broadcast. This service allows users to access and watch archived videos on demand, which enhances the user experience and provides access to historical content.

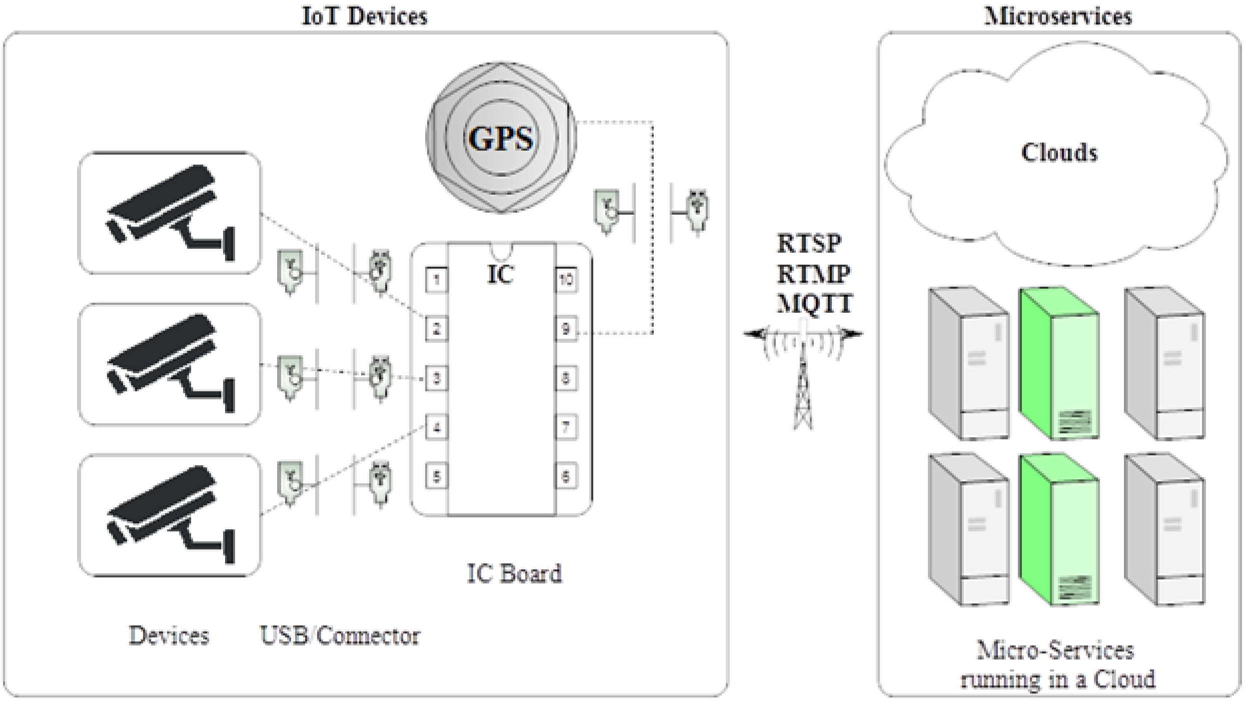

Figure 4-2 The different parts of the envisioned IoTSCP platform.

4.2. Security Threat Scenarios

4.2.1. Threat Scenario 1 - Unlawful access to IoT gateways, platform's APIs, and IoT data violating data privacy

4.2.1.1. Threat Scenario Description

Several potential threat scenarios need to be addressed in the context of smart city IoT platforms. These include unauthorized access to the IoT gateways and devices, unauthorized access to the APIs provided by the services of the IoT platform and its micro-services, and unauthorized access to the data generated by the IoT gateways and communicated to the backend system. It is critical to mitigate these threats to ensure the security and integrity of the IoT infrastructure.

4.2.1.2. Mitigation Approach and Relevant Tools

To ensure the security of platform APIs, it is crucial to follow the best security practices in service development. One tool that can be utilized for this purpose is ISTIO Security Services. Only authorized users and authorized (micro)services should have access to secure the remote access of IoT gateways, while the platform's backend system must restrict access to these gateways. This can be achieved by using different scalable and fast authentication mechanisms. To authorize an IoT gateway's access to the IoT service system, a legitimate user, typically the operator or owner of the gateway, can utilize relevant gateway data, such as the gateway's serial number, default authentication code, Universal Unique Identifier (UUID), and device model. These data must be pre-registered in the system's database before the IoT gateways are shipped to users. When a user wants to authenticate and activate an IoT gateway within the system, they must log into the system using their credentials, such as a user ID and password. After successful login, the user/owner of the IoT gateway must enter the gateway's serial number, model, and default authentication code into the system. The provided information is then verified against the data stored in the system's database. Once the verification process is successful, the IoT gateway becomes bound to the user, confirming that the user has the legal right to possess and operate the IoT gateway. The user may then have the option to change the authentication code.

Many IoT gateways/device manufacturers, such as Hikvision, widely employ these authentication procedures. Messaging protocols like MQTT can be used to exchange control messages between IoT gateways and the system backend. Robust security measures can ensure the safety of this exchange. One effective approach for securing control messages involves serializing the data format and using BASE64 encoding for encryption. To further enhance security, some of the data can be salted, subjected to MD5 encryption, and mixed with the original data. This combined data can then be subjected to MD5 encryption twice, using the same salted data. Multiple rounds of MD5 encryption significantly increase the complexity of the encrypted data, making it extremely difficult for unauthorized users to decrypt.

It is worth noting that many large internet companies currently use these encryption techniques to ensure strong security. Encryption and decryption mechanisms protect IoT data and prevent privacy violations. To support smart-city IoT platforms, it is important to have an Encryption as a Service (EaaS) platform that provides cryptographic services to IoT gateways, especially those with limited processing capabilities. The EaaS platform can also offer homomorphic encryption services, enabling the development of privacy-preserving AI/ML models to process encrypted data. The high-level architecture of the EaaS platform developed in RIGOUROUS (Refer to RIGOUROUS deliverable D4.1) is illustrated in Figure 4-3. The EaaS platform allows the autonomous creation and management of EaaS instances, each dedicated to providing encryption and decryption services for an IoT service provider.

Each EaaS instance comprises five key components: an encryptor, a decryptor, a request handler, a key manager, and a key generator. Utilizing the Encryption as a Service (EaaS) platform, UC2, as an IoT service provider, may enable the specification of encryption/decryption parameters through a user-friendly web interface. Users can define the preferred algorithm, provide specific details related to the chosen encryption/decryption method, determine the deployment location, specify the number of instances to activate, and set the duration for the encryption/decryption service [7].

This streamlined approach empowers users to tailor their security measures with precision and flexibility, supporting some of the DevSecOps features.

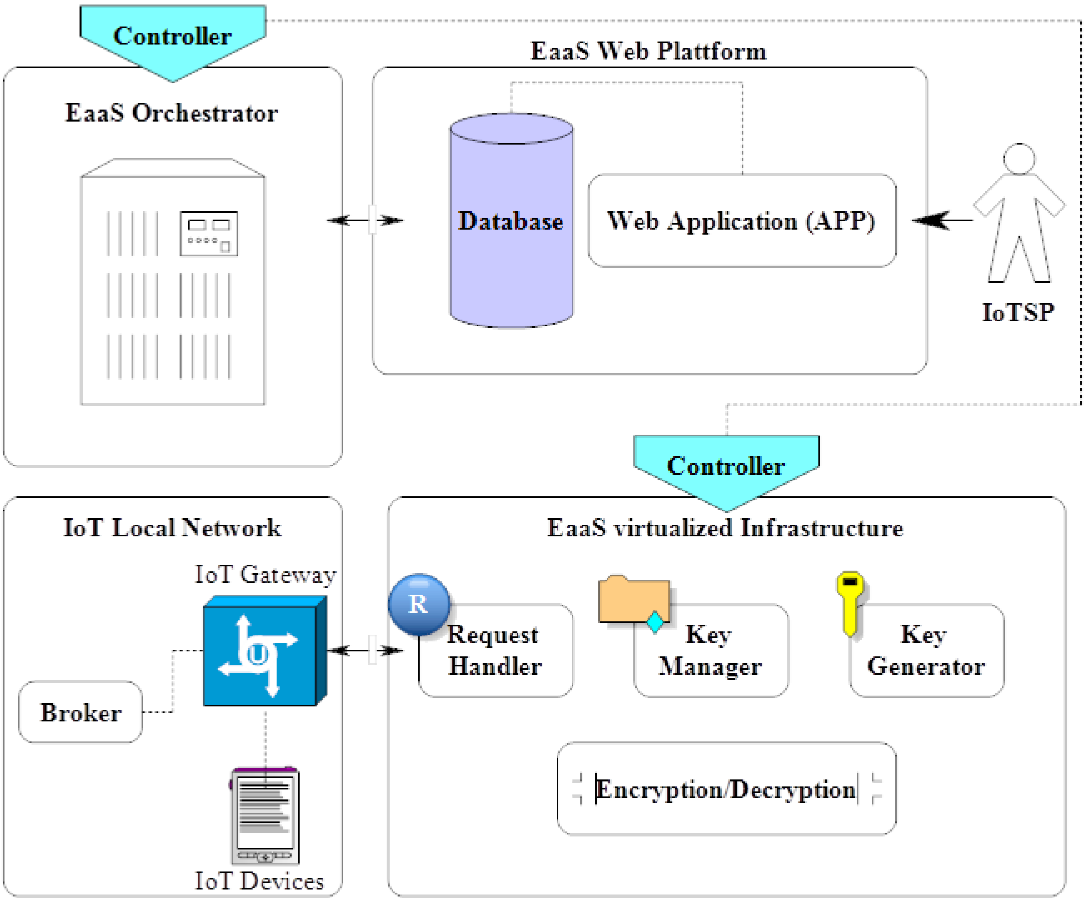

Figure 4-3 High level architecture of the EaaS platform.

4.2.1.3. KPI and KVI

The two key metrics relevant to Encryption as a Service are scalability and resource utilization, including CPU and RAM usage.

Table 4-1 key metrics relevant to Encryption as a Service are scalability and resource utilization

KPI	Description
Scalability of the system	System scalability is measured by the number of encryption requests processed per second. Scalability can be improved (i.e., by 7%) through virtualization, launching container-based encryptors/decryptors as per the underlying needs.
Key Generation Time	Key Generation Time is crucial for efficient encryption or decryption. This value can be improved (i.e., by 7%) through optimized load balancing of encryption/decryption requests among available container-based encryptors/decryptors.
CPU Usage and RAM Usage	Establishing benchmarks for CPU and RAM usage levels optimizes resource utilization for encryption and decryption instances. We intend to improve CPU and RAM usage by more than 10%.

Service Scalability Efficiency	Service Scalability Efficiency (SSE) is a KVI that measures the ratio of achieved scalability to the target scalability for encryption and decryption. A higher percentage indicates efficient scalability. We intend to improve SSE by 10%.
Resource Utilization Efficiency	Optimizing CPU and RAM usage for encryption/decryption instances to hopefully improve resource utilization efficiency by more than 10%.

4.2.1.4. Relevance to RIGOUROUS Objectives and Technical Tasks

Objective 1 - Holistic Smart Service framework for securing the IoT-Edge-Cloud continuum lifecycle management

To a certain extent, this use case relates to Objective 1, and that is as it targets securing the communication between the IoT gateways and the microservices of the platform's backend running at the edge or the cloud and securing data against privacy violations.

Objective 2 - Human-Centric DevSecOps

To a certain extent, this use case relates to Objective 2. Effectively, as part of the management of services and IoT devices, this use case aims to provide an operating Encryption/Decryption as a Service platform that can help in the privacy protection of IoT data, and contribute to the DevSecOps pipeline.

Objective 5 - Demonstration of a Set of Industrially Relevant Use Cases in Operational Environments

An operating Encryption/Decryption platform offered as a service to safeguard the IoT data privacy of smart cities will be demonstrated.

4.2.2. Threat Scenario 2 - Unauthorized communications to micro-services of an IoT smart city platform

4.2.2.1. Threat Scenario Description

Smart city IoT platforms are built using a cloud-native approach. This means they consist of micro-services that can be deployed and distributed across multiple cloud domains. In certain situations, it becomes necessary to establish secure communication between the micro-services that belong to the same service and are running within the same cloud or across different cloud domains. The risk of unauthorized communications among micro-services within cloud-native IoT platforms, particularly those that are distributed across multiple cloud domains, poses a significant threat to the security of smart city infrastructures. It is crucial to implement a secure integration fabric that involves utilizing a combination of service mesh solutions like Apache Kafka (event streaming platforms) to ensure secure communication.

4.2.2.2. Mitigation Approach and Relevant Tools

In cloud-native environments, micro-services need to communicate among themselves securely. A dedicated infrastructure layer called the secure integration fabric may be used to facilitate this. Service mesh solutions, such as ISTIO and Linkerd, may provide essential features such as service discovery, load balancing, and encryption to ensure secure communication between micro-services. They also enable the implementation of security policies and mutual TLS (mTLS) to authenticate communication between the micro-services. ISTIO and Linkerd have widely adopted service mesh solutions that play a key role in enforcing these security measures.

4.2.2.3. KPI and KVI

Some of the metrics are as follows:

Table 4-2 key role in enforcing these security measures

KPI/KVI	Description
Role of Service Mesh Metrics	Measure the accuracy and speed of service discovery within the mesh. Evaluate traffic balancing among micro-services to ensure optimal resource utilization. Assess the percentage of encrypted communications, indicating the security level provided by the service mesh. · Minimum Value: Service discovery should ideally occur within milliseconds, ensuring quick and efficient communication between microservices.
Role of Istio and Linkerd Metrics	Measure the extent to which mutual TLS (mTLS) is adopted for secure, authenticated communication. Assess adherence to security policies set by Istio or Linkerd for micro-service interactions. Quantify the improvement in communication latency achieved by Istio or Linkerd's features such as load balancing and routing. · Minimum Value: Aim for 70% adoption of mTLS for all microservices communication.

4.2.2.4. Relevance to RIGOUROUS Objectives and Technical Tasks

Objective 1 - Holistic Smart Service framework for securing the IoT-Edge-Cloud continuum lifecycle management

Towards securing the communication among the microservices running across multiple (edge) clouds, Objective 1 of the RIGOUROUS project aims to develop a comprehensive Smart Service framework for securing the IoT-Edge-Cloud continuum's entire lifecycle management.

Objective 3 - Model-based and AI-driven Automated Security Orchestration, Trust Management, and deployment

Secure communication among microservices requires integrating AI-driven techniques for security orchestration, trust management, and deployment, to move toward a dynamic and innovative approach. This approach ensures a secure and adaptable framework that meets the changing needs of users in real-time.

4.2.3. Threat Scenario 3 - Economical Denial of Service and Adversary AI attacks

4.2.3.1. Threat Scenario Description

The backend systems of various smart city IoT platforms may be deployed across multiple cloud domains, with virtual resources being shared with other tenants. In addition, artificial intelligence is used to automate the deployment and lifecycle management of multiple smart city IoT platforms, including micro-services initial placement, migration across edge/cloud nodes, and scaling cloud resources allocated for a given service. However, these AI techniques are vulnerable to attacks that could lead to economic denial of sustainability.

4.2.3.2. Mitigation Approach and Relevant Tools

It is important to investigate and develop solutions for potential malicious use of machine learning and artificial intelligence technology by adversaries. One example of this is the need for an AI-driven framework to detect and mitigate EDoS attacks. This framework could consider various solutions, such as moving affected micro-services to safer edge cloud nodes and rejecting the auto-scaling operation. It would also be useful to use MTD-based robust ML models to prevent adversarial attacks against ML models. Incorporating metrics relevant to the cloud infrastructure is a good idea to enhance the detection accuracy of the EDoS detection and mitigation framework. However, establishing an interface with the IoT service provider is advisable to make it even more effective. The framework can then inquire about any significant changes in the service consumption pattern [4].

For instance, when the EDoS mitigator needs to auto scale-up the operation, it can leverage the trained model and the collected infrastructure-related data to evaluate the operation's legitimacy. Before rejecting the operation, the EDoS mitigator can communicate with the relevant IoT service provider and inquire whether there have been any notable changes in the IoT service consumption.

These changes could manifest as increased activated IoT gateways, resulting in a higher generation of IoT data such as video streams. This would subsequently require additional cloud resources for processing. Alternatively, it could be an influx of users accessing the system and consuming IoT data. If the IoT service provider confirms such changes, the EDoS mitigator can reassess its decision and allow the necessary scaling up of resources. In case the IoT service provider refuses to accept any changes, the EDoS mitigator can reject the auto-scaling operation as it may be considered potentially malicious. By connecting with the IoT service provider and cross-checking the details, the EDoS detection and mitigation framework can improve its accuracy and make better decisions regarding resource scaling [5,6].

As part of its DevSecOps package, UC2 provides the functionality to activate or deactivate EDoS mitigation. This feature can be integrated into the user's workflow. When EDoS mitigation is enabled, users can further customize their settings, allowing them to determine whether the EDoS mitigator should consult the service provider before taking action on an autoscaling request. This user-centric approach ensures a fine-tuned and responsive EDoS mitigation strategy aligned with the specific needs of the IoT service provider. To ensure a personalized experience, users have the flexibility to define criteria for allowing or blocking autoscaling requests based on pertinent information, such as the current number of connected IoT devices or variations in device connections over specific time intervals (e.g., 1 minute, 5 minutes, 10 minutes). These configurations can be seamlessly managed through an intuitive web interface, enabling users to manage their EDoS mitigation strategy. The web interface provides a detailed view of the EDoS mitigation strategy, allowing users to monitor how their EDoS mitigation strategy is performing. This real-time monitoring enables users to make necessary adjustments to their configurations, ensuring that the EDoS mitigator is always working optimally. The details presented in Figure 4-4 provide an overview of the UC2 EDoS mitigation feature and its customizable configurations.

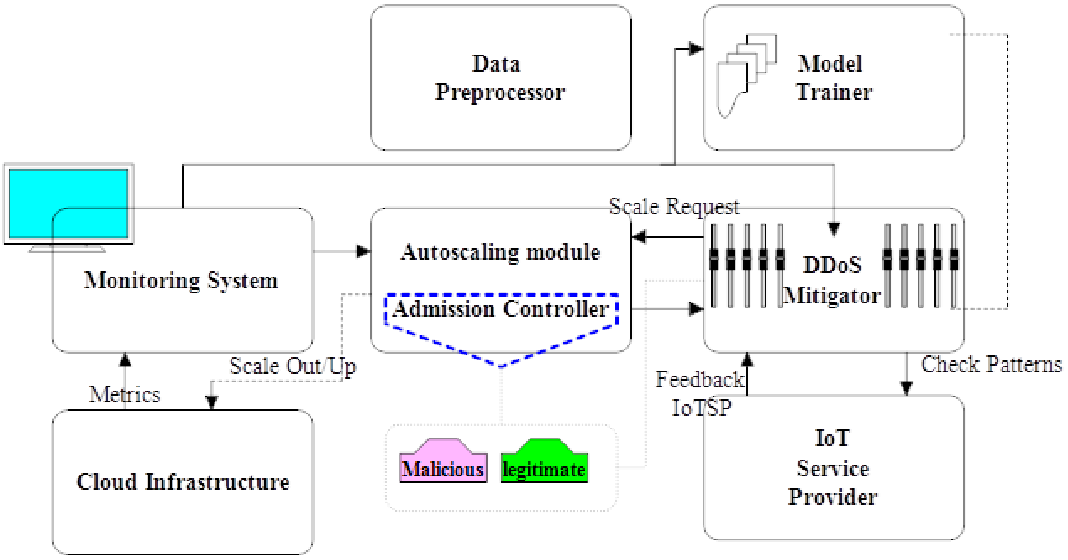

Figure 4-4 Enhancing the accuracy of the EDoS mitigator by inquiring about any change in the IoT service consumption pattern.

4.2.3.3. KPI and KVI

Some of the metrics relevant to the AI/ML algorithms are as follows:

Table 4-3 metrics relevant to the AI/ML

KPI	Description
Detection accuracy	This metric measures the number of accurately detected anomalies, such as EDoS attacks, by an ML model with centralized and federated learning. Our objective is to increase detection accuracy by 10%.
Mean time to detection	The time between the attack launch and its detection by the ML model. Our objective is to decrease this by 5%.
Mean time to mitigation	The time between the anomaly detection by the ML model and its mitigation. Our objective is to decrease this by 5%.
Blocked adversarial examples rate	The percentage of adversarial examples that the ML model can resist (when the MTD technique is applied) compared to the total number of adversarial examples generated by the attacker.
Training time	The time for collecting data, processing data, and building a suitable model. Our objective is to decrease this by 5%.

Computational/Communication Cost	The computation/communication cost for performing the data processing

4.2.3.4. Relevance to RIGOUROUS Objectives and Technical Tasks

This threat scenario pertains to all the project objectives. It defines the core threat scenario of this use case.:

Objective 1 Holistic Smart Service framework for securing the IoT-Edge-Cloud continuum lifecycle management
By protecting the underlying infrastructure from EDoS and associated adversary AIs, the whole IoT-Edge Cloud continuum lifecycle management can be protected.

Objective 2 Human-Centric DevSecOps
The settings of the adversary AI techniques as well as the enabling/disabling of EDoS mitigation, consultation of the IoT service provider, etc can be an integral part of the DevSecOps pipelines.

Objective 3 Model-based and AI-driven Automated Security Orchestration, Trust Management, and deployment
This use case targets securing the underlying infrastructure and the orchestration of its resources in an AI-driven fashion, coping also with the risks of adversary AIs. The EDoS mitigation is entirely AI-based.

Objective 4 Advanced AI-driven Anomaly Detection, decision, and Mitigation Strategies
This use case involves AI-driven anomaly detection and mitigation mechanisms, and that includes AI-powered EDoS mitigation and MTD-based Robust ML Models.

Objective 5 Demonstration of a Set of Industrially Relevant Use Cases in Operational Environments
The above-mentioned AI-powered EDoS mitigation and MTD-based Robust ML Models will be evaluated and demonstrated.

4.2.4. Correlation to assets

Use Case 2, focusing on the IoT-based Smart City Platform, features a multi-layer encryption scheme designed to ensure the confidentiality and integrity of sensitive data exchanged between the end-devices and the platform's backend system. To address data privacy concerns, proactive measures are to be leveraged to prevent and mitigate violations. Maintaining the security of the platform is paramount, necessitating the implementation of strict access controls and monitoring mechanisms to deter unauthorized access. To enhance data confidentiality and integrity in UC2, we can use Encryption as a Service (EaaS) and Privacy-preserving Federated AI and Holistic Security and Privacy Framework. EaaS encrypts sensitive data to protect it from unauthorized access while Federated AI and Holistic Security use advanced models for anomaly detection while preserving privacy.

Central to the RIGOUROUS system, the Security Analytics Engine and the Cognitive Decision, Orchestration, and Management plane are pivotal components responsible for enforcing security measures. Within them, AI-powered decision-making functional blocks detect and classify various threats, offering valuable insights into potential risks. This capability is particularly crucial in situations requiring meticulous information gathering and categorization. The AI-powered decision-making functional blocks may facilitate the deployment of critical elements, including Economical Denial of Service (EDoS) mitigators, serving as a proactive defence mechanism against disruptive EDoS attacks and safeguarding essential assets. The detection accuracy of the EDoS mitigator can be improved by leveraging components that can monitor changes in IoT service consumption patterns. In this use case, cybersecurity measures are fundamental to safeguarding sensitive data and establishing a smooth correlation with essential assets throughout the IoT service ecosystem.

5 Use Case III - Utilities Management and security

5.1. Use Case's High Level Description

As mobile network and cloud adoption gain momentum in the utilities sector, the utility manager needs to understand the security and compliance implications of network and cloud migration. Network and cloud services are often delivered over the public internet, which exposes it to several risks that need to be considered and requires necessary security controls to be put in place to protect their data and applications.

WINGS has developed and launched the ARTEMIS platform (Artificial Intelligence and IoT Powered Platform for the Proactive Management of Utilities) (Figure 5-1). ARTEMIS is an end-to-end solution, comprising the integration of a) Embedded intelligence - IoT infrastructure, Communication networks, b) cloud and big data platforms, c) Artificial Intelligence (AI), and d) Visualization, in one stop shop solution. Physical/IoT devices are connected to the ARTEMIS platform through the ARTEMIS Smart Gateway, which offers interfaces to meters and sensors and transmits data & measurements over any available network (4G/5G, NB-IoT, GPRS, LoRa), while enabling edge computing, e.g. identifying alerts at a local level and adapting measurement and transmission profiles accordingly (e.g., more frequent measurements /transmissions in case of alerts - push notifications), and remote management capabilities.

In terms of domains, the specific use case considers either the diverse applications and systems that the utilities have or the different subsystems that exist in the same application and system (e.g. IoT devices, gateways, edge, cloud, and the networks among the previous parts). This is illustrated in Figure 5-2.

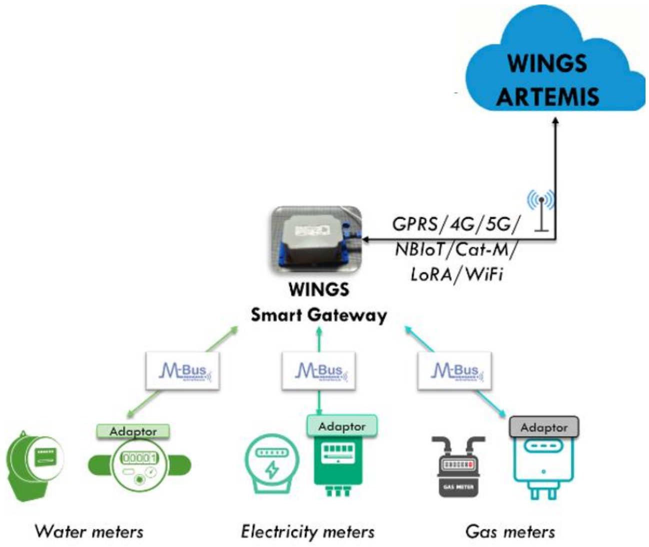

Figure 5-1 Utilities Management and security Use Case Overview

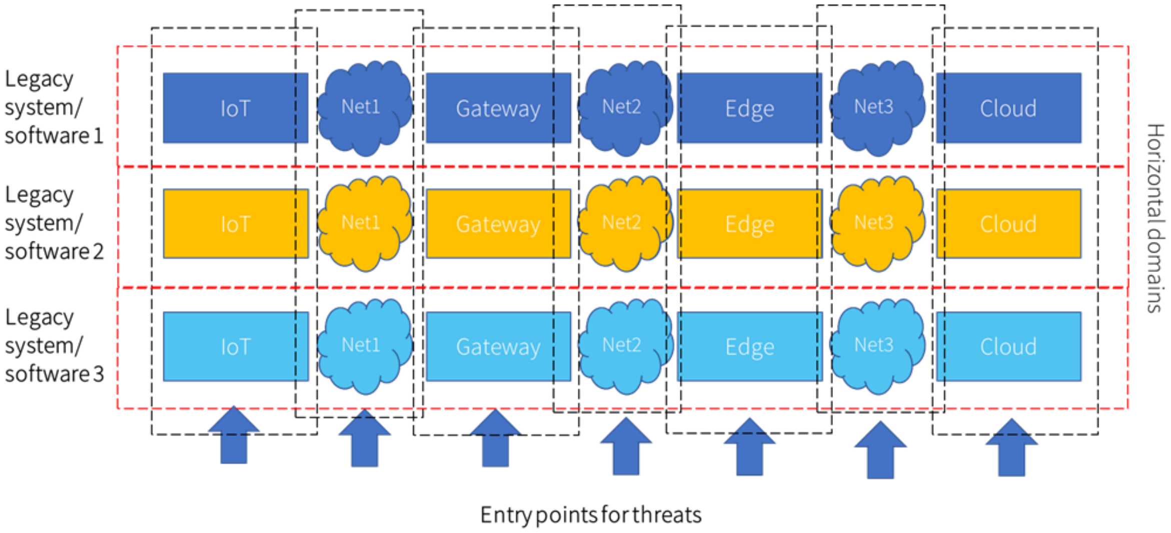
Legacy system/ software 1
Legacy system/ software 2
Legacy system/ software 3
IoT
Net1
Gateway
Net2
Edge
Net3
Cloud
Horizontal domains
Entry points for threats

Figure 5-2 Different subsystems that exist in the same application and system

5.2. Security Threat Scenarios

5.2.1. Data Security - Unauthorized access

The energy and utilities sector deals with a large amount of sensitive data, such as customer information and confidential business data. Hence, it is essential that this data is protected from unauthorized access, and is only accessible to authorized personnel as data breaches are a serious concern for organizations in this sector and can have a major impact on their business.

5.2.1.1. Threat Scenario Description

One of the main problems encountered is that several domains multiply the entry points for unauthorized access. As aforementioned, domains can be either the diverse applications and systems that the utilities have or the different subsystems that exist in the same application and system (e.g. IoT devices, gateways, edge, cloud, and the networks among the previous parts). By gaining access to one of these domains, the attackers can use privilege escalation to expand their reach. Horizontal privilege escalation involves attackers gaining access to additional, adjacent systems, and vertical escalation means attackers gain a higher level of privileges for the same systems.

5.2.1.2. Mitigation Approach and Relevant Tools

In order to protect data, organizations need to implement security measures, such as intrusion detection and prevention mechanisms. These mechanisms should be anomaly-based which means that they do not follow hard coded rules since this generality makes it extremely hard for intruders to avoid. Cyber-Physical Correlator will be able to detect intrusion detections by analyzing the network traffic flow and will inform the user in the event of an attack, enabling him to protect the organization's data.

5.2.1.3. KPI and KVI

Table 5-1 Classification metrics and Security measures

KPI/KVI	Description
Classification metrics	The metrics that show how accurately the algorithm detect the physical intrusion of an unauthorised person in the infrastructure or a cyber intrusion in the network. the accuracy should be > 90%
Training time	The time that is required for the algorithm to be trained on the training set should be less than 1 hour
Interface	Check if interface is compatible with existing interfaces/systems (Yes/No)

5.2.1.4. Relevance to RIGOUROUS Objectives and Technical Tasks

Objective 4: Advanced AI-driven Anomaly Detection, decision, and Mitigation Strategies

Cyber-Physical Correlator will be enhanced to detect attacks based on the network traffic flow. In that way, it can notify the user of potential cyber attacks. This scenario serves as a demonstrator for some of the key results of the project, and work being developed in the multiple tasks of WP4, which are detailed next, highlighting their relevance for this specific scenario.

- R18: Cyber Physical Correlator (T4.3)

5.2.2. Distributed Denial of Service (DDoS) attacks

Attackers build botnets, large fleets of compromised devices, and use them to direct false traffic at your network or servers. DDoS can occur at the network level, for example by sending huge volumes of packets which can overwhelm a network or a server, or at the application level, for example by performing complex queries that bring a database to its limits.

5.2.2.1. Threat Scenario Description

One of the main problems encountered is again that several domains multiply the entry points for Distributed Denial of Service (DDoS) attacks. As aforementioned, domains can be either the diverse applications and systems that the utilities have or the different subsystems that exist in the same application and system (e.g. IoT devices, gateways, edge, cloud, and the networks among the previous parts). By attacking one of these domains, the attackers can block the whole application and system.

5.2.2.2. Mitigation Approach and Relevant Tools

A first mitigation approach is to monitor the network traffic, in order to ensure that we have a complete visibility of incoming, outgoing, and internal network traffic, with the ability to automatically detect threats, and understand their context and impact. We should monitor and combine data from all different domains to get a clear picture of what is happening on the network, recognizing that many attacks span multiple IT systems, user accounts and threat vectors in all these domains.

One potential solution for avoiding DDoS attacks is dividing a network into zones based on security requirements. This can be done using sub-slices within the same network, each of which behaves like a complete separate network. This segmentation limits the potential impact of an attack to one zone, while we can mitigate the specific zone by assigning a minimum throughput. Cyber Physical

Correlator will be able to detect DDoS attacks by analyzing the traffic flow of the network. Additionally, it could propose the appropriate mitigation actions to protect the infrastructure from the attack.

5.2.2.3. KPI and KVI

Table 5-2 The details of Classification metrics (Accuracy, Precision, Recall, F1 score)

KPI/KVI	Description
Classification metrics	The metrics show how accurately the algorithm detects the anomaly in the traffic flow as well as the specific type of attack. the accuracy of the attack detection should be > 90%
Time required for detection	The time that is required for the algorithm to detect the attack should be less than 1 second
Training time	The time that is required for the algorithm to be trained on the training set should be less than 1 hour

5.2.2.4. Relevance to RIGOUROUS Objectives and Technical Tasks

Objective 4: Advanced AI-driven Anomaly Detection, decision, and Mitigation Strategies

- Cyber-Physical Correlator will be enhanced to detect attacks based on the network traffic flow. In that way it can notify the user for potential cyber attacks like DDoS and ensure the smooth operation of the platform and the devices connected to it. This scenario serves as a demonstrator for some of the key results of the project, and work being developed in the multiple tasks of WP3 and WP4, which are detailed next, highlighting their relevance for this specific scenario:
- R7: Multi-domain AI-driven Orchestrator (T3.2)
- R18: Cyber Physical Correlator (T4.3)

5.2.3. Code and data injection attacks

Several applications may be attacked to accept malicious user inputs and fail to validate and sanitize those inputs. Attackers can then fill out a form or make an API call, passing malicious code or data instead of the expected data values. The code is executed on the server and allows attackers to compromise it.

5.2.3.1. Threat Scenario Description

Again, the complexity raises a lot, since there can be different domains that multiply the entry points for the code and data injection attacks. As aforementioned, domains can be either the diverse applications and systems that the utilities have or the different subsystems that exist in the same application and system (e.g. IoT devices, gateways, edge, cloud, and the networks among the previous parts). By attacking one of these domains, and especially the IoT devices or the gateways, the attackers can escalate their attacks and propagate the erroneous data to additional, adjacent systems and applications, or at a higher level of privileges for the same systems (e.g. to the edge and the cloud).

5.2.3.2. Mitigation Approach and Relevant Tools

Here, we need tools that analyze the data in each domain and understand the quality, relevance, and validity of the specific data. Predictive analytics can be used to derive the anticipated data and then compare it with the data in the network. If we see that the available network data are far different from the expected ones, data quality management techniques can be used to replace the false data with estimated values based on the built patterns. Cyber Physical Correlator will be able to detect injection attacks by analyzing the network traffic flow. Additionally, the tool will be able to detect anomalies in time series and understand when these anomalies are due to a false data injection attack.

5.2.3.3. KPI and KVI

Table 5-3 The details of Classification metrics (Accuracy, Precision, Recall, F1 score)

KPI/KVI	Description
Classification metrics	The metrics that shows how accurately the algorithm detects the falsified data. The accuracy should be > 90%
Escalation	The model should be able to detect attacks that come from 15 or more IPs in less than a second

5.2.3.4. Relevance to RIGOUROUS Objectives and Technical Tasks

Objective 1 Holistic Smart Service framework for securing the IoT-Edge-Cloud continuum lifecycle management

Cyber-Physical Correlator, as part of the ARTEMIS platform, can provide protection to the platform as well as to all connected IoT devices.

Objective 2 Human-Centric DevSecOps

Cyber Physical Correlator can generate security policies and on boarding specifications for enforcing the required security trust and privacy properties during the entire lifecycle, at design state and during operation, and to be enforced in both IoT-edge-Core-Cloud continuum and vertical layer.

Objective 4: Advanced AI-driven Anomaly Detection, decision, and Mitigation Strategies

Cyber-Physical Correlator can detect false data injection attacks following the traffic flow of the network. In case of an attack, it immediately notifies the user. Additionally, Correlator is able to detect changes in patterns of time series. So, it can inform the user of potential anomalous values transmitted by the devices and correlate the anomalies id data with anomalies in the traffic flow to increase the accuracy of the detections.

This scenario serves as a demonstrator for some of the key results of the project, and work being developed in the multiple tasks of WP4, which are detailed next, highlighting their relevance for this specific scenario:

- R18: Cyber Physical Correlator (T4.3)

5.2.4. Outdated systems

One of the key challenges facing organizations in the utility sector is that many legacy systems were not designed with interoperability and security in mind. Legacy systems often use proprietary protocols and standards that are not compatible with modern security tools and technologies. This makes it difficult to implement or deploy effective security controls/solutions in a mobile network and cloud environment.

5.2.4.1. Threat Scenario Description

Again, the complexity raises a lot, since there can be different domains that multiply the number of systems that are not able to interoperate. As aforementioned, domains can be the diverse applications and systems that the utilities have and they can not interoperate among them, or between them and the security tools. Alternatively, the domains can be the different subsystems that exist in the same application and system (e.g. IoT devices, gateways, edge, cloud, and the networks among the previous parts). Any failure in the compatibility and interoperability among systems and their domains and the security tools, it can create problems in the end-to-end operation of the systems and the associated applications.

5.2.4.2. Mitigation Approach and Relevant Tools

Here, we need dynamic and automated service composition mechanisms, in order to detect and resolve the interconnection problems among components that are attempting to interoperate, and one (or more) of them is outdated. This interconnection problem should be resolved without bringing down the whole system or the individual components. The components should be able to gracefully suspend operations (without requiring a full fault-tolerance design of the component).

5.2.4.3. KPI and KVI

Table 5-4 The details of 5.2.4.3. KPI and KVI

KPI/KVI	Description
No need for human intervention	The mechanism should be able to operate without human intervention.
Compatibility	The extent to which the security mechanism is compatible with legacy systems (percentage). the compatibility should be > 90%
Detection ability	The number of different issues detected or resolved should be > 5.
Availability of the system	The system should be down for less than 10 minutes.

5.2.4.4. Relevance to RIGOUROUS Objectives and Technical Tasks

Objective 2 Human-Centric DevSecOps

Dynamic Automated service Composition which will be integrated with ARTEMIS generates recommendations for interoperability issues between the different components so that they can be fixed before security gaps are created.

Objective 3: Model-based and AI-driven Automated Security Orchestration, Trust Management, and deployment

Dynamic Automated Service Composition can deliver self-recovery mechanisms for both infrastructures and services, to dynamically mitigate the impact of cyber incidents, according to the context and the assessment provided by components endowed with AI-based security analytics.

This scenario serves as a demonstrator for some of the key results of the project, and work being developed in the multiple tasks of WP3/WP4, which are detailed next, highlighting their relevance for this specific scenario:

- R2: Security and Privacy formal data models for 6G networks (T3.1)
- R15: Dynamic and Automated Service Composition technologies: Digital Twin, Run time Monitoring, Self-learning/healing AI algorithms. (T4.2)

5.2.5. Correlation to assets

In order to detect various types of attacks, three different scenarios - scenarios 1, 2, and 3 - have been developed. Scenario 1 focuses on detecting unauthorized access, scenario 2 deals with identifying DDoS attacks, while scenario 3 addresses false data injection attacks. All these attacks can be detected by using the Cyber Physical Correlator, which analyzes the network data flow and data from sensors installed in the field, and notifies the operator when it detects any abnormal activity. Additionally, it communicates with AI-driven Decision to proceed with further analysis and to propose specific mitigation actions. For the anomaly detection, Privacy-preserving Federated AI for anomaly detection can also be used.

In terms of decentralized computation, Decentralized services based Identity and Trust management specification will be applied to the three scenarios. Additionally, Trust evaluation and Trust enabler service framework specification can be used to achieve high level of trust evaluation capabilities. To address the challenges of bootstrapping a device, IoT bootstrapping specifications should be considered. Moreover, Intent-based Security & Privacy formal modelling and onboarding specification can provide solutions to address privacy issues, along with Human-centric Privacy risk management for DevSecOps. Finally, a threat risk assessor could help in calculating the risk levels of the infrastructure.

Scenario 4 aims to identify mismatches between different protocols used by a legacy system. To achieve this, dynamic automated service composition can be used to identify interoperability issues between different components. It then proposes fixes that make the system compatible with modern security tools. Digital Twin will be used to simulate the different components of a system, one (or more) of which will be outdated.

6 USE CASE IV

6.1. Use Case‘s High Level Description

The increasing significance of Information and Communications Technology (ICT) is evident in its role in coordinating and planning Public Protection and Disaster Relief (PPDR) scenarios. These scenarios entail real-time coordination between field teams and Command-and-Control Centre (CCC) operators, particularly in challenging environments. The advent of 5G and subsequent technology generations has paved the way for Augmented Reality (AR) and Virtual Reality (VR) applications to enhance PPDR, improving the Quality of Experience (QoE). To address these needs, OneSource has developed Mobitrust, an IoT-driven situational awareness platform for PPDR. Mobitrust capitalizes on edge/cloud computing paradigms to facilitate efficient monitoring, aggregation, and analysis of PPDR data from diverse sources like positioning devices, field stations, vehicles, and wearable sensors worn by field operators.

Mobitrust not only empowers real-time communication between CCC operators and field personnel through text, audio, and video but also incorporates AI/ML algorithms strategically positioned along the edge/cloud continuum. This transforms Mobitrust into an intelligent platform capable of processing data and videos to enhance PPDR mission performance. This intelligence proves vital in detecting critical situations such as man-down incidents, environmental hazards, and physical threats, benefiting both field operators and decision-makers in the control center. Mobitrust also explores the potential of AR/VR technologies within PPDR scenarios, offering improved field views through AR Head-Mounted Displays (HMDs) and more intuitive interactions via VR HMDs.

Security remains a central concern in PPDR scenarios, demanding a comprehensive protection across devices, microservices, components, and network communications. OneSource's project delves into mechanisms for authentication, authorization, and differentiated access, while also focusing on secure lifecycle management. The project aims to ensure the platform's secure behavior, detect anomalies, and facilitate remote and secure updates. In essence, Mobitrust stands as a pioneering solution at the intersection of technology, disaster response, and security, poised to reshape and enhance the efficiency of PPDR operations.

6.2. Security Threat Scenarios

6.2.1. PPDR scene and teams provisioning

6.2.1.1. Threat Scenario Description

Whenever a new operation begins, and throughout its course, many different teams and elements will arrive and join the operation, from field operatives to on-premises control operations. This means multiple devices being connected to the infrastructure that need secure authentication and authorization to access not only the services but also the network itself. As such, one possible threat is for unwanted devices to try to authenticate against the network and get access to the services deployed, which would have implications in terms of privacy as well as security and trust. Moreover, it could also be the case where in some situations, there would be a need for teams the use personal devices, usually referred to as Bring Your Own Device (BYOD). This increases the need for security analysis, since at the start, these devices are deemed insecure until an analysis is made. Because

PPDR events are usually isolated and occur occasionally, the Mobitrust platform might be deployed on demand, whenever it is needed at a given location. For this, a cloud/infrastructure manager will trigger the deployment of the platform, letting the orchestrator take control and manage it.

6.2.1.2. Mitigation Approach and Relevant Tools

The secure deployment of the Mobitrust platform, together with the network isolation on all communications, from the end-devices to the cloud, through slicing, will allow decreasing the chances of any device intrusion, going from the device registration in the network and slice access to continuous monitoring of the deployed services, doing any necessary life-cycle adjustments. For this management, the *Multi-Domain AI-driven Orchestrator* will be the key component, which will take control from the beginning of the deployment of the framework, throughout the course of the operation, and ending with a controlled wrap-up of the scenario, taking any necessary actions for removing the deployment when it is no longer needed.

During the life-cycle of the provisioning operations, in case of rogue devices being detected or failures in the bootstrapping of certain devices, alerts will be generated by the RIGOUROUS assets, being analysed by a cloud analyst and/or a platform analyst, but also processed automatically by the RIGOUROUS SOAR and acted upon following the Zero Touch Paradigm.

6.2.1.3. KPI and KVI

The list of relevant KPIs to be measured linked with this scenario are presented in Table 6-1.

Table 6-1 List of relevant KPIs to be measured

Name	Measurement	Measure
Framework Deployment	Measure the time taken from the first instruction to deploy the framework until all the services are up and running on the edge/cloud.	<1s
End-to-end slicing	Measure the time taken for the configuration of the new slice across the different network segments.	<1s
BYOD trust analysis	Measure the time taken to analyse the device and deem it secure/insecure to be used in the operation.	<1s
Device bootstrapping	Measure the time taken for the bootstrapping of the end-devices with all needed configurations.	<1s
KPI-11	OPEX reduction in detection, decision, and mitigation	-15%
KPI-5	Increased accuracy in orchestration	+10%

The list of KVIs linked to this scenario and identified in Table 6-2.

Table 6-2 KPIs for the "PPDR scene and teams provisioning" scenario

Name	Explanation
Zero-touch configuration	Having the configuration/reconfiguration of the end-devices automated, takes a big burden from the support/management teams, while lowering the chances of applying bad configurations and disrupting the operation in course.
Trusted deployment	Due to the sensitivity of the information captured and transmitted, security is a key point. By having guarantees that all network elements that support the

	deployment are trusted and secured, the overall trustworthiness of the framework is increased.
Secure and prioritized communications	End-to-end slicing has an impact in two distinct ways. For one hand, with traffic isolation enhances the security of communications, reducing the means of intrusion. On the other hand, it elevates the QoS capabilities from the transport layer to the entire network, ensuring a more reliable and performant communication across the IoT-edge-cloud continuum.

6.2.1.4. Relevance to RIGOUROUS Objectives and Technical Tasks

This scenario serves as a demonstrator for some of the key results of the project, and work being developed in the multiple tasks of WP3, which are detailed next, highlighting their relevance for these specific objectives:

Objective 3 - Model-based and AI-driven Automated Security Orchestration, Trust Management, and deployment

- R7- Multi-Domain AI-driven Orchestrator: The deployment and maintenance of the framework will be managed by the Orchestrator, which will be the central control point, integrating with the different tools and technologies of the project.
- R8- Trust evaluation and Trust enabler service framework for the B5G and 6G system: The security and trustworthiness of the nodes and network components are a key aspect to ensure the overall security of the framework deployment.
- R9- IoT bootstrapping mechanisms and R10- Trusted application onboarding: The deployment of the framework, also considers the bootstrapping of the end-devices, which is aimed to follow a zero-touch approach for the entire setup and configuration.
- R11- Security Agents and Security Slice Controllers for End-to-end multi-domain slicing: In order to have control over the network and isolation of the traffic for this application, network slicing will be a key element in achieving and maintaining it.

Objective 4 - Advanced AI-driven Anomaly Detection, decision, and Mitigation Strategies

- Encryption as a Service: The use of the EaaS will allow the further increase of security and privacy when dealing with delicate data exchanged throughout the cloud continuum.

6.2.2. Intrusion into system to access privileged information or cause disruption of services

6.2.2.1. Threat Scenario Description

While the systems are deployed, an intrusion may be detected in the network, coming from anywhere in the infrastructure. This intrusion may have multiple purposes, from eavesdropping and trying to acquire sensitive information about ongoing/past operations, to causing harm, by making changes to the data and/or manipulating actions under execution.

6.2.2.2. Mitigation Approach and Relevant Tools

In order to improve the security of the deployed services and minimize/stop any attack being made, continuous monitoring will be a key feature, using AI-based mechanisms for the detection and mitigation of the ongoing attacks. Anomaly detection may have a key impact on improving the detection of unknown attacks, allowing to take any needed measures. Moreover, defence mechanisms, such as, MTD, can also take a key role in increasing the security of the deployed services.

The detection of such intrusions or anomalies by the RIGOUROUS functional components will trigger its SOAR to act accordingly, while the alerts coming from those assets can also be inspected by the infrastructure analysts, which may decide to later on take different measures or not. This post-incident analysis can also loop back into the AI-driven decision mechanisms to further enhance the analysis and decision-making processes.

6.2.2.3. KPI and KVI

The list of relevant KPIs to be measured linked with this scenario is presented in Table 6-3.

Table 6-3 KPIs for the "intrusion into system to access privileged information or cause disruption of services" scenario

Name	Measurement	Measure
Mitigation time	Measure the time taken to deploy measures to mitigate the attack under course.	<1s
KPI-14	Time to detection to reach real-time detection of order of milliseconds.	<1s
KPI-6	AI-powered Orchestration of four (04) kinds of resources, namely: services, devices, virtual network functions, and physical network functions.	4 Resources
KPI-30	Demonstration of the RIGOUROUS main innovations in the use cases using conditions based real operational environments.	4 Use Cases
KPI-13	Increase of accuracy in anomaly detection.	>95%

The list of KVIs linked to this scenario and identified in Table 6-4.

Table 6-4 KVIs for the "intrusion into system to access privileged information or cause disruption of services" scenario

Name	Explanation
Secured platform	The security measures taken from the beginning increase the overall base security, reducing the chances for possible attacks or manipulations of the framework. This then guarantees smoother management of the operations, increasing the potential success of the actions being taken.
Decreased interferences and downtime	Despite the increased based security, some attacks or interferences might still occur. Decreasing the time taken to detect and mitigate those cases can lead to less impact on the ongoing actions, preventing possible riskier scenarios due to system unavailability.

6.2.2.4. Relevance to RIGOUROUS Objectives and Technical Tasks

This scenario aligns with some of the relevant outcomes of the project, serving as a demonstrator for some of the work being done in WP4. The relevant project results that can be demonstrated and evaluated in this scenario are:

Objective 3 - Model-based and AI-driven Automated Security Orchestration, Trust Management, and deployment

- R11- Security Agents and Security Slice Controllers for End-to-end multi-domain slicing: In order to properly handle
- disruption of services and isolation of the application ends comes as a relevant factor for security improvement.

Objective 4 - Advanced AI-driven Anomaly Detection, decision, and Mitigation Strategies

- R12- Privacy-preserving FL-based Anomaly Detector: Continuous monitoring for potential attacks and anomalies increases the response time for mitigation actions and recovery actions.
- R14- MTD-based Robust ML Models: Enhancing security from the get-go reduces the chances of attack, resulting in an increased base level of security.
- R16- AI-driven decision making: The alerts coming from the anomaly detection functional blocks, together with other relevant data will be used to make the decisions on the mitigation actions to apply to each detection.
- R19- Threat Risk Assessment Tool: Identifying threats through the anomaly detection functional blocks and vulnerabilities in a system and making informed decisions about risk allows for an assessment and prioritization of risks based on their likelihood and potential impact.

6.2.3. Disclosure of device vulnerability or unlawful appropriation of a device

6.2.3.1. Threat Scenario Description

Throughout the course of an ongoing operation, it could be disclosed that one or more equipment have disclosed vulnerabilities identified. Moreover, it could also happen that a device is lost or stolen amidst the stress of the operation. As such, appropriate measures must be taken to address both these scenarios.

6.2.3.2. Mitigation Approach and Relevant Tools

Since the devices used in these scenarios have access to restricted networks and information, having any sort of vulnerability detected or unlawful usage poses high security threats. As such, dealing with these cases is of paramount importance. Whenever either of these cases occurs, the steps to take is to erase all information from the devices, followed by the necessary steps to unauthorize the device in the network, so that it can no longer connect to any of the secure channels.

Similarly to the above scenarios, the detection of such cases should be swiftly acted upon by the RIGOUROUS SOAR, while also generating the necessary alerts which will allow the analysts to do a proper inspection of the issues and take extra/different measures if deemed necessary.

6.2.3.3. KPI and KVI

The list of relevant KPIs to be measured linked with this scenario is presented in Table 6-5.

Table 6-5 KPIs for the "disclosure of device vulnerability or unlawful appropriation of a device" scenario

Name	Measurement	Measure
Device data deletion	Time taken to delete all critical data of the device.	<10s
Authorization revocation	Time is taken to unauthorize the device and for it to be de-registered from the network**.**	<10s
KPI-14	Time to detection to reach real-time detection of order of milliseconds.	<1s
KPI-12	Reduction of false alarms.	-30%

The list of KVIs linked to this scenario and identified in Table 6-6.

Table 6-6 KVIs for the "disclosure of device vulnerability or unlawful appropriation of a device" scenario

Name	Explanation
Vulnerability exposure	In situations that deal with a lot of sensitive information, there are many cases of exploration of vulnerabilities when trying to access said information. As such, mitigating those vulnerabilities as soon as they are detected reduces the chances of their unlawful exploration and access to privileged data.
Lost/Stolen devices	Since the devices used are registered to secure channels and have special accesses and permissions, having one of these lost or stolen can greatly compromise the security of the entire network. As such, being proficient on dealing with these scenarios will reduce the amount of time where the scenario security is compromised.

6.2.3.4. Relevance to RIGOUROUS Objectives and Technical Tasks

This scenario aligns with some of the relevant outcomes of the project, serving as a demonstrator for some of the work being done in WP3 and WP4. The relevant project results that can be demonstrated and evaluated in this scenario are:

Objective 2 - Human-Centric DevSecOps

- R3- Human-centric user-friendly tools for DevSecOps and risk management: With devices that have a user-friendly interface we bring a more likely adoption by teams leading to better engagement with security practices throughout development and operation cycles.
- R5- User controlled verifiable secure digital identification service: With information of devices being restricted, networks and information should be identifiable and registered in a way that devices can't be replicated for malicious purposes.

Objective 4 - Advanced AI-driven Anomaly Detection, decision, and Mitigation Strategies

- R19- Threat Risk Assessment Tool: With heterogeneous device requirements in technical environments there is a need for appropriate measures to be taken in place to protect the confidentiality, integrity and availability of private information.

6.2.4. Correlation to assets

In Scenario 2, the Privacy-preserving Federated AI for Anomaly Detection asset (UMU) can be integrated for real-time monitoring, anomaly detection, and attack classification so that mitigation agents, such as the AI-driven Decision Engine, can receive the alerts with the necessary information to come up with the optimal set of countermeasures to mitigate the attacks. Several FL Agents, as well as FL Aggregators, can be deployed in the infrastructure as Security Agents, so they can collect traffic flow features and train a detection model (Deep Autoencoder) able to discern between non-anomalous and anomalous/attack flow samples, which will be later classified as known attack types or, if not possible, as a potential zero-day/unknown attack. For validation, a set of attack scripts (both for user-plane and control-plane attacks) can be executed, data can be collected and, after Federated Learning is performed, the final model can be used for real-time attack detection and alerting.

On the other hand, the Privacy-preserving Cyber Threat Information Sharing asset (UMU) could be integrated both in Scenario 2 and 3. For instance, in Scenario 2, Indicators of Compromise (IoCs) about identified intrusions/attacks after detection is performed, could be shared with other domains, and some information such as the attacker and victim IPs are considered sensitive so they have to be protected before sharing. In Scenario 3, information about vulnerabilities discovered in devices/services in the infrastructure could also be shared with the corresponding sensitive data protection in case it is necessary.

Scenario 2 and Scenario 3 both present opportunities for incorporating the Holistic Security and Privacy Framework (ONE) as an effective solution for real-time monitoring and reporting anomalies. The Continual Learning Convolutional and Conventional Autoencoder model of HSPF, complemented by Privacy Enhancing Techniques like Zero-Knowledge Proof and Differential Privacy, ensures that transmitted information between components remains secure. The versatility of HSPF allows seamless integration into various equipment, providing a valuable defence against potential attacks on remote devices in Scenario 3, and facilitating the detection of intrusions in deployed communication services in Scenario 2.

Encryption as a Service (ICTFI) benefits Scenario 1 and 3, as it introduces a solution for delivering secure and efficient encryption of data for protection of the IoT Gateways and Devices involved in the ongoing operations, improving the security of all the involved elements.

The AI-powered decision-making functional blocks through AI-powered EDoS Mitigator (OULU) can benefit across all Scenarios as it introduces a method for dealing with malicious resource scaling requests which can interfere with the normal device operational behaviour as well as component communications.

Dynamic automated service composition is a service that can detect and resolve the interconnection problems among components that are attempting to interoperate. The interconnection problems may be due to different communication protocols that are used by the different components, encoding mismatches, notation mismatches, mismatches in units, etc. When a mismatch is detected, Dynamic automated service composition suggests some conversions to overcome the issue. Recommendations may involve changes to the source code or changes in the container. Additionally, an ontology can be used for mismatch identification. Finally, the service can use machine learning algorithms to classify the causes of the problems in different categories. Dynamic automated service composition uses interfaces to connect with Digital Twin and Response-Mitigation. Digital Twin provides simulation of different software and hardware components that interact with each other, and Dynamic automated service composition analyses if there are interconnection problems. In case of interoperability issues, the service proposes solutions via Response-Mitigation component.

7 Use Case Synergies

Along with the progress of RIGOUROUS, fine-tuning of components, assets and Use Cases comes as a natural process of development. The similarities and advantages of merge of efforts become more apparent as is the case of the proposed synergistic scenarios of Use Case 2 IoT-Based Smart City Platform and Use Case 4 PPDR IoT Situational Awareness.

Both Use Cases have a backend system architecture composed of microservices deployed on slices of the cloud resources. Certainly, the microservices differ in the type of information that they process or generate, but the logic behind the initial deployment and lifecycle management of these microservices is the same. Effectively, these micro-services need to communicate among themselves securely, run on dedicated slices with the right amount of resources allocated for them, and their placement (i.e., micro-service migration) or their allocated cloud resources (i.e., micro-service elasticity) may change during the service time. Naturally, any change in the allocated cloud resources should be carried out while coping with the risk of any economical denial of sustainability. Furthermore, the lifecycle management of these microservices should be carried out most autonomously, leveraging suitable AI algorithms. Naturally, these AI algorithms should be robust to adversarial attacks.

On the other hand, both Use Cases involve end-devices that need to authenticate with the backend system and exchange date securely, while preserving privacy of certain data. In this vein, the usage of homomorphic algorithms could be of vital importance. For end-devices with limited capabilities whose data need to be encrypted or decrypted, encryption and decryption could be provided as a service. In this vein, the project's EaaS platform could be leveraged. Effectively, it is one of the main points of the joint cooperation of both partners, as this topic can not only be applied to other factions of the RIGOUROUS framework but it can also be further developed into a publication and contribution for an Open-Source software initiative for RIGOUROUS.

Given the aforementioned context, the consortium has opted to amalgamate Use Case 2 and Use Case 4, along with their corresponding threat scenarios. This consolidation is approached through a dual-pillar framework: Pillar 1, emphasizes IoT data for Public Protection and Disaster Relief (PPDR), and Pillar 2, spotlights video streaming and Extended Reality (XR) technologies for PPDR and smart city applications. The resulting amalgamation is now denoted as Use Case 5.

It is important to note that the description of Use Case 5 may appear redundant, as it incorporates language used in the narratives of both Use Case 2 and Use Case 4. Below, the description of UC5 is presented, utilizing the descriptive elements from the two original use cases and their associated threat scenarios. However, the content is restructured to align with the specified dual-pillar approach outlined above.

7.1 Use Case V

7.1.1 Use Case‘s High Level Description

The increasing significance of Information and Communications Technology (ICT) is evident in its role in coordinating and planning Public Protection and Disaster Relief (PPDR) scenarios. These scenarios entail real-time coordination between field teams and Command-and-Control Centre (CCC) operators, particularly in challenging environments. The advent of 5G and subsequent technology generations has paved the way for Augmented Reality (AR) and Virtual Reality (VR) applications to enhance PPDR, improving the Quality of Experience (QoE). To address these needs, OneSource has developed Mobitrust, an IoT-driven situational awareness platform for PPDR. Mobitrust capitalizes on edge/cloud computing paradigms to facilitate efficient monitoring, aggregation, and analysis of PPDR data from diverse sources like positioning devices, field stations, vehicles, and wearable sensors worn by field operators.

Mobitrust not only empowers real-time communication between CCC operators and field personnel through text, audio, and video but also incorporates AI/ML algorithms strategically positioned along the edge/cloud continuum. This transforms Mobitrust into an intelligent platform capable of processing data and videos to enhance PPDR mission performance. This intelligence proves vital in detecting critical situations such as man-down incidents, environmental hazards, and physical threats, benefiting both field operators and decision-makers in the control center. Mobitrust also explores the potential of AR/VR technologies within PPDR scenarios, offering improved field views through AR Head-Mounted Displays (HMDs) and more intuitive interactions via VR HMDs.

Security remains a central concern in PPDR scenarios, demanding comprehensive protection across devices, microservices, components, and network communications. OneSource delves into mechanisms for authentication, authorization, and differentiated access, while also focusing on secure lifecycle management. The project aims to ensure the platform's secure behaviour, detect anomalies, and facilitate remote and secure updates. In essence, Mobitrust stands as a pioneering solution at the intersection of technology, disaster response, and security, poised to reshape and enhance the efficiency of PPDR operations.

This use case can be viewed from two perspectives: IoT for PPDR; and video streaming and XR technologies for PPDR. These two pillars are of upmost relevance but have very different requirements and characteristics, thus this UC is split into these two pillars.

Exploring video streaming and XR technologies in the context of PPDR through AR and VR reveals significant security and privacy challenges. The testing and deployment criteria for these technologies differ significantly from IoT. Notably, issues such as tracking vulnerabilities arise, where attackers may compromise finger and eye tracking data if not adequately secured. Additionally, concerns like DoS, spoofing, sniffing, and data manipulation pose specific risks, especially in UDP-concentrated communication.

As of IoT, distinct concerns centre around sensors and internal component communications. These components are susceptible to attacks such as spoofing, DDoS, DoS, XSS Injection, and SQL Injection, among others. It's important to note that the primary mode of network communication in IoT relies on TCP.

For each scenario presented next, we address the two pillars separately. In many cases, the KPIs and KVIs apply to both pillars, but the requirements and impact are different for each one. These differences will be explored in the assessment and evaluation phase of the assets in the use cases.

7.2 Security Threat Scenarios

7.2.1. SCENARIO 1 - PPDR scene and teams provisioning

7.2.1.1. Threat Scenario Description

Whenever a new operation begins, and throughout its course, many different teams and elements will arrive and join the operation, from field operatives to on-premises control operations. This means multiple devices being connected to the infrastructure that need secure authentication and authorization to access not only the services but also the network itself. As such, one possible threat is for unwanted devices to try to authenticate against the network and get access to the services deployed, which would have implications in terms of privacy as well as security and trust. Moreover, it could also be the case where in some situations, there would be a need for teams the use personal devices, usually referred to as Bring Your Own Device (BYOD). This increases the need for security analysis, since at the start, these devices are deemed unsecured until an analysis is made. Because PPDR events are usually isolated and occur occasionally, the Mobitrust platform might be deployed on demand, whenever it is needed at a given location. For this, a cloud/infrastructure manager will trigger the deployment of the platform, letting the orchestrator take control and manage it.

Pillar IoT for PPDR: this scenario is relevant to this pillar.
Pillar Video streaming and XR technologies for PPDR: this scenario is relevant to this pillar.

7.2.1.2. Mitigation Approach and Relevant Tools

The secure deployment of the Mobitrust platform, together with the network isolation on all communications, from the end-devices to the cloud, through slicing, will allow decreasing the chances of any device intrusion, going from the device registration in the network and slice access to continuous monitoring of the deployed services, doing any necessary life-cycle adjustments. For this management, the multi-Domain AI-driven Orchestrator will be the key component, which will take control from the beginning of the deployment of the framework, throughout the operations course, and ending with a controlled wrap-up of the scenario, taking any necessary actions for removing the deployment when it is no longer needed.

During the life cycle of the provisioning operations, in case of rogue devices being detected or failures in the bootstrapping of certain devices, alerts will be generated by the RIGOUROUS assets, being analysed by a cloud analyst and/or a platform analyst, but also processed automatically by the RIGOUROUS SOAR and acted upon following the Zero Touch Paradigm.

7.2.1.3. KPI and KVI

KPIs:

Table 7-1 The details of KPIs

Name	Measurement	Measure	Pillar

Framework Deployment	Measure the time taken from the first instruction of deploying the framework until all the services are up and running on the edge/cloud.	<1s	Both
End-to-end slicing	Measure the time taken for the configuration of the new slice across the different network segments.	<1s	Both
BYOD trust analysis	Measure the time taken to analyse the device and deem it secure/insecure to be used in the operation.	<1s	Both
Device bootstrapping	Measure the time taken for the bootstrapping of the end-devices with all needed configurations.	<1s	Both

KVIs:

Table 7-2 The details of KVIs

Name	Explanation	Pillar
Zero-touch configuration	Having the configuration/reconfiguration of the end-devices automated, takes a big burden from the support/management teams, while lowering the chances of applying bad configurations and disrupting the operation in course.	Both
Trusted deployment	Due to the sensitivity of the information captured and transmitted, security is a key point. By having guarantees that all network elements that support the deployment are trusted and secured, the overall trustworthiness of the framework is increased.	Both
Secure and prioritized communications	End-to-end slicing has an impact in two distinct ways. For one hand, with the traffic isolation it enhances the security of communications, reducing the means of intrusion. On the other hand, it elevates the QoS capabilities from the transport layer to the entire network, ensuring a more reliable and performant communication across the IoT-edge-cloud continuum.	Both

7.2.1.4. Relevance to RIGOUROUS Objectives and Technical Tasks

Objective 3 - Model-based and AI-driven Automated Security Orchestration, Trust Management, and deployment

- R7- Multi-Domain AI-driven Orchestrator: The deployment and maintenance of the framework will be managed by the Orchestrator, which will be the central control point, integrating with the different tools and technologies of the project.
- R8- Trust evaluation and Trust enabler service framework for the B5G and 6G system: The security and trustworthiness of the nodes and network components are a key aspect to ensure the overall security of the framework deployment.
- R9- IoT bootstrapping mechanisms and R10- Trusted application onboarding: The deployment of the framework, also considers the bootstrapping of the end-devices, which is aimed to follow a zero-touch approach for the entire setup and configuration.

- R11- Security Agents and Security Slice Controllers for End-to-end multi-domain slicing: In order to have control over the network and isolation of the traffic for this application, network slicing will be a key element in achieving and maintaining it.

Objective 4 - Advanced AI-driven Anomaly Detection, decision, and Mitigation Strategies

- Encryption as a Service: The use of the EaaS will allow the further increase of security and privacy when dealing with delicate data exchanged throughout the cloud continuum.

7.2.2 SCENARIO 2 - Unlawful access to IoT gateways, platform’s APIs, and IoT data violating data privacy

7.2.2.1. Threat Scenario Description

The compromising of data privacy is a major risk for information that is related to public safety and disaster response, as the identification of bodies of workers involved in emergencies violates not only their integrity as well as their privacy rights.

Pillar IoT for PPDR: this scenario is relevant to this pillar.
Pillar Video streaming and XR technologies for PPDR: not relevant to this pillar.

7.2.2.2. Mitigation Approach and Relevant Tools

To secure platform APIs, adherence to best security practices in service development, utilizing tools like ISTIO Security Services. For IoT gateway remote access, restrict authorization to authorized users and services from the platform's backend. Employ scalable authentication mechanisms, using data like serial numbers, default codes, UUIDs, and device models. Pre-register this data in the system's database before shipping IoT gateways. Users authenticate by logging in with credentials, and then input gateway details for verification against the database. Successful verification binds the IoT gateway to the user, confirming their legal right to operate it. Users may subsequently change authentication codes.

To protect IoT data from privacy violations, encryption and decryption mechanisms should be used. In this vein, it is important to support PPDR platforms by an Encryption as a Service platform that shall provide cryptographic services to IoT gateways, particularly those with limited processing capabilities. Moreover, the Encryption as a Service platform may also provide homomorphic encryption, differential privacy and zero-knowledge proof services, allowing to build privacy-preserving AI/ML models that can process encrypted data. Figure 4-3 of Chapter 4 illustrates a high-level architecture of such EaaS platform.

7.2.2.3. KPI and KVI

Table 7-3 The details of KPIs and KVIs

KPIs:

Name	Measurement	Measure	Pillars

Scalability	Number of encryption requests handled per second by an encryption algorithm running on a container with specific features.	>4 Req/s	IoT
Scalability	Number of decryption requests handled per second by a decryption algorithm running on a container with specific features.	>4 Req/s	IoT
Responsiveness	Time needed to encrypt an IoT data with a specific text length using a specific key length using a specific encryption algorithm running on a container with specific features	<1s	IoT
Responsiveness	Time needed to decrypt a ciphered text with a specific length using a specific key length using a specific decryption algorithm running on a container with specific features	<1s	IoT
Key Generation Time	Time needed to generate a key for encryption or decryption	<1s	IoT
CPU Usage	Reduction of CPU consumption for each encryption/decryption instance	>10%	IoT
RAM Usage	Reduction of RAM consumption for each encryption/decryption instance	>10%	IoT

KVIs:

Name	Explanation	Pillars
Service Scalability Efficiency	Service Scalability Efficiency, a KVI, measures the ratio of achieved scalability to the target scalability for both encryption and decryption. This percentage-based calculation helps in managing scalability effectively, with a higher percentage indicating efficient scalability.	IoT
Resource Utilization Efficiency	The efficiency of CPU and RAM usage for encryption and decryption instances. The calculation considers the actual usage about the maximum capacity, aiming for a high percentage to ensure optimal resource utilization.	IoT

7.2.2.3. Relevance to RIGOUROUS Objectives and Technical Tasks

Objective 1 - Holistic Smart Service framework for securing the IoT-Edge-Cloud continuum lifecycle management

This use case targets securing the communication between the IoT gateways and the microservices of the platform's backend running at the edge or the cloud, as well as securing data against privacy violations.

Objective 2 - Human-Centric DevSecOps

As part of the management of services and IoT devices, this use case aims to provide an operating Encryption/Decryption as a Service platform that can help in the privacy protection of IoT data and contributing to the DevSecOps pipeline.

Objective 5 - Demonstration of a Set of Industrially Relevant Use Cases in Operational Environments

An operating Decryption/Encryption as a Service platform to protect the IoT data privacy of microservice based platforms will be demonstrated.

7.2.3. SCENARIO 3 - Intrusion into system to access privileged information or cause disruption of services

7.2.3.1 Threat Scenario Description

While the systems are deployed, an intrusion may be detected in the network, coming from anywhere in the infrastructure. This intrusion may have multiple purposes, from eavesdropping and trying to acquire sensitive information about on-going/past operations, to causing harm, by making changes to the data and/or manipulating actions under execution.

Pillar IoT for PPDR: this scenario is relevant to this pillar.
Pillar Video streaming and XR technologies for PPDR: this scenario is relevant to this pillar.

7.2.3.2 Mitigation Approach and Relevant Tools

To improve the security of the deployed services and minimize/stop any attack being made, continuous monitoring will be a key feature, using AI-based mechanisms for the detection and mitigation of ongoing attacks. Anomaly detection may have a key impact on improving the detection of unknown attacks, allowing to take any needed measures. Moreover, defence mechanisms, such as, MTD, can also take a key role on increasing the security of the deployed services.

The detection of such intrusions or anomalies by the RIGOUROUS functional components will trigger its SOAR to act accordingly, while the alerts coming from those assets can also be inspected by the infrastructure analysts, which may decide to take different measures or not. This post-incident analysis can also loop-back into the AI-driven decision mechanisms to further enhance the analysis and decision-making processes.

7.2.3.3 KPI and KVI

Table 7-4 The details of KPIs and KVIs for measure the time taken to detect a known attack

KPIs:

Name	Measurement	Measure	Pillar
Known attack detection time	Measure the time taken to detect a known attack being made to one of the framework components.	<1s	Both
Unknown attack detection time	Measure the time taken to detect an unknown attack being made to one of the framework components.	<1s	Both
Mitigation time	Measure the time taken to deploy measures to mitigate the attack under course.	<1s	Both

KVIs:

Name	Explanation	Pillar
Secured platform	The security measures taken from the beginning increase the overall base security, reducing the chances for possible attacks or manipulations of the framework. This then guarantees smoother management of the operations, increasing the potential success of the actions being taken.	Both
Decreased interferences and downtime	Despite the increased based security, some attacks or interferences might still occur. Decreasing the time taken to detect and mitigate those cases can lead to less impact on the ongoing actions, preventing possible riskier scenarios due to system unavailability.	Both

7.2.3.4 Relevance to RIGOUROUS Objectives and Technical Tasks

Objective 3 - Model-based and AI-driven Automated Security Orchestration, Trust Management, and deployment

- R11- Security Agents and Security Slice Controllers for End-to-end multi-domain slicing: In order to properly handle disruption of services isolation of the application ends comes as a relevant factor for security improvement.

Objective 4 - Advanced AI-driven Anomaly Detection, decision, and Mitigation Strategies

- R12- Privacy-preserving FL-based Anomaly Detector: Continuous monitoring for potential attacks and anomalies increases the response time for mitigation actions and recovery actions.
- R14- MTD-based Robust ML Models: Enhancing security from the get-go reduces the chances of attack, resulting in an increased base level of security.
- R16- AI-driven decision making: The alerts coming from the anomaly detection functional blocks, together with other relevant data will be used to make the decisions on the mitigation actions to apply to each detection.
- R19- Threat Risk Assessment Tool: Identifying threats through the anomaly detection functional blocks and vulnerabilities in a system and making informed decisions about risk allows for an assessment and prioritization of risks based on their likelihood and potential impact.

7.2.4. SCENARIO 4 - Disclosure of device vulnerability or unlawful appropriation of a device

7.2.4.1 Threat Scenario Description

Throughout an ongoing operation, it could be disclosed that one or more pieces of equipment have disclosed vulnerabilities identified. Moreover, it could also happen that a device is lost or stolen amidst the stress of the operation. As such, appropriate measures must be taken to address both these scenarios.

Pillar IoT for PPDR: this scenario is relevant to this pillar.
Pillar Video streaming and XR technologies for PPDR: this scenario is relevant to this pillar.

7.2.4.2 Mitigation Approach and Relevant Tools

Since the devices used in these scenarios have access to restricted networks and information, having any sort of vulnerability detected or unlawful usage poses high security threats. As such, dealing with these cases is of paramount importance. Whenever either of these cases occurs, the steps to take is to erase all information from the devices, followed by the necessary steps to unauthorize the device in the network, so that it can no longer connect to any of the secure channels.

Similarly, to the above scenarios, the detection of such cases should be swiftly acted upon by the RIGOUROUS SOAR, while also generating the necessary alerts which will allow the analysts to do a proper inspection of the issues and take extra/different measures if deemed necessary.

7.2.4.3 KPI and KVI

Table 7-5 The details of KPIs and KVIs for detect the vulnerability

KPIs:

Name	Measurement	Measure	Pillars
Vulnerability detection time	In the scenarios where it is possible to detect the vulnerability, measure the time it takes to achieve said detection.	<1s	Both
Device data deletion	Measure the time taken to delete all critical data of the device.	<10s	Both
Authorization revocation	Measure the time taken to unauthorize the device and for it to be de-registered from the network.	<10s	Both

KVIs:

Name	Explanation	Pillars
Vulnerability exposure	In situations that deal with a lot of sensitive information, there are many cases of exploration of vulnerabilities when trying to access said information. As such, mitigating those vulnerabilities as soon as they are detected reduces the chances of their unlawful exploration and access to privileged data.	Both
Lost/Stollen devices	Since the devices used are registered to secure channels and have special accesses and permissions, having one of these lost or stollen can greatly compromise the security of the entire network. As such, being proficient on dealing with these scenarios will reduce the amount of time where the scenario security is compromised.	Both

7.2.4.4 Relevance to RIGOUROUS Objectives and Technical Tasks

Objective 2 - Human-Centric DevSecOps

- R3- Human-centric user-friendly tools for DevSecOps and risk management: With devices that have a user-friendly interface we bring a more likely adoption by teams leading to better engagement with security practices throughout development and operation cycles.
- R5- User controlled verifiable secure digital identification service: With information of devices being restricted, networks and information should be identifiable and registered in a way that devices can't be replicated for malicious purposes.

Objective 4 - Advanced AI-driven Anomaly Detection, decision, and Mitigation Strategies

- R19- Threat Risk Assessment Tool: With heterogeneous device requirements in technical environments there is a need for appropriate measures to be taken in place to protect confidentiality, integrity, and availability of private information.

7.2.5. SCENARIO 5 - Economical Denial of Service and Adversary AI attacks

7.2.5.1. Threat Scenario Description

The PPDR platform which can be utilized by different teams operating in different regions can be deployed across different cloud domains, and by manipulating factors such as the allocation of cloud resources there can be a huge impact on communications and scaling of needed components such as VR or AR. The lack of these resources can cause critical problems and possibly put human lives in cause.

Pillar IoT for PPDR: this scenario is relevant to this pillar.
Pillar Video streaming and XR technologies for PPDR: this scenario is relevant to this pillar.

7.2.5.2. Mitigation Approach and Relevant Tools

To address potential adversarial machine learning/artificial intelligence (ML/AI) threats, an AI-based EDoS (Economic Denial of Sustainability) Detection & Mitigation framework is essential. Mitigation strategies include migrating impacted microservices to secure edge cloud nodes and rejecting auto-scaling operations. Implementing Moving Target Defense (MTD) with robust ML models helps prevent adversarial attacks on ML models.

To enhance the accuracy of EDoS detection, incorporating metrics relevant to the cloud infrastructure is crucial. Establishing an interface with IoT service providers further improves effectiveness. The framework can query providers about significant changes in service consumption patterns, especially during auto-scaling operations. By leveraging trained models and infrastructure-related data, the framework evaluates the legitimacy of operations. In cases of uncertainty, communication with the IoT service provider helps validate changes in IoT service consumption. If confirmed, the framework adjusts its decision to allow necessary resource scaling; if denied, it rejects the operation as potentially malicious. This mechanism of interfacing and cross-referencing information enhances the EDoS detection and mitigation framework's accuracy, enabling more informed decisions on resource scaling.

7.2.5.3. KPI and KVI

Table 7-6 The details of KPIs and KVIs for detection, mitigation accuracy

KPIs:

Name	Measurement	Measure	Pillars
Detection accuracy	This metric measures the number of actual anomalies (e.g., EDoS attacks) correctly detected by a ML model. Both centralized and federated learning will be considered.	%	Both
Mean time to detection	The time between the attack launch and its detection by the ML model.	ms	Both
Mean time to mitigation	The time between the anomaly detection by the ML model and its mitigation.	s	Both
Blocked adversarial examples rate	The percentage of adversarial examples that the ML model can resist (when MTD technique is applied) compared to the total number of adversarial examples generated by the attacker.	%	Both

KVIs:

Name	Explanation	Pillars
Resource allocation and Prioritization	Efficient allocation of resources to prioritize legitimate user requests over malicious traffic during an attack.	Both
User Authentication and Authorization	Strong authentication methods to ensure that legitimate users can access services while unauthorized users are prevented from causing harm.	Both

7.2.5.4. Relevance to RIGOUROUS Objectives and Technical Tasks

This scenario pertains to all the project objectives.

Objective 1- Holistic Smart Service framework for securing the IoT-Edge-Cloud continuum lifecycle management

By protecting the underlying infrastructure from adversary AIs, the whole IoT-Edge Cloud continuum lifecycle management can be protected.

Objective 2- Human-Centric DevSecOps

The adversary AI techniques till be an integral part of the DevSecOps pipeline.

Objective 3- Model-based and AI-driven Automated Security Orchestration, Trust Management, and deployment

This use case targets securing the underlying infrastructure and the orchestration of its resources in in an AI-driven fashion, coping also with the risks of adversary AIs.

Objective 4- Advanced AI-driven Anomaly Detection, decision, and Mitigation Strategies
This use case involves AI-driven anomaly detection and mitigation mechanisms, and that includes privacy-preserving FL-based anomaly detection, AI-powered EDoS mitigation, and MTD-based Robust ML Models.

Objective 5- Demonstration of a Set of Industrially Relevant Use Cases in Operational Environments
The above-mentioned privacy-preserving FL-based anomaly detection, AI-powered EDoS mitigation, and MTD-based Robust ML Models will be evaluated and demonstrated.

8 Mapping with the RIGOUROUS Architecture

In Use Case 1, various functional components are described in detail in the high-level architecture section of D2.1. These components are designed to ensure that any threats to the system are mitigated effectively. The aim is to flag any suspicious authentication attempts, block any unauthorized activities, scan technology signatures, and ensure that superior service monitoring and orchestration can address any detected attacks. One of the most important components is the security orchestrator, which is responsible for enforcing security requirements through virtual network security functions and local domain policies. It relies on Intent-Based Security Management (ISM) for security policy management and deploys agents like, Slice Manager (SM), or NFV MANO to ensure the system is protected from potential threats. The AI-driven decision (AID) functional block plays a critical role in threat type detection and classification, especially in the threat scenario focused on information gathering and classification. RIGOUROUS should be able to detect and block scanning technology signatures and enumeration attempts. The zero trust identity management functional component (ZTM) is also essential to minimize network access based on authentication, authorization, and security posture. The RIGOUROUS Framework offers a Zero Trust Management function collecting data from Network Repository Functions. Data services (DS) and monitoring are required to collect useful data on the devices discovered in the network and the network ports. Up-to-date topology discovery could be performed using the Topology Service, and updates for hosts, devices, and ports for the Slice Mitigation Planning could be implemented. Regarding privacy-enhancing techniques, the Cyber Threat Information block could be used to protect sensitive data. It includes a privacy-preserving service and a Threat Intelligence Platform (CTI), generating CTI information, including attacks, AI models, security requirements, and software updates. With these components and techniques in place, the system can be effectively protected against potential threats, ensuring it is always secure and reliable.

Use Case 2 of the IoT-based Smart City Platform is designed to withstand potential threat scenarios by employing a range of carefully considered mechanisms. These mechanisms are intended to enhance data confidentiality and prevent unauthorized access to both data and the platform's backend system. To reinforce data confidentiality, a multi-layer encryption scheme has been implemented, complemented by a robust authentication and authorization mechanism that governs device access to the platform. Encryption as a Service (EaaS) platform has also been utilized to explore the potential for further enhancing data confidentiality. In addition to these measures, the platform's backend system is fortified against Economical Denial of Service (EDoS) and Adversary AI attacks by leveraging key components from the RIGOUROUS architecture. These components include the Security Analytics Engine (SAE) and elements of Cognitive Decision, Orchestration, and Management, which are instrumental in identifying and categorizing various threat types. They make use of tailored algorithms to counter specific threats, like EDoS mitigation for Economical Denial of Service attacks. Moreover, Use Case 2 can benefit from integrating the RIGOUROUS component privacy-preserving CTI sharing (CTI). This component offers valuable anonymization techniques that safeguard the identity of involved entities, aligning with industry best practices for information exchange. In essence, the proposed measures not only strengthen data confidentiality and protect against potential threats but also underscore the proactive and comprehensive approach embedded in the RIGOUROUS project's architecture. The strategic integration of these security measures ensures that Use Case 2 is well-positioned to address evolving challenges in the context of the IoT-based Smart City Platform.

As part of our analysis for Use Case 3, we have undertaken an in-depth exploration of data security, specifically focusing on RIGOUROUS Architecture - Utilities Management and Security. Our investigation encompasses a wide range of potential threats, including data breaches, distributed denial-of-service (DDoS) attacks, and code and data injection, as well as the challenges that can arise from outdated systems. Throughout our report, we highlight the importance of mapping the RIGOUROUS Architecture to gain a more detailed understanding of the intricate interplay between different aspects of facilities management and data security. By doing so, we can provide a more nuanced assessment of the potential risks and strategies for mitigating them.

In Use Case 3 several functional blocks of RIGOUROUS Architecture will be used to protect the Utilities sector from cyberattacks. More specifically, Security Analytics Engine (SAE) will be used to detect anomalies in the network traffic flow that are due to a possible cyberattack. SAE communicates with AI driven Decision (AID), which is the functional block that proposes the required actions based on the calculated risk level. Additionally, Dynamic and Automated Service Composition (DSC) will be used in order to detect mismatches between different components, especially those that are due to outdated systems. The system consisting of the different components will be modelled using the Digital Twin (DT). Finally, Response-Mitigation (PM)is responsible for proposing the appropriate mitigation measures to resolve the issues.

In Use Case 4, the presence of various services offering diverse communication types, ranging from IoT to video and XR using AR and VR components, creates the potential for utilizing several components in different scenarios. One such example is the Security Analytics Engine (SAE), which facilitates threat analysis and detection through federated means. It serves as an informant for the Cognitive Decision, Orchestration, and Management, which takes appropriate action based on the assessed level of risk derived from the identified threats. This decision-making process performed by the AI-driven Decision (AID) is of paramount importance in this use case, particularly since some threats may originate from compromised equipment, and timely intervention is crucial to prevent adverse effects on other operational elements. The incorporation of Zero Trust and Identity Management (ZTM) emerges as a valuable functional component, contributing to the mitigation of faulty and rogue equipment in the field. It helps to ensure that only authorized devices and users can access the system, thereby limiting the potential for malicious activities to occur. These components work together to provide a comprehensive and secure communication framework that enables efficient and safe operations in various scenarios. In addition to these mitigation efforts, Encryption as a Service (EaaS) is employed to enhance the privacy of transmitted information across components and devices. Human-centric Privacy risk management (PUI) and Threat Risk Assesor (TRA) is also utilized to enhance the authenticity of devices across different orchestration slices, incorporating Network-based MTD and AI-based Security Orchestration (SO) across network segments. This approach increases the complexity of the attack surface for malicious actors, making it more challenging to predict and exploit vulnerabilities in the devices.

9 PRELIMINARY MAPPING WITH THE RIGOUROUS ASSETS

The initial alignments between project use cases and corresponding assets are succinctly outlined in the descriptions of the respective use cases. To expound upon this, Table 9-1 illustrates a comprehensive plan for further mapping, showcasing anticipated connections between project assets and use cases. It is crucial to acknowledge that this is a preliminary plan, and adjustments may transpire for the project.

Table 9-1 Preliminary mapping between RIGOUROUS Assets and Use cases

	Partner	Task	Assets	UC1	UC2	UC3	UC4
R01	UMU		open-source AI-driven framework for securing the IoT-Edge-Cloud Continuum	x	x	x	x
R02 / R04	UMU		Intent-based Security & Privacy formal modelling and onboarding specification	x		x	
R03	ITAV	3.1	Human-centric Privacy risk management for DevSecOps			x	x
R04	ITAV	3.1	Onboarding tools (T3.1)			x	x
R05	LNVO	3.1	Decentralized services based Identity and Trust managment specification	x		x	
R07	UMU	3.2	AI-based Security Orchestration across network segments	x			x
R08	LNVO	3.3	Trust evaluation and Trust enabler service framework specification	x			
R09	LNVO	3.2	IoT bootstrapping specification		x	x	x
R10	LNVO	3.2	Trusted application onboarding specification			x	x
R11	UWS	3.4	Slice manager	x			x
R11	UWS	3.4	Network Self-Protection	x			x
R12	ONE	4.1	Holistic Security and Privacy Framework		x		x
R12	OULU	4.1	Privacy-preserving FL-based Anomaly Detector		x		x
R12	UMU	4.1	Privacy-preserving Federated AI for anomaly detection.	x		x	x
R13	OULU	4.1	AI-powered EDoS Mitigator		x		x
R14	OULU	4.1	MTD-based Robust ML Model(s)		x		x
R15	WINGS	4.2	Dynamic and Automated Service Composition			x	x
R15	WINGS	4.2	Digital Twin			x	
R16	eBOS	4.3	AI-driven decision making	x	x	x	x
R16	eBOS	4.4	AI-driven algorithm for risk management and mitigation provision	x			
R17	eBOS	4.3	Multiple ML models to provide multiple opinions to the AI-driven decision-maker (T4.3)				x

R18	WINGS	4.3	Cyber Physical Correlator			x	
R19	RHEA	4.3	Threat Risk assessor (TRA)	x		x	x
R20	UWS	4.4	Network Flow Monitoring	x			
R20	UWS	4.4	SOAR solution: Resource Inventory Agent, Security Detection Tool, Security Planner (T4.4)	x			
R21	ICT-FI	4.4	Encryption as a Service		x		x
R22	ITAV	3.1	Network-based MTD modeling and specification for DevSecOps and risk management			x	x
R23	UMU	4.1	Privacy-preserving CTI sharing	x		x	

10 CONCLUSIONS

This deliverable is of utmost importance as it outlines in detail the various use cases of the RIGOUROUS project. The use cases discussed here have been carefully curated to encompass different scenarios, threat analyses, and mitigation strategies across diverse domains, such as 6G-enabled services, IoT-based Smart City Platforms, utility management, and Public Protection and Disaster Relief (PPDR).

One of the key highlights of this document is the proactive defence mechanisms embedded in RIGOUROUS components to address specific cybersecurity challenges in each scenario. This is an essential aspect of the project as it ensures that the RIGOUROUS project is well-equipped to handle any potential threats and challenges.

This deliverable establishes a crucial link between the various use cases and the project's high-level architecture. This strategic framework for addressing evolving telecommunications and security challenges is significant as it offers a roadmap for future research efforts within the project.

11 REFERENCES

[1] Benzaïd, Chafika, Tarik Taleb, and JaeSeung Song. "AI-based autonomic and scalable security management architecture for secure network slicing in b5g." IEEE Network 36.6 (2022): 165-174.

[2] Benzaïd, Chafika, Tarik Taleb, and Muhammad Zubair Farooqi. "Trust in 5G and beyond networks." IEEE Network 35.3 (2021): 212-222.

[3] Benzaïd, Chafika, and Tarik Taleb. "AI for beyond 5G networks: a cyber-security defense or offense enabler?." IEEE network 34.6 (2020): 140-147.

[4] C. Benzaid and T. Taleb, "ZSM Security: Threat Surface and Best Practices," in IEEE Network Magazine, Vol. 34, No. 3, Jun. 2020, pp. 124 - 133.

[5] Benzaïd, C., Taleb, T., Sami, A., & Hireche, O. (2023). FortisEDoS: A Deep Transfer Learning-empowered Economical Denial of Sustainability Detection Framework for Cloud-Native Network Slicing. IEEE Transactions on Dependable and Secure Computing.

[6] Taleb, T., Benzaïd, C., Addad, R. A., & Samdanis, K. (2023). AI/ML for beyond 5G systems: Concepts, technology enablers & solutions. Computer Networks, 237, 110044.

[7] Amir Javadpour, Forough Ja'fari, Tarik Taleb, Yue Zhao, Yang Bin, and Chafika Benzaïd, " Encryption as a Service for IoT: Opportunities, Challenges and Solutions," in IEEE Internet of Things Journal, 2024.