IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 29 May 2024, accepted 9 July 2024, date of publication 15 July 2024, date of current version 24 July 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3427661

RESEARCH ARTICLE

A Security Services Management Architecture Toward Resilient 6G Wireless and Computing Ecosystems

EVA RODRIGUEZ[1], XAVI MASIP-BRUIN[1], JOSEP MARTRAT[2], RODRIGO DIAZ[2], ADMELA JUKAN[3], (Fellow, IEEE), FABRIZIO GRANELLI[4], (Senior Member, IEEE), PANAGIOTIS TRAKADAS[5], AND GEORGE XILOURIS[5]

[1]Advanced Network Architectures Laboratory (CRAAX), Universitat Politècnica de Catalunya (UPC), Vilanova i la Geltru, 08800 Barcelona, Spain
[2]Eviden Research and Innovation, 08020 Barcelona, Spain
[3]Department of Communication Networks, Technische Universität Braunschweig, 38106 Braunschweig, Germany
[4]CNIT, University of Trento, 38123 Trento, Italy
[5]Department of Port Management and Shipping, National and Kapodistrian University of Athens, 344 00 Athens, Greece

Corresponding author: Xavi Masip-Bruin (xavier.masip@upc.edu)

This work was supported by the European union's Horizon Europe, under the project HORSE, Grant 101096342. The work of Eva Rodriguez and Xavi Masip-Bruin was supported in part by the Spanish Ministry of Science and Innovation funded by MCIN/AEI/10.13039/501100011033 and ERDF: A way of making Europe under Grant PID2021-124463OB-I00, and in part by the Catalan Government under Contract 2021 SGR 00326.

ABSTRACT The upcoming sixth-generation (6G) networks are expected to be more heterogeneous, scalable, reliable, secure and energy-efficient. 6G services and applications will benefit from the fast data transmission rates, global coverage, precise positioning, and widespread intelligence capabilities provided by 6G technology. In this complex scenario, new attack surfaces and vectors will emerge, due to the distributed, disaggregated, dynamic, programmable and open nature of the entire end-to-end 6G infrastructure along with the fragmentation of data, as well as the need for supporting cross-platforms interoperability, making the application of security and trust fundamentally challenging. To securely manage services in the future 6G mobile networks along with the set of functions ruling its management, conceptual work is needed to defining functional blocks supporting a secure end-to-end 6G systems management. This is especially critical in handling specific functionalities, such as network disaggregation, risk and threats business impact, energy-efficiency, self-configuration or dynamic discovery. This paper positions an innovative 6G security services management architecture, which builds on a set of innovative building blocks, leveraging key technologies, such as AI-assisted models and Digital Twin, while enabling a human-centric approach toward an end-to-end security solution. Two canonical workflows along with two illustrative application scenarios are proposed, Light Rail Transit and Extended Reality, to conceptually highlight the proposed architecture impact and its expected benefits when high bandwidth, ultra-low latency, and secure communications are required.

INDEX TERMS 6G, communication systems, wireless communication, network architecture, security.

I. INTRODUCTION

The rapid evolution towards sixth-generation (6G) networks has repositioned networking, computing and communications at the center of technological innovation, making them valuable and viable for new types of high-speed and compute-intensive applications or services, while guaranteeing their pervasiveness and dependability. 6G technologies, benefiting from softwarization, Gb/s speed and sub-THz communications paradigms, open up opportunities for developing new and innovative network management strategies. 6G applications aim to provide a superb user experience, for

The associate editor coordinating the review of this manuscript and approving it for publication was Rentao Gu.

virtual presence, robotic industrial and health applications and autonomous driving, all melting in a mix of virtual and real worlds. As the vision of new, smart and innovative capabilities is becoming the reality at a rapid pace, creating a novel 6G infrastructure is crucial, as a driving force in the development of novel services. In this network context, security, privacy and resiliency features are not only requested ''by design'', instead, they push the envelope of managing a truly evolving system, with features engineered ''by the evolution itself''. In particular, the fundamentally new and unknown features of advanced, disaggregated, virtualized and multi-vendor 6G based infrastructures challenge the security and resilience design at the new levels, which requires novel management architectures for the complex and highly versatile infrastructures and services [1].

The envisioned challenges will undoubtedly be addressed through solutions leveraging modern technology tools, such as Artificial Intelligence (AI) [2]. In future 6G networks, AI-methods will be used to, on one hand improve response and resilience of systems, such as for the early detection of threats and anomalies, while on the other hand, identify and correct vulnerabilities by attacking the systems predicted to be exposed in a sandbox environment, such as in Digital Twins (DT). From the services management perspective, the application of AI should follow a coordinated approach, by combining both reactive and predictive methods [3]. To this end, we envision a novel smart and adaptive security services management layer, designed to reduce the incident disruption and response time by providing improved predictive orchestration toward a zero-touch/zero-trust architecture encompassing compute, storage, data and network resources as well as services to be deployed.

This paper proposes and positions the key foundations behind a conceptual security services management architecture for future 6G networks, including a human-centric, open-source, green, sustainable, coordinated provisioning and protection evolutionary platform, designed to work under the envisioned 6G landscape. The architecture is part of the ongoing work in the EU project HORSE, which encompasses a few distinct tools, technologies and functionalities, such as predictive threats detection and impact analysis, proactive business-wise threats and breaches mitigation actions, programmable networking, Network Function Virtualization (NFV), intent-based networking, AI-based techniques, and cross-layer management of physical layer features, as they emerge in the 6G realm. The project is envisioned to efficiently accommodate the specific security needs and requirements demanded by the future 6G landscape.

The rest of the paper is as follows: Section II reviews related work in 6G mobile networks focusing on security, threat modeling, and mitigation. Section III presents the scenario considered for the definition of the HORSE architecture, Section IV deeply describes the main modules in the HORSE architecture, Section V introduces two workflows to describe the expected interactions between the different modules and components defined in the architecture proposed in Section II, and Section VI proposes two real-world application scenarios. Finally, Section VII concludes the paper.

II. RELATED WORK

This section presents 6G related work focusing on security, threat modeling, and AI-based solutions for threat detection and mitigation.

A. SECURITY IN THE 6G WORLD

Nowadays, 5G and B5G mobile networks have been coping with multiple diverse threats with an accessible user information explosion [4]. Nevertheless, so far, security and privacy issues for 6G have remained largely in concept [5], [6]. Satellite-based communications is an important enabling technology for the development of the upcoming 6G networks [7], [8], [9]. The authors in [10] made a survey with the aim of classifying security solutions. Reconfigurable intelligent surface (RIS) is a promising technique that can be deployed for future 6G wireless systems to improve both spectrum and energy efficiency of wireless networks [11]. As security is one of the important issues for future wireless networks, different studies investigated the secrecy capacity of RIS in different scenarios, as underwater Optical Wireless Communication [12] or vehicle-to-infrastructure (V2I) communications [13]. Additionally, a novel air interface technology with non-orthogonal multiple access (NOMA) has been used for massive connectivity in the 6G era [14]. Its link security issue was investigated in [15]. Most promising efforts aimed at tackling security and privacy issues in the envisioned 6G architecture are those combining and integrating AI in the respective workflows [16]. Paper [17] provided an interesting study on the combination of AI and 6G describing intelligent and robust security solutions. In [18], a 6G IoT model was considered including IoT devices connected to cellular networks and it was proposed to use an AI-based adaptive security specification method. There is a consensus through the fact that human-centric communication technology is one of the important aspects for a successful development and deployment of future networks beyond 5G (B5G) [19], [20]. Paper [21] showed a novel vision of human-centric networking with new concepts of ''Collective-Intelligence'' and sociotechnical design proposed as key pillars for driving future network architectures.

The main motivation behind the HORSE architecture is to advance the state of the art by proposing a holistic, human-centric and sustainable security framework for end-to-end 6G systems, securing the lifecycle management in multi-stakeholder and multi-domain resource environments. HORSE proposes to use intent-based orchestration functions aiming at automating the processing, storage and management by mapping specific security intents, using advanced AI/ML algorithms, into security and reliability actions and policies spanning across multiple heterogeneous domains. In addition, predictive threat detection and mitigation procedures based on AI/ML techniques are considered in the

HORSE architecture to protect 6G systems from attacks that can potentially impact the performance or availability of the services as well as the data privacy.

B. THREATS IDENTIFICATION & MODELLING

Characterizing and modelling threats along with getting knowledge about potential attackers would allow security actions to be properly deployed [22], [23]. Indeed, the impact the same attack may have when occurring on distinct systems, may differ not only based on the system landscape but also on other key aspects, such as the attacker itself and the business model behind. These factors should notably contribute to define the actions to be taken by the system to get protected and stay resilient. Hence, it is of paramount importance to regain as much knowledge as possible from possible attacks, threats and also attackers. To this end, the HORSE architecture leverages the work done in the MITRE ATT&CK Framework [24], as an international standard of attacks model mapping. The MITRE ATT&CK matrix contains a set of techniques used by adversaries to accomplish a specific objective, categorized as tactics in the ATT&CK Matrix: Reconnaissance (gathering information to plan future adversary operations); Resource Development (setting resources to support operations); Initial Access (trying to get into your network); Execution (trying to run malicious code); Persistence (trying to maintain their foothold); Privilege Escalation (trying to gain higher-level permissions);Defense Evasion (trying to avoid being detected); Credential Access (stealing accounts names and passwords); Discovery (trying to figure out your environment); Lateral Movement (moving through your environment); Collection (gathering data of interest to the adversary goal); Command and Control (communicating with compromised systems to control them); Exfiltration (stealing data); Impact (manipulate, interrupt, or destroy systems and data). HORSE aims at identifying the specific threats and attacks that a 6G ecosystem may be sensitive to, by using and extending the work done in MITRE ATT&CK Framework, and in particular by defining the attributes and parameters needed to successfully develop such characterization. Moreover, it will use novel predictive strategies, detection measures and mitigation solutions that will strengthen the 6G landscape cybersecurity, while also spreading out knowledge on potential attacks and corrective measures within the involved community.

C. AI-ENABLED SOLUTIONS FOR SECURITY ENHANCEMENT AND THREAT MITIGATION

The cyberattacks in 6G networks are expected to be polymorphic in nature as well as rather sophisticated, requiring smart decision support systems to evaluate different factors, such as the severity of the incident, the criticality and resilience of the infrastructure compromised or the cost of enforcing a mitigation [25]. In [26], a detailed analysis of the threat landscape of 6G networks is provided, while in [27], an optimization framework was proposed to address the security challenges, by optimizing security scheme selection and configurations to balance the security-energy trade-off in various scenarios. In [25], new threats caused by the introduction of new technologies were analyzed as they relate to the usage of open-source tools and frameworks for 6G network deployment, along with possible mitigation strategies to address these threats. In general, AI solutions are based on centralized data collection [28], which not only poses serious privacy issues, but it is also not aligned to the distributed architecture of 6G networks. ML and AI-based optimization approaches can be used to improve time-series and statistics-based methods to operate beyond abnormal conditions and train the system generating attacks. For instance, in [29] the use of Generative Adversarial Networks (GANs) is explored to simulate intrusions and malware for improving its detection. In [30], several DL architectures are used for the detection of threats. In [31], the current methods used in AI-assisted malware analysis are described, while in [32] a fully unsupervised DL model is presented to proactively detect DDoS attacks. Even when a security and privacy policy is successfully developed and implemented, the security systems in use are rather static with respect to the highly dynamic threat prevention and mitigation techniques needed. In most of the cases, neither the network elements nor the security appliances support a reconfiguration framework to meet the pace of the highly dynamically changing nature of threats.

The HORSE architecture addresses these challenges, as it provides a spatially distributed AI/ML approach for security enhancement in 6G networks, closer to the source of data of interest. In this context, the implementation of Federated Learning (FL) represents a major goal towards service disaggregation and security optimization. Based on FL [28], data selection and training are performed locally, an approach that obviously protects the data privacy and offers a considerable reduction of the overhead/latency as a side positive effect. HORSE notably innovates by deploying Deep Reinforcement Learning methods, applying FL [33] and metalearning (AutoML), to meet policies for trustworthy AI and improve security strategies.

III. THE 6G LANDSCAPE

This section presents the complex landscape considered for the definition of the HORSE architecture. Starting from the 5G Service-Based Architecture (SBA) [34], we consider 6G as the evolution of 5G, and an enabler towards a new era of highly demanding services to be deployed anywhere, from anyone and at any time, with strict demands on the quality to be delivered, where openness, models sharing and the demands for high reliability, are all imposing extreme constraints in security provisioning. Assumed is an overall system willing to be human-centric although self-automated, green although capable to manage extreme data, as well as secure and trustworthy although open and dynamic. All these envisioned services must be secure by design and conceptually supported not only by the evolution of the network itself but also by adopting additional technologies, systems and

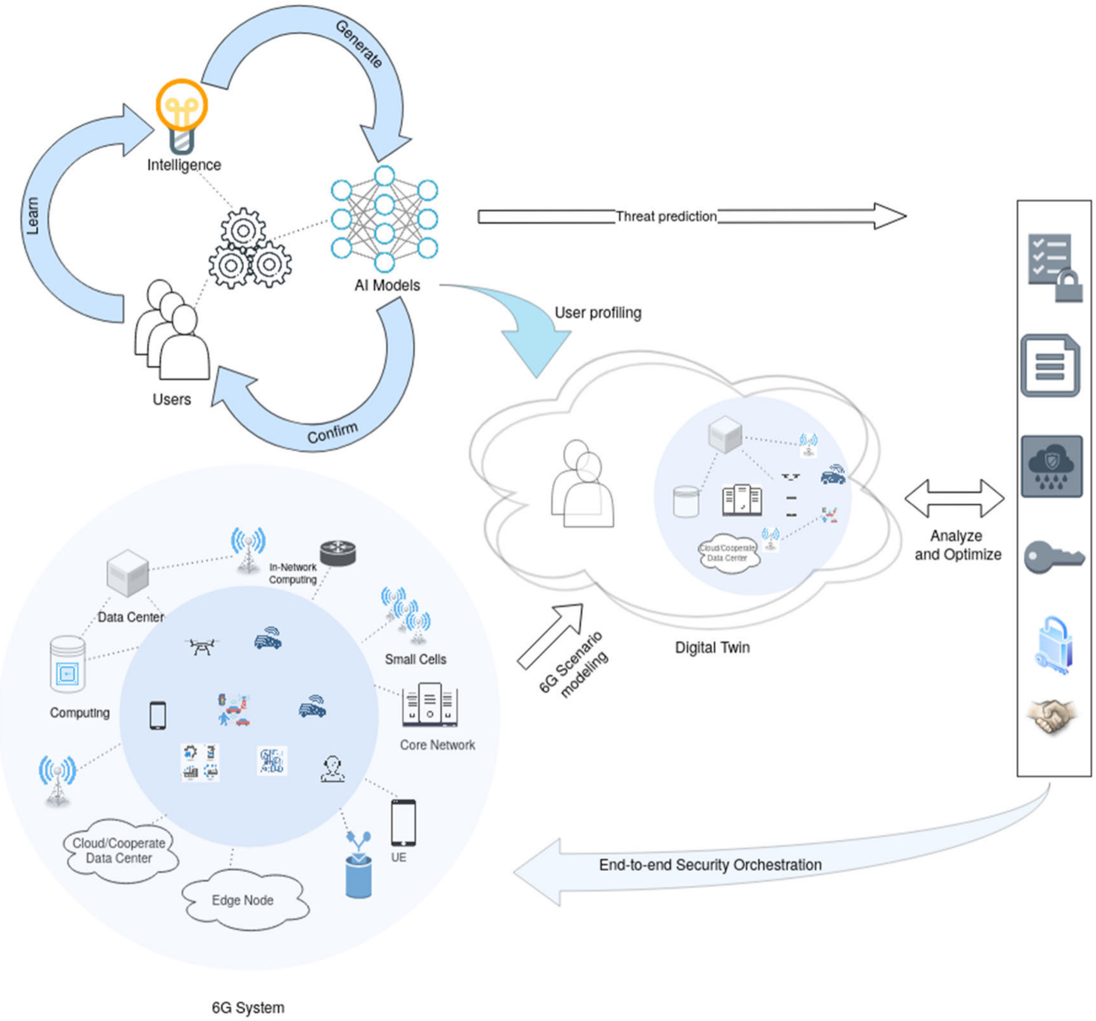


FIGURE 1. The 6G landscape.

concepts. The envisioned 6G landscape encompasses: i) edge computing and its extension to the cloud continuum concept; ii) disaggregation and virtualization of services and infrastructures; iii) utilization of DT to assist AI-based decision processes in order to proactively assess the performance of predictive strategies; iv) design of intent-based approaches to facilitate human engagement, and; v) green AI approaches where the huge demands on data processing do not hinder the deployment of smart services.

It is also worth mentioning that the envisioned 6G landscape is open, dynamic and mobile, which indeed increases the attacks surface. This assessment makes security provisioning extremely challenging, and strongly pushes for two key concepts: designing radically security approaches, starting by a clean-slate characterization and identification of potential attacks, and; building on a completely predictive scenario, that must not react but ‘‘proact’’ to maintain systems secure, in order to grant high quality for 6G services. An example of such an envisioned 6G landscape is illustrated in Fig. 1. It consists of different features covering distinct technologies, from wired to wireless and ranging from the edge up to the cloud, such as future RAN design [35], Core Network, In-Network computing, Intent communication, Centralized/Dynamic cell-less wireless network, and digital twin (DT).

IV. THE SECURITY SERVICES MANAGEMENT ARCHITECTURE

Based on the 6G landscape presented above, a high-level view of the main HORSE functional blocks, building the HORSE architecture is defined, emphasizing the key elements envisioned, namely AI secure and trustable orchestration along with platform intelligence, all supported by proper data management and impacting on human engagement and on securing the complete 6G landscape (see Fig.2). It is worth noticing, that intelligence is a central component of the HORSE architecture, applied to both the orchestration and also to the security provisioning. Orchestration operations

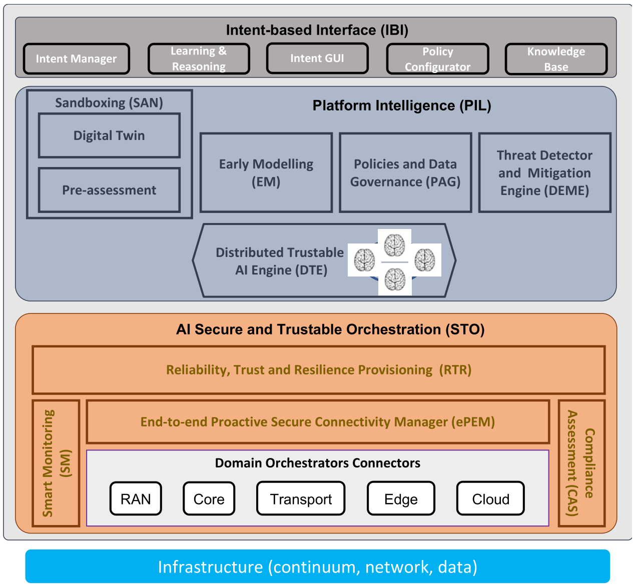

Intent-based Interface (IBI)
Intent Manager
Learning & Reasoning
Intent GUI
Policy Configurator
Knowledge Base
Sandboxing (SAN)
Digital Twin
Pre-assessment
Platform Intelligence (PIL)
Early Modelling (EM)
Policies and Data Governance (PAG)
Threat Detector and Mitigation Engine (DEME)
Distributed Trustable AI Engine (DTE)
AI Secure and Trustable Orchestration (STO)
Reliability, Trust and Resilience Provisioning (RTR)
Smart Monitoring (SM)
End-to-end Proactive Secure Connectivity Manager (ePEM)
Domain Orchestrators Connectors
RAN
Core
Transport
Edge
Cloud
Compliance Assessment (CAS)
Infrastructure (continuum, network, data)

FIGURE 2. HORSE functional blocks.

for provisioning, and restoration operations, as well as actions responding to feedback from the network, encompass orchestration of the network as well as of secure services provisioning. Hence, the intent-based orchestration function introduced in the HORSE architecture aims to automate the processing, storage and management of intents using advanced AI/ML algorithms factored in security and reliability actions and policies, which will be translated into network security functions and network resilience functions within the HORSE architecture. These functional blocks are properly interacting to define the envisioned HORSE architecture, as shown in Fig. 3.

In the proposed architecture, the goal is to interconnect the enforced security policies with existing orchestration strategies at all stages during the deployment of advanced services and applications spanning across multiple heterogeneous environments. To this end, the generated security APIs from the HORSE architecture, are properly applied in each service slice (i.e., virtual network tailored to specific service requirements), in order to ensure uninterrupted provision of security quality and policies. Novel functionalities in 6G are expected to include proactive slicing enabled by prediction of demand on one hand, and resource utilization on the other hand. Therefore, security enforcement should be flexible as well, allowing a dynamic update of the provided APIs per case according to the deployed slice.

Once the different needs and key components in the envisioned HORSE architecture are analyzed, the three main architectural modules will be presented in detail next. More specifically, the AI Secure and Trustable Orchestration (STO), responsible for endowing the 6G infrastructure with the performance, reliability and trust framework necessary to correctly orchestrate resources and deploy smart services; the Platform Intelligence (PIL), comprising the whole set of intelligent strategies and mechanisms supporting the predictive approach objective of HORSE and serving as interface to existing orchestration solutions, and; the Intent-based Interface (IBI), responsible for guaranteeing an easy user engagement into the overall landscape. Moreover, for the sake of illustration, Fig. 4. represents a preliminary mapping of the proposed HORSE functional blocks into the 6G landscape.

A. INTENT-BASED INTERFACE

The Intent-based Interface aligns the received management intents with the configured policies and translates these requirements into compatible policies using appropriate ML techniques.

The Intent GUI is a dashboard that reads the users' high-level input in text. The received intents are stored and parsed by the Intent Manager. Each intent has a specific structure that contains the necessary information to define the intent requirements and options. The Intent Manager sends the intent requirements to the policy configurator to match the adequate policies existing in the policy store, ensuring consistency with the requirements. AI and ML algorithms are used to analyze the history of executions and decisions, then predict the best decisions to take, helping the administrator understand what policies to choose. The data used in such a process will be gathered from the Smart Monitoring (SM) module.

B. PLATFORM INTELLIGENCE

The PIL module combines methodologies, procedures, and tools to enable machines and systems to operate at human-like levels of intelligence. This module uses AI/ML techniques and other tools to build a Digital Twin (DT) that reflects the current state of the physical object. An important goal of this block is to ensure a high level of synchronization between the physical and the virtual entities. The PIL module comprises the following five components:

1) SANDBOXING

The sandboxing environment supports the representation and emulation of multiple realistic situations in a "network in network" approach, based on provisioned demand, providing realistic useful data. To this end, it leverages the capacities of the network DT concept. The network DT approach will allow to emulate and experiment in a secure, controlled and realistic environment with different services, with alternative connectivity topologies and traffic paths, and with the placement of specific security network functions in different network situations, delivering information and telemetry to other PIL components. In order to support the required dynamism of a network, the network DT component orchestrates and manages the emulation environment following NFV/SDN principles. Data generated by the DT, based on network flows and device behaviors, are to be made accessible to security components, so they can perform intelligent analysis and predictions

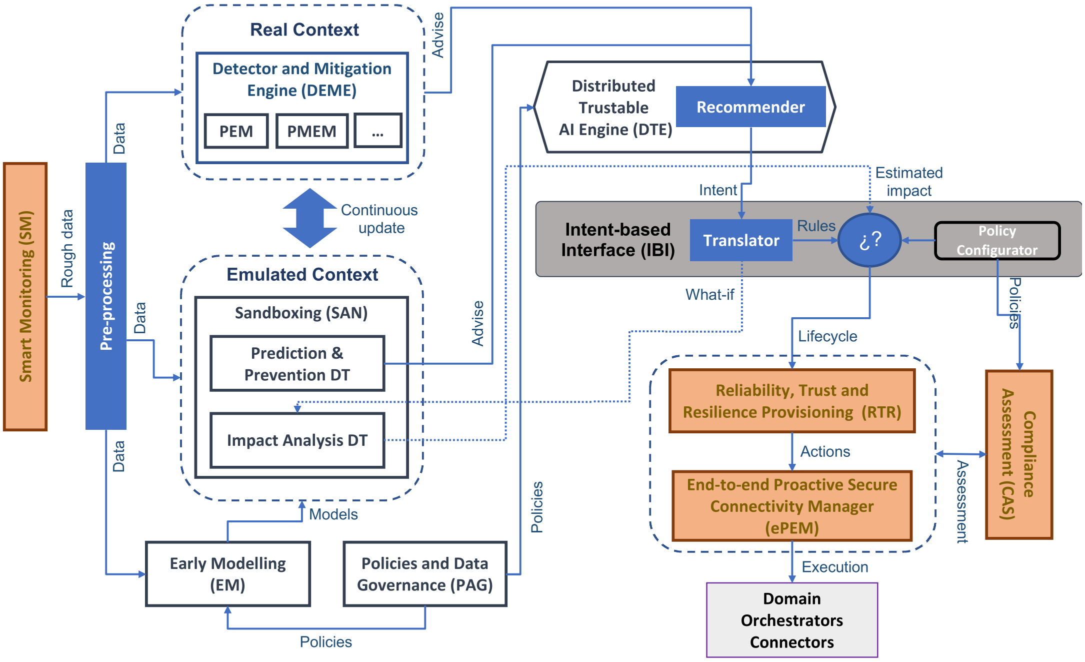

Real Context
Detector and Mitigation Engine (DEME)
PEM
PMEM
...
Advise
Data
Smart Monitoring (SM)
Rough data
Pre-processing
Continuous update
Emulated Context
Sandboxing (SAN)
Prediction & Prevention DT
Impact Analysis DT
Data
Advise
Distributed Trustable AI Engine (DTE)
Recommender
Intent
Estimated impact
Intent-based Interface (IBI)
Translator
Rules
¿?
Policy Configurator
What-if
Lifecycle
Policies
Reliability, Trust and Resilience Provisioning (RTR)
Actions
End-to-end Proactive Secure Connectivity Manager (ePEM)
Assessment
Compliance Assessment (CAS)
Execution
Domain Orchestrators Connectors
Models
Early Modelling (EM)
Policies and Data Governance (PAG)
Policies

FIGURE 3. The HORSE architecture.

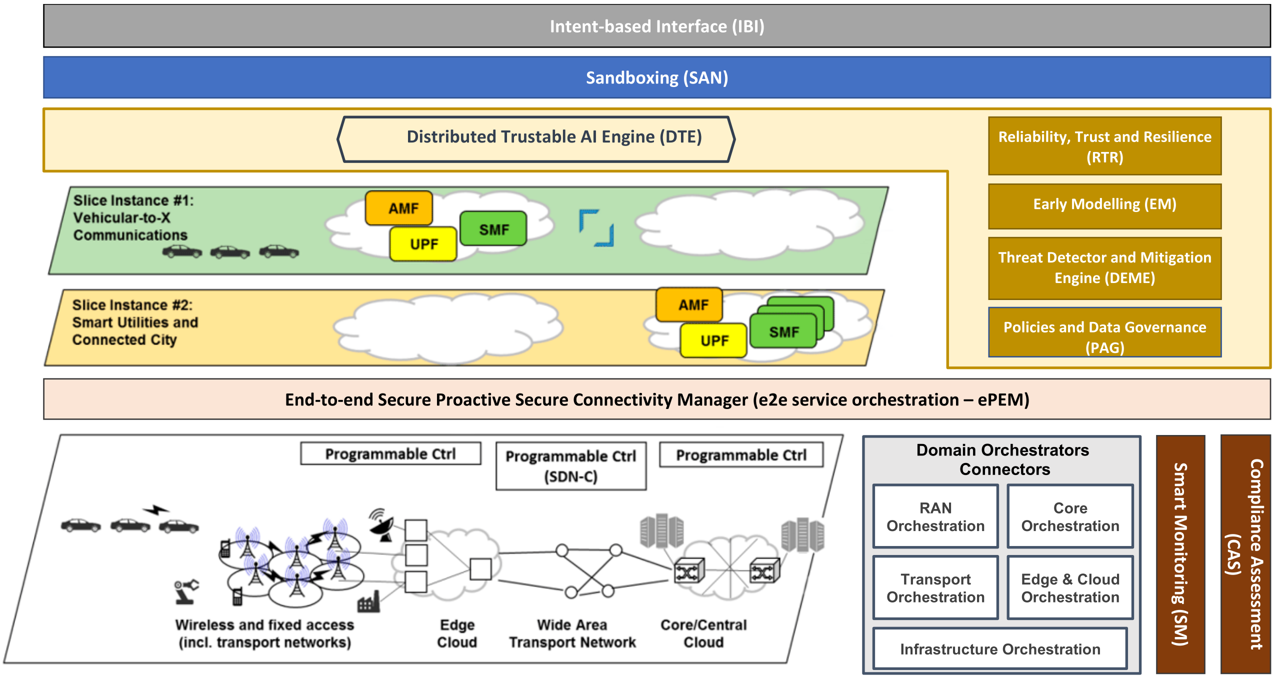

Intent-based Interface (IBI)
Sandboxing (SAN)
Distributed Trustable AI Engine (DTE)
Reliability, Trust and Resilience (RTR)
Early Modelling (EM)
Threat Detector and Mitigation Engine (DEME)
Policies and Data Governance (PAG)
Slice Instance #1: Vehicular-to-X Communications
AMF
UPF
SMF
Slice Instance #2: Smart Utilities and Connected City
AMF
UPF
SMF
End-to-end Secure Proactive Secure Connectivity Manager (e2e service orchestration – ePEM)
Programmable Ctrl
Programmable Ctrl (SDN-C)
Programmable Ctrl
Wireless and fixed access (incl. transport networks)
Edge Cloud
Wide Area Transport Network
Core/Central Cloud
Domain Orchestrators Connectors
RAN Orchestration
Core Orchestration
Transport Orchestration
Edge & Cloud Orchestration
Infrastructure Orchestration
Smart Monitoring (SM)
Compliance Assessment (CAS)

FIGURE 4. The HORSE link to the 6G field.

2) EARLY MODELLING

The Early Modelling (EM) generates the information required by the Sandboxing (SAN) to carry out, along with the Distributed Trustable Engine (DTE), its expected functionalities dealing with preliminary testing and assessment. Indeed, the logical context defined by the DT in the SAN relies on the different models to be produced by the EM. These models must map the overall 6G landscape into a logical view where, once represented in the DT, the security strategies proposed for security provisioning may be pre-assessed. It is important to notice that the EM will remain continuously active in order to proactively act to any deviation or potential issue that may come up affecting the services delivery and the overall connectivity. To this end, EM characterizes and profiles the different components to be represented in the 6G context within the DT, i.e., network infrastructure, services, data, IT resources, policies, users' behavior and threats. The outcome of this process must be useful to identifying what the real impact of any threat, disruption or change in the context may have on the services to be delivered, and consequently to help designing the predictive action to be tested and pre-assessed in the SAN before being deployed in the STO.

3) POLICIES AND DATA GOVERNANCE

The PAG component of the PIL module integrates all the required mechanisms for ensuring data quality, privacy, integrity and easy access, enabling data flows and facilitating data control, while preserving both legal and ethical data management principles. Such mechanisms include access policies, based on different attributes to fully control which stakeholders can potentially be allowed or must be denied from accessing specific data. Additionally, rules to safeguard privacy and prevent accidental exposure of personal or corporate details, encryption standards to be enforced during data transfer, and data retention policies for overseeing the lifecycle, including retention, archiving, and backup regulations, are necessary. Two different types of data are considered: users/application's data, including both, repositories of preserved data sets stored in large nodes and fresh data just collected from the IoT/IoE sources; and system data collected during monitoring purposes to feed all internal AI processes.

4) THREAT DETECTOR AND MITIGATION ENGINE

The Threat Detector and Mitigation Engine (DEME) component analyzes and processes network streams in complex and highly distributed network and infrastructure scenarios, focusing on threat detection and mitigation actions of the most dangerous attack cases, able to impact, and often paralyze, whole portions of the network for a long amount of time. The massive amount of data dynamically collected, will be pre-elaborated using advanced techniques borrowed from big-data modern applications, comprising scalable solutions, based on concurrent elaboration and micro-services dedicated deployments, multi-dimensionalities reduction techniques and innovative sketching methods applied to ML.

Finally, the mitigation actions, triggered by DEME, will allow both the operator to dynamically follow the network status and any cyber-security emergency; and the actuators to immediately deploy the foreseen action, e.g., the orchestrator to redeploy a particular connection, isolating some VNFs, redirecting some path to honeypots

5) DISTRIBUTED TRUSTABLE AI ENGINE

The DTE AI module collects various data from diverse sources of the HORSE infrastructure, and the employment of AI/ML modules to define the optimum set of policies leveraging security against all potential attacks as well as privacy rules. The DTE will provide a programming interface to offer AI models and predictions to other modules and thus, support the distributed trustable AI assisted cybersecurity tools. A series of explainable AI models are to be created, as the ability to comprehend the decision-making process of an AI model remains a central aspect of contemporary AI research and acts as a crucial element influencing trust in AI technology. This module also manages data prior to the actual training, by employing the appropriate policies for anomaly detection (tampered data) as well as data anonymization. Moreover, it takes over the compliance of the proposed solutions with the policies module.

C. AI SECURE AND TRUSTABLE ORCHESTRATION

The STO module consists of the following five components:

1) RELIABILITY, TRUST AND PROVISIONING MODULE

The Reliability, Trust and Provisioning module (RTR) provisions security and reliability services in the HORSE architecture. It performs vulnerability assessment, where security weaknesses is identified and categorized. This tool evaluates if the system is susceptible to any known vulnerabilities, it assigns severity levels to those vulnerabilities, as well as it recommends remediation or mitigation, if and whenever needed, according to the outcomes of the trustable AI engine. The goal of the threat-attack repository is to facilitate data interoperability among the various and diverse infrastructure elements of the HORSE architecture. On the other hand, the RTR also ensures data anonymization and identity protection of the HORSE end-users. It is responsible for enforcing privacy-aware policies and restrictions for data accessing. In this context, all adopted privacy policies and rules will be automatically adapted based on a continuous active learning process from monitoring of security incidents.

2) END-TO-END PROACTIVE SECURE CONNECTIVITY MANAGER

The End-to-end Proactive Secure Connectivity Manager (ePEM) manages all functions and operations required for the PIL modules, services and applications placement over the available infrastructure and for its connection to a properly configured network slice, as well as maintaining the information on all the data regarding the deployed applications, network services, and available infrastructure resources.

The ePEM also performs the following functions: i) receiving the intents from the PIL mapped into specific actions for security provisioning decided by the RTR module, and; ii) coordinating the work of all the other building blocks in the infrastructure domain to set up and to properly configure secure 6G network services, RAN, network slices, and edge computing resources. With respect to the well-known NFV and softwarized architecture, the ePEM module represents an Operations Support System (OSS) in charge of providing end-to-end secure connectivity

3) SMART MONITORING

This module collects data from the various and diverse sources of the HORSE infrastructure. It also performs the additional functions including i) retrieving data and security logs from running services and software packages, physical servers and SDN controllers running on different administrative domains; ii) implementing a data modelling/indexing schema that enable flexible management and processing of the collected data in a homogeneous manner; and; iii) permanently storing data in a metrics database to be accessed by analytics tools to perform intelligent resource management and orchestration. To achieve this entire goal, the monitoring component relies on a high performance, distributed, and scalable message queue that would allow exchange of monitoring information between publishers (running services) and subscribers (analytics tools that consume monitoring metrics).

4) COMPLIANCE ASSESSMENT

The Compliance Assessment (CAS) module supports the development and implementation of a CAS framework, which include: analysis of the regulatory framework, development of ethics guidelines to ensure a proper framework for the management and continuous monitoring of the ethical issues, transforming in this way regulatory data into meaningful regulatory intelligence. The development of a trustworthy AI system, by adopting both technical (e.g., by ensuring the implementation of "by-design" concepts within the system architecture to bring an ethical lens to what we design and build) and non-technical (e.g., ensuring stakeholder participation) methods will allow to combine methodologies, procedures, and tools and also to enable machines and systems to operate at human-like levels of intelligence.

5) DOMAIN ORCHESTRATOR CONNECTOR

The Domain Orchestrators Connector aims at providing an integrated resource stratum to the upper layers of the HORSE architecture, thus performing the proper orchestration of the network, storage and computing resources, either virtual or physical, regardless of their location. As a result, it creates an heterogenous set of resources across the computing continuum and integrates management and orchestration functionalities for all the different network sections of an end-to-end 6G system, encompassing RAN, transport, core, near edge, far edge and cloud. This concept unifies the orchestration processes among the different network segments. The Domain Orchestrators Connector implements a zero-trust model aiming at providing Trusted Execution Environments (TEE) based on Distributed Ledger Technology (DLT) in order to trustworthy integrate and securely connect highly distributed multi-domain and multi-stakeholder infrastructures.

V. CANONICAL WORKFLOWS

This subsection aims at exploring the expected functionalities the proposed security provisioning solution should deliver. To this end, specific illustrative workflows are defined. Indeed, the main objective of the so-called "canonical" workflows is to show the basic functionality of all modules in the proposed architecture while determining the operational data flow. Two different workflows are defined, describing the detection and the prediction of threats, and how the different components in the proposed architecture will interact to successfully perform. It is worth noticing that both workflows are intended to be considered as a kind of template to fuel more elaborated workflows at lower level and also to create workflows tailored to the different verticals where the 6G ecosystem may contribute to. The two proposed workflows, described as a sequence diagram, are described next.

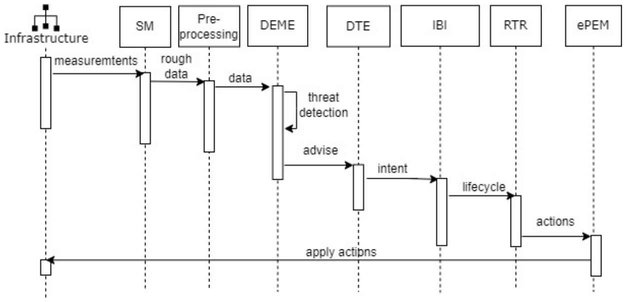


FIGURE 5. Threat-detection workflow.

A. THREAT-DETECTION WORKFLOW

The Threat Detection Workflow, sketched in Fig. 5, starts by gathering measurements from the infrastructure. The SM module is the responsible for gathering the data from the infrastructure. The collected rough data is sent to the Pre-processing module which performs normalization tasks to unify all the received data. Once normalized, the data feeds the DEME module, where efficient attacks and threats detection mechanisms are continuously running. When a threat or an attack is detected, the DEME generates an advice, suggesting a high-level description of the path to be potentially taken to deal with the detected attack or threat. The advice is received by the DTE, which generates the corresponding intent (according to a set of rules and policies already identified) that transforms into a readable layout, the previous path into specific although yet high level actions. The intent is sent to the IBI, which maps the received readable intent into a lifecycle of concrete actions, covering the whole set of steps to be taken to handle the detected attack or threat. If the generated lifecycle is aligned with several policies defined in HORSE, it is sent to the RTR, that is responsible for defining the concrete set of mitigation actions inferred from the previous lifecycle, to be deployed in the infrastructure. Finally, the set of actions are sent to the ePEM, as a playbook, which executes the required technologies and solutions in the infrastructure to properly react to the detected attack or threat triggering this workflow.

B. THREAT-PREDICTION WORKFLOW

The Threat Prediction Workflow, presented in Fig. 6, runs quite similar to the previous one, although in a different time

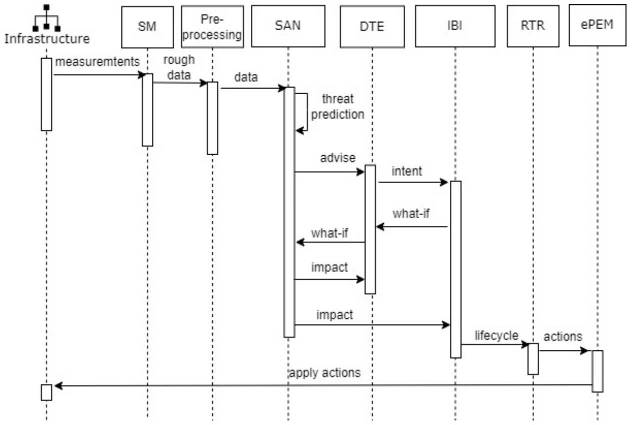


FIGURE 6. **Threat-prediction workflow.**

window, as it does not deal with detection but prediction purposes. It also starts by gathering measurements from the infrastructure, in terms of rough data, which is sent to the Pre-processing module for normalization. Unlike the previous workflow where the data is used to detect attacks and threats, in this workflow the collected data is used to predict through the SAN module. Indeed, the generated normalized data received by the SAN module, is smartly processed by the Prediction & Prevention DT. The main objective of this component is to predict a threat or an attack about to come with a certain probability. In this case, it generates an advice, also including a suggested path referring to the potential set of preventive actions to be taken. The advice is then sent to the DTE, which generates the corresponding intent (also according to a well-defined set of policies and with particular attention to the accuracy of the prediction), that translates the suggested path into a set of high-level preventive actions to be sent to the IBI module. As described for the previous workflow, the IBI module processes the received intent and generates a lifecycle of specific preventive actions, containing the entire set of steps to be taken. Unlike the detection workflow, recognized the fact that in this workflow the overall decision process will deal with estimated and non-completely accurate predictions, before being forwarded to the RTR, the lifecycle is sent to the SAN module, where the Impact Analysis DT runs the foreseen preventive actions into an emulated scenario, so a clearer overview of the real outcome of deploying such a lifecycle may be deeply observed. Indeed, the Impact Analysis DT estimates the impact of executing the proactive actions (the lifecycle) in the emulated infrastructure, handling out the estimated impact to the IBI, which processes this estimation and evaluates if it would be acceptable, according to some specific and well-defined policies. In the case the impact is acceptable, the IBI evaluates if the generated lifecycle is aligned with several policies defined in HORSE, and if so, the lifecycle is sent to the RTR. The RTR based on the received lifecycle defines the set of proactive actions to be executed in the infrastructure, to be finally deployed by the ePEM.

VI. CONCEPTUAL ANALYSIS IN ILLUSTRATIVE SCENARIOS

We envision that a security services management proposed in HORSE is to be effectively deployed in many different real world scenarios, and particularly in those demanding low latency communications, high available bandwidth, secure communications, as well as resilience and disaster recovery. These scenarios cover a wide range of application domains as smart industry, transportation, smart cities or eHealth. In this section, two illustrative scenarios are described, Light Rail Transit (LRT) and Extended Reality, in order to conceptually highlight the potential benefits and impact a HORSE-based solution may bring in. These benefits are quantified in terms of envisioned expectations (indicators).

In sum, the application scenarios are expected to from the HORSE architecture in a few distinct ways: i) improvement of business continuity and recovery, since the secure orchestration provided by the HORSE's SCO component can help to minimize the effects of security threats; ii) the improved time to react to a threat or to a threat prediction in incident response process, reducing both, the time interval between the detection of an adversary activity and the reaching of the final system state, and the time interval passed between the initiation of an adversary activity targeting scenario components and the initiation of a communication of detection, and finally; iii) minimizing the errors by applying AI models, reducing the percentage of false positive detections of threats out of the total adversary actions.

A. SECURE SMART LRT SYTEMS

LRT or Metro Operation involves the management and orchestration, with high availability, of several systems, applications and end to end services, supported by equipment that typically are deployed on tram stops, trams and in the Command Center. Usually, these Command Centers are deployed in private networks, for security reasons and are located in the Operator premises, by latency reasons. A key challenge in LRT is the use of low latency communications and high available bandwidth for video, infotainment and data exchanges between the trams, stops and the command centre. Moreover, it is expected that LTR will benefit from new 6G networks paradigms, related to communications, disaster recovery, security, and resilience. The geographically distributed operation (even supported by cloud solutions) will pose a significant impact on both, overall availability and decision support capabilities. Finally, in terms of analytics and statistical computations related to operation, nowadays, operators are facing some restrictions, related to communications and latency limitations, meaning that data is only validated at the end of the day. Through 6G networks a better performance can be achieved allowing statistical operation and decisions capabilities in almost real time.

The HORSE architecture, will provide cyber security functionalities, in the different LRT scenarios, i.e. Public Announcement, CCTV, Help-point and Maintenance agents.

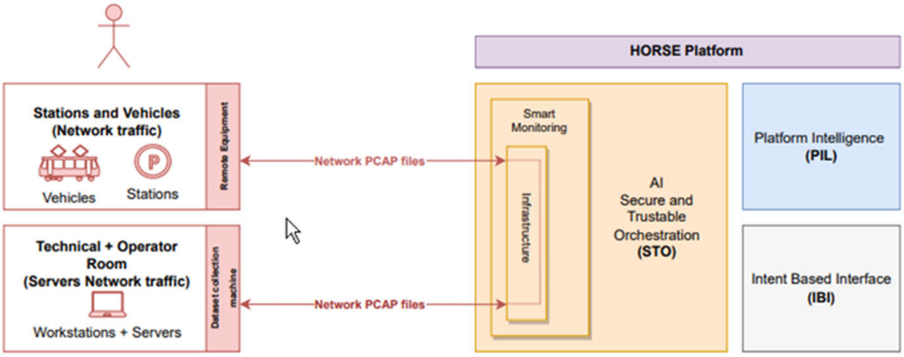


FIGURE 7. The SS-LRT illustrative scenario.

Fig. 7 depicts the main modules of the HORSE architecture that can be involved in this scenario, which are: i) IBI module to allow configuration and event visualization; ii) SM module to collect data from systems onboard, stations and technical room on 6G networks; iii) PIL module comprising all required mechanisms to support the detection/prediction of events, including DEME module for the detection of threats from real-time network traffic against the AI models elaborated by the EM module (according to the configuration defined in the IBI, DEME alarms the operator or block protocol usage on that network until proper validation); iv). DTE module to assure services security and performance, optimized with AI/ML mechanisms, and finally; v), STO module to assure security and reliability.

By adopting HORSE architecture, LRT is expected to substantially improve resilience and disaster recovery compared with current private networks. When a threat is detected, the HORSE secure orchestrator will launch the actions to properly react. These actions will be previously assessed by the DT to evaluate the expected performance in such highly distributed scenario. Moreover, it is also expected to improve the availability of remote operations and to provide to the decision support system the ability to calculate the operation statistics data almost in real-time.

B. REMOTE RENDERING TO POWER XR INDUSTRIAL

Multiuser XR (Extended Reality) multi-sites collaboration provides Industry 4.0 professionals with the means to solve complex issues in a much easier and efficient way, giving them the opportunity to meet in a virtual common space to collaborate and share virtual 3D objects. However, industrial espionage is a growing threat, requiring proactive, resilient and secure systems, which protect valuable data and intellectual property from unauthorized access ensuring a free flow of information throughout all actors involved. In this context, a Remote Rendering to Power XR Industrial system can benefit from the HORSE architecture in terms of a secure, reliable and orchestrated continuum, addressing the following challenges: sharp and secure offloading renderings, multiuser remote rendering approaches, and secure multiuser communication and interaction. To face the above-mentioned application challenges, the HORSE architecture will provide the means to address specific requirements the service poses on the network infrastructure, in terms of: i) very high bandwidth, to transmit and render very complex 3D models, and; ii) ultra-low latency, to support multi-users human-machine interaction and dense situations in the context of 6G. This illustrative scenario will consider a multiuser environment where different professional stakeholders can interact and teleport to another context that are completely virtual or mixed. The service will offer a resilient and secure environment, professional users located at different sites and leveraging XR technology can benefit from, as depicted in Fig. 8.

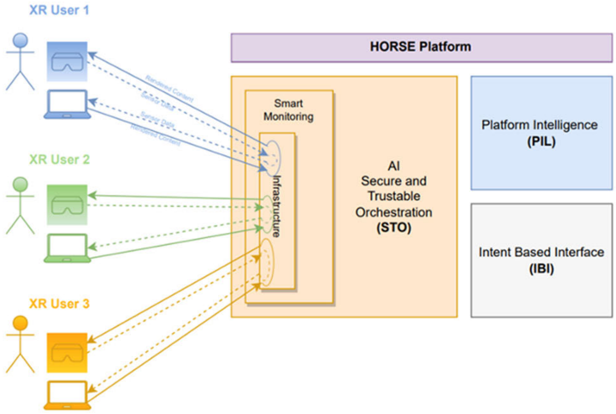


FIGURE 8. The remote rendering to power XR illustrative scenario.

The main rationale within the service is that supporting these key benefits sits on simplifying the use of XR applications. To this end, every app can be accessed via the internet through one client app or simple browser login and then be streamed on demand. Via the platform the applications are globally available at any time and no updating or maintenance is necessary. By this, engineers will be able to visualize and work with 3D CAD data in an XR environment while they can communicate with each other. Taking prototyping, factory planning, quality control, and technical education to the next level without the need to compromise the quality of the data visualized.

By adopting the HORSE architecture, it is expected that the Remote Rendering to Power XR Industrial system will improve the prototyping and design processes reducing costs errors and decreasing the product release time, speeding up the time-to-market of the products.

VII. CONCLUSION

This paper proposed a novel reference architecture for future 6G wireless and computing ecosystems which provides a human-centric approach to security workflows, by enabling top-down, bottom-up and end-to-end security solutions. The proposed architecture is expected to advance current solutions, defining a smart and adaptive security layer which will make use of AI-methods for both, improving response and resilience of systems (early detection of threats), as well as identifying and correcting vulnerabilities, in a sandbox environment, by attacking the systems predicted to be exposed. The security layer was designed to reduce the incident disruption and response time by providing improved predictive orchestrations.

The potential development of the HORSE architectural solution was outlined in industrial and transport environments where low latency communications, high available bandwidth, security and resilience is requested. More specifically, two scenarios were proposed to illustrate the HORSE architecture, Secure Smart LRT Systems and Remote Rendering to Power XR Industrial. For both scenarios, requirements, HORSE framework adoption, and an estimation of the potential benefits were discussed in terms of envisioned indicators. Future work will address the implementation of the components foreseen by the HORSE architecture and the verification of the proposed indicators in the two presented real-world scenarios

REFERENCES

[1] E.-K. Hong, I. Lee, B. Shim, Y.-C. Ko, S.-H. Kim, S. Pack, K. Lee, S. Kim, J.-H. Kim, Y. Shin, Y. Kim, and H. Jung, "6G R&D vision: Requirements and candidate technologies," *J. Commun. Netw.*, vol. 24, no. 2, pp. 232–245, Apr. 2022, doi: 10.23919/JCN.2022.000015.

[2] Y. Siriwardhana, P. Porambage, M. Liyanage, and M. Ylianttila, "AI and 6G security: Opportunities and challenges," in *Proc. Joint Eur. Conf. Netw. Commun. 6G Summit (EuCNC/6G Summit)*, Porto, Portugal, Jun. 2021, pp. 616–621, doi: 10.1109/EuCNC/6GSummit51104.2021.9482503.

[3] S. Majumdar, R. Trivisonno, W. Yi Poe, and G. Carle, "Distributing intelligence for 6G network automation: Performance and architectural impact," in *Proc. IEEE Int. Conf. Commun.*, Jun. 2023, pp. 6224–6229, doi: 10.1109/ICC45041.2023.10279655.

[4] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, "5G security: Analysis of threats and solutions," in *Proc. IEEE Conf. Standards Commun. Netw.*, 2017, pp. 193–199.

[5] S. H. A. Kazmi, R. Hassan, F. Qamar, K. Nisar, and A. A. A. Ibrahim, "Security concepts in emerging 6G communication: Threats, countermeasures, authentication techniques and research directions," *Symmetry*, vol. 15, no. 6, p. 1147, May 2023, doi: 10.3390/sym15061147.

[6] V.-L. Nguyen, P.-C. Lin, B.-C. Cheng, R.-H. Hwang, and Y.-D. Lin, "Security and privacy for 6G: A survey on prospective technologies and challenges," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 4, pp. 2384–2428, 4th Quart., 2021, doi: 10.1109/COMST.2021.3108618.

[7] X. Zhu and C. Jiang, "Creating efficient integrated satellite-terrestrial networks in the 6G era," *IEEE Wireless Commun.*, vol. 29, no. 4, pp. 154–160, Aug. 2022, doi: 10.1109/MWC.011.2100643.

[8] X. Zhu and C. Jiang, "Integrated satellite-terrestrial networks toward 6G: Architectures, applications, and challenges," *IEEE Internet Things J.*, vol. 9, no. 1, pp. 437–461, Jan. 2022, doi: 10.1109/JIOT.2021.3126825.

[9] P. Tedeschi, S. Sciancalepore, and R. Di Pietro, "Satellite-based communications security: A survey of threats, solutions, and research challenges," *Comput. Netw.*, vol. 216, Oct. 2022, Art. no. 109246, doi: 10.1016/j.comnet.2022.109246.

[10] B. Mao, J. Liu, Y. Wu, and N. Kato, "Security and privacy on 6G network edge: A survey," *IEEE Commun. Surveys Tuts.*, vol. 1, pp. 1–16, 2nd Quart., 2023, doi: 10.1109/COMST.2023.3244674.

[11] F. Naeem, M. Ali, G. Kaddoum, C. Huang, and C. Yuen, "Security and privacy for reconfigurable intelligent surface in 6G: A review of prospective applications and challenges," *IEEE Open J. Commun. Soc.*, vol. 4, pp. 1196–1217, 2023, doi: 10.1109/OJCOMS.2023.3273507.

[12] W. Khalid, M. Atif Ur Rehman, T. Van Chien, Z. Kaleem, H. Lee, and H. Yu, "Reconfigurable intelligent surface for physical layer security in 6G-IoT: Designs, issues, and advances," *IEEE Internet Things J.*, vol. 11, no. 2, pp. 3599–3613, Jan. 2024, doi: 10.1109/JIOT.2023.3297241.

[13] H. Ayaz, M. Waqas, G. Abbas, Z. H. Abbas, and M. Bilal, "Multiple re-configurable intelligent surfaces based physical layer eavesdropper detection for V2I communications," *Phys. Commun.*, vol. 58, Jun. 2023, Art. no. 102074, doi: 10.1016/j.phycom.2023.102074.

[14] Y. Liu, W. Yi, Z. Ding, X. Liu, O. A. Dobre, and N. Al-Dhahir, "Developing NOMA to next generation multiple access: Future vision and research opportunities," *IEEE Wireless Commun.*, vol. 29, no. 6, pp. 120–127, Dec. 2022, doi: 10.1109/MWC.007.2100553.

[15] S. Pakravan, J. Y. Chouinard, X. Li, M. Zeng, W. Hao, Q. V. Pham, and O. A. Dobre, "Physical layer security for NOMA systems: Requirements, issues, and recommendations," *IEEE Internet Things J.*, vol. 10, no. 24, pp. 21721–21737, Dec. 2023, doi: 10.1109/JIOT.2023.3296319.

[16] Y. Zuo, J. Guo, N. Gao, Y. Zhu, S. Jin, and X. Li, "A survey of blockchain and artificial intelligence for 6G wireless communications," *IEEE Commun. Surveys Tuts.*, vol. 25, no. 4, pp. 2494–2528, 4th Quart., 2023, doi: 10.1109/COMST.2023.3315374.

[17] C.-X. Wang, X. You, X. Gao, X. Zhu, Z. Li, C. Zhang, H. Wang, Y. Huang, Y. Chen, H. Haas, J. S. Thompson, E. G. Larsson, M. D. Renzo, W. Tong, P. Zhu, X. Shen, H. V. Poor, and L. Hanzo, "On the road to 6G: Visions, requirements, key technologies and testbeds," *IEEE Commun. Surveys Tuts.*, pp. 1–17, 2nd Quart., 2023, doi: 10.1109/COMST.2023.3249835.

[18] B. Mao, Y. Kawamoto, and N. Kato, "AI-based joint optimization of QoS and security for 6G energy harvesting Internet of Things," *IEEE Internet Things J.*, vol. 7, no. 8, pp. 7032–7042, Aug. 2020, doi: 10.1109/JIOT.2020.2982417.

[19] S. Dang, O. Amin, B. Shihada, and M.-S. Alouini, "What should 6G be?" *Nature Electron.*, vol. 3, no. 1, pp. 20–29, Jan. 2020, doi: 10.1038/s41928-019-0355-6.

[20] K. F. Ystgaard and K. de Moor, "Bring the human to the network: 5G and beyond," in *Proc. 28th Int. Conf. Telecommun. (ICT)*, Jun. 2021, pp. 1–7, doi: 10.1109/ICT52184.2021.9511537.

[21] D. Simeonidou and R. Nejabati, "Human-centric networking: From device-centric 5G networks to full cyber-physical convergence in 6G," in *Proc. Eur. Conf. Opt. Commun. (ECOC)*, Bordeaux, France, Sep. 2021, pp. 1–2, doi: 10.1109/ECOC52684.2021.9605913.

[22] A. Seeam, O. S. Ogbeh, S. Guness, and X. Bellekens, "Threat modeling and security issues for the Internet of Things," in *Proc. Conf. Next Gener. Comput. Appl.*, Sep. 2019, pp. 1–8, doi: 10.1109/NEXTCOMP.2019.8883642.

[23] K. Tuma, R. Scandariato, M. Scandariato, and C. Scandariato, *Towards Security Threats That Matter*, vol. 10683. Cham, Switzerland: Springer, 2018.

[24] *MITRE ATT&CK*. Accessed: Jan. 2024. [Online]. Available: https://attack.mitre.org

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

[26] P. Porambage, G. Gur, D. P. M. Osorio, M. Liyanage, A. Gurtov, and M. Ylianttila, "The roadmap to 6G security and privacy," *IEEE Open J. Commun. Soc.*, vol. 2, pp. 1094–1122, 2021, doi: 10.1109/OJCOMS.2021.3078081.

[27] S. Shen, C. Yu, K. Zhang, J. Ni, and S. Ci, "Adaptive and dynamic security in AI-empowered 6G: From an energy efficiency perspective," *IEEE Commun. Standards Mag.*, vol. 5, no. 3, pp. 80–88, Sep. 2021, doi: 10.1109/MCOMSTD.101.2000090.

[28] D. C. Nguyen, M. Ding, P. N. Pathirana, A. Seneviratne, J. Li, and H. V. Poor, "Federated learning for Internet of Things: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 3, pp. 1622–1658, 3rd Quart., 2021, doi: 10.1109/COMST.2021.3075439.

[29] E. Jayabalan and R. Pugazendi, "Generative adversarial networks for secure data transmission in wireless network," *Intell. Autom. Soft Comput.*, vol. 35, no. 3, pp. 3757–3784, 2023, doi: 10.32604/iasc.2023.031200.

[30] P. Dixit and S. Silakari, "Deep learning algorithms for cybersecurity applications: A technological and status review," *Comput. Sci. Rev.*, vol. 39, Feb. 2021, Art. no. 100317, doi: 10.1016/j.cosrev.2020.100317.

[31] M. Abdelsalam, M. Gupta, and S. Mittal, "Artificial intelligence assisted malware analysis," in *Proc. ACM Workshop Secure Trustworthy Cyber-Physical Syst.*, Apr. 2021, pp. 75–77, doi: 10.1145/3445969.3450433.

[32] E. Paolini, L. Valcarenghi, L. Maggiani, and N. Andriolli, "Real-time clustering based on deep embeddings for threat detection in 6G networks," *IEEE Access*, vol. 11, pp. 115827–115835, 2023, doi: 10.1109/ACCESS.2023.3325721.

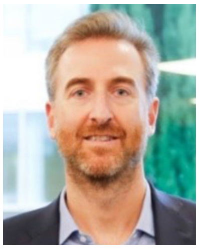
[33] M. Venkatasubramanian, A. H. Lashkari, and S. Hakak, "IoT malware analysis using federated learning: A comprehensive survey," *IEEE Access*, vol. 11, pp. 5004–5018, 2023, doi: 10.1109/ACCESS.2023.3235389.

[34] X. D. Duan, X. Y. Wang, L. Lu, N. X. Shi, C. Liu, T. Zhang, and T. Sun, "6G architecture design: From overall, logical and networking perspective," *IEEE Commun. Mag.*, vol. 61, no. 7, pp. 158–164, Jul. 2023, doi: 10.1109/MCOM.001.2200326.

[35] J. Chen, X. Liang, J. Xue, Y. Sun, H. Zhou, and X. Shen, "Evolution of RAN architectures towards 6G: Motivation, development, and enabling technologies," *IEEE Commun. Surveys Tuts.*, pp. 1–16, 2nd Quart., 2024, doi: 10.1109/comst.2024.3388511.

EVA RODRIGUEZ received the B.Sc. degree in telecommunication engineer from the Universitat Politècnica de Catalunya (UPC), in 2001, and the Ph.D. degree in computer science from Universitat Pompeu Fabra (UPF), in 2007. She has been with the Department of Computer Architecture, UPC, as an Assistant Professor, since 2005. From 2002 to 2005, she was a Researcher with the Department of Technology, UPF. She has participating in several national projects and EU contracts in the areas of security and multimedia information management. She has authored several papers, published in international journals and conferences. Her research interests include security, privacy, multimedia information retrieval, and object recognition.

XAVI MASIP-BRUIN received the M.Sc. and Ph.D. degrees in telecommunications engineering from the Technical University of Catalonia. He is currently a Full Professor with UPC and the Director of the Advanced Network Architectures Laboratory (CRAAX). His publications include more than 200 papers in international refereed journals and conferences. He has participated and/or led many national and regional projects and EU contracts and has also led contracts with industry. In 2013, he has co-founded MATPOL Technologies, a Bay Area based start-up. His contributions were recognized with the 2016 IBM Faculty Award. He has chaired and co-chaired many international conferences, such as ONDM, WWIC, NOC, Saconet, Med-Hoc-Net, IEEE IWQoS, and DRCN. He serves as an Editor for the *Optical Switching and Networking* (OSN) and *Computer Communications*.



JOSEP MARTRAT received the degree in telecommunication engineering from the Universitat Politècnica de Catalunya (UPC). He is currently the Head of smart network and edge computing with Eviden Research and Innovation, an Atos business. He has participated in several collaborative research projects in area of edge-cloud and software networks. He has coordinated BonFIRE research initiative about designing, building, and operating a multi-cloud facility for experimentation with hybrid clouds (public and private). He also coordinated 5GTANGO project about agile network service development and deployment on software networks that released an NFV-based service development kit, a validation and verification (V&V) framework for NFV testing, and a service platform with advance MANO functionalities. He coordinated Affordable5G project about roll-out of 5G SA private networks following an Open RAN architecture. He is currently a Technical Manager of HORSE SNS research project about cybersecurity challenges to provide resilient services for future 6G wireless and computing systems. His research interests include the study of cloud and edge technologies, network virtualization (SDN/NFV), and 5G private networks.

RODRIGO DIAZ received the master's degree in computer science from the Universitat Autònoma de Barcelona, in 1995. He is a distinguished professional in the field of cybersecurity. Since 2010, he has been with the helm of the Cybersecurity Team, Research and Development Group, Spain. In February 2015, he joined the esteemed Atos Scientific Community, an elite community comprising the top 100 scientific minds within the organization. Since 2016, he has been held membership in the Atos Expert Community, where he contributes his expertise to the cybersecurity domain. Transitioning to the Security Unit in 2009 marked a pivotal moment in his career journey. From then on, he has played key roles as a coordinator and a technical manager in numerous projects funded under the FP7, H2020, and HE frameworks. Prior to his leadership role, he was a Senior Engineer with the Aerospace and Communications Unit, Atos Research and Innovation Department, Barcelona, until 2009. During this period, he played a pivotal role as a Technical Manager in various co-funded projects by prestigious entities, such as the European Commission, European Space Agency, and European Global Navigation Satellite Systems Agency. His contributions spanned diverse domains including satellite communications, satellite navigation, aeronautics, and sensor networks. His dedication to advancing cybersecurity solutions, his multifaceted expertise together with his versatility and proficiency in cutting-edge technology fields have solidified his reputation as a trusted leader and an innovator in the field.

ADMELA JUKAN (Fellow, IEEE) was the Dean of Studies for a joint degree program between computer science and engineering, IST, from 2017 to 2019. She is currently the Chair Professor of Communication Networks, Technische Universität Braunschweig, Germany. She was a recipient of the Award of Excellence for the BMBF/CELTIC Project "100Gb Ethernet." She received the IBM Innovation Award, in 2009. She was elected as the Chair of the IEEE Optical Network Technical Committee, ONTC, from 2014 to 2015. She has chaired and co-chaired several international conferences, including IEEE/ACM IWQoS, IEEE ANTS, IFIP ONDM, IEEE ICC, and IEEE GLOBECOM. She serves as a Senior Editor for IEEE Journal of Selected Areas in Communications. She is the Co-Editor-in-Chief of the *Optical Switching and Networking* (OSN) (Elsevier). From 2015 to 2017, she was elected as a Distinguished Lecturer of the IEEE Communications Society.

FABRIZIO GRANELLI (Senior Member, IEEE) is a Full Professor with the Department of Information Engineering and Computer Science (DISI), University of Trento, Italy. He was a Visiting Professor with the State University of Campinas, Brazil, and The University of Tokyo, Japan. He is the author or co-author of more than 270 papers published in international journals, books, and conferences. He was an IEEE ComSoc Distinguished Lecturer, from 2012 to 2015 and 2021 to 2023 (four terms); the ComSoc Director for Online Content, from 2016 to 2017; a Delegate for Education at DISI, from 2015 to 2017; and the IEEE ComSoc Director for Educational Services (2018–2019) and Conference Development (2022–2023). He was the General Chair or the TPC Chair of several prestigious IEEE conferences, such as IEEE Globecom, IEEE NFV-SDN, and IEEE CAMAD. He has chaired several symposia at IEEE ICC and Globecom.

PANAGIOTIS TRAKADAS received the Dipl.-Ing. degree in electrical and computer engineering and the Ph.D. degree from the National Technical University of Athens (NTUA). He is currently an Associate Professor with the National and Kapodistrian University of Athens. He has been actively involved in many EU FP7 and H2020 research projects. He has published more than 170 papers in magazines, journals, and conference proceedings. His research interests include the fields of wireless and mobile communications, wireless sensor networking, network function virtualization, and cloud computing. He is a Reviewer in several journals, including IEEE Transactions on Communications and IEEE Transactions on Electromagnetic Compatibility.

GEORGE XILOURIS received the B.Sc. degree in physics from the University of Ioannina, in 1999, and the M.Sc. degree in automation control systems from the National Technical University of Athens (NTUA), in 2001. He is currently working in the Ph.D. at the National Technical University of Athens (NTUA). He has been a Research Scientist (Grade C) with the Institute of Informatics and Telecommunications, NCSR "Demokritos," and the Head of the NCSRD Networks Operation Center (NOC), since 2021. He has been an Active Research Associate of Media Net Laboratory, National Centre of Scientific Research "Demokritos," since 2000. He has participated in numerous EU-funded and national funded projects, collaborating with various academia and enterprises with presentations and publications at international conferences, scientific journals, and book chapters. He has strong technical and research expertise in the fields of network virtualization and management, programmable networks, cloud networks, satellite networks, media delivery technologies and performance evaluation of IT services. He is the author/co-author of more than 80 scientific papers in international journals, technical books, and book chapters, numbering at least 1302 citations and H-index of 20.