iTrust6G: Zero-Trust Security for 6G Networks

Mir Ghoraishi*, Muhammad Shuaib Siddiqui†, Maxime Compastié†, Saber Mhiri†, Christos Ntanos‡, Michael Kontoulis‡, Diego R. Lopez§, Antonio Lioy¶, Evangelos Markakis‖**, Sheeba Backia Mary Baskaran††,
*Gigasys Solutions SL, Malaga, Spain. – †i2CAT Foundation, Barcelona, Catalonia, Spain.
‡National Technical University of Athens, Athens, Greece. – §Telefonica I+D, Madrid, Spain.
¶Politecnico di Torino,Turin, Italy.– ‖Adrestia, Heraklion, Creete, Greece.
**Hellenic Mediterranean University, Heraklion, Creete, Greece. – ††Lenovo, Oberursel, Germany.

***Abstract*—The emergence of 6G networks is expected to bring forth a host of new technological advancements such as integrated radio systems, further network softwarisation, collaborations across multiple vendors, and artificial intelligence-led network governance. These developments are likely to expand the current scope of security threats by involving additional specialised stakeholders, thus requiring more advanced and multi-layered security measures. In this paper, we present iTrust6G's multipronged approach for enabling "zero-trust" security for 6G networks. Our approach exploits a multi-faceted trust evaluation accounting for security posture of entities interacting with the network, threat intelligence sharing for fostering collaboration, and security orchestration for maintaining the security stance. A system security architecture is proposed that leverages zero-trust principles to ensure a end-to-end trustworthy 6G system. Furthermore, a set of use-cases serving as evaluation playground for this reference architecture is proposed in the light of the next generation of software networks.**

***Index Terms*—B5G & 6G Networks, Security & Privacy, Zero-trust, Cyber-threat Intelligence, Security Orchestration, data-driven networks.**

I. Introduction

Communications in the 2030s will be heavily influenced by 6G technology and its system architecture, offering significant potential and opportunity to support wide diversity of services. The 6G era will be about connecting the physical, and digital realms to provide humans with new experiences by augmenting our intelligence, enabling new and immersive virtual environments, and controlling automations systems and life-like automatons of the 2030s. One of the key prerequisites to realising the full potential and benefits of 6G will be cyber resilience, alongside secure and trustworthy services. This implies the adoption of a security architecture able to intelligently conduct a trustable and secure management of communication services coping with several constraints:

- **the openness and involvement of multiple stakeholders**, due to operation of multi-vendor and open source network services on an infrastructure disaggregated on the cloud continuum [1], [2],
- **the dynamism of the network**, due to the adoption of AI-driven solutions in telecom operation complicating the definition of a perimeter of assets to protect while introducing a new threat surface [3], [4],
- **the heterogenity** of infrastructure, interfaces and physical layer, having already challenged security management methods [5], [6].

The iTrust6G [7] project introduces a unified and intelligent security architecture for distributed networks that spans across cloud and administrative domains, capable of addressing the security needs of advanced 6G applications.

More specifically, we aim to design and develop a network architecture and supporting enablers that conform to zero-trust [8] (ZT) principles, enhancing the trustworthiness of 6G networks. The project will exploit AI/ML for security management purposes, (enacting security automation and contribute to the security of the service orchestration), trust management (via the trust assessment process), and at the control layer (for threat detection and mitigation purpose). The project also considers exploiting security orchestration to maintain 6G applications in a trustworthy deployment all along their operation via an active detection and mitigation of threats. iTrust6G's added value is the pervasiveness of the monitoring and actuation capabilities based on security programmability. The project aims to specify, develop, and integrate intent-based security policies engine, for explainable and automated E2E security orchestration and to model trust aspects of the 6G platform and its entities (including 3rd parties), as well as express trust requirements and threat assessment strategies in natural language and capturing them in a well-defined intent model.

To this end, in this paper we present an overview of the iTrust6G Horizon Europe project. We detail iTrust6G's conceptual architecture, and the advancement from the state of the art needed to meet the needed architectural enablers. The remainder of this paper is organised as follows: Section II presents iTrust6G security architecture while Section III justifies its foundation in contrast to the current state of the art. Several use-cases are stated in Section IV to illustrate how this architecture shall extend security operation. We finally conclude in Section V.

II. iTrust6G Architecture

The zero trust (ZT) security model addresses the issue of the complexity of the threat surface by never making assumptions about trustworthiness (never-trust, always-verify) [9], [10], [8], [11]. In practice, within a zero-trust architecture (ZTA) secure network, access to resources (data, devices, and services) is granted only to authorised and approved subjects. ZTA is founded on an identity-centric approach, which is based on the execution of policy-driven authorisation at runtime, combined

with defence-in-depth security principles. In this section, we detail how iTrust6G plans a conceptual architecture endhorse ZT principles to deliver a security and trust management in 6G architecture.

A. Scientific and Technical Objectives

iTrust6G contemplates the five scientific and technical objectives to elaborate a security architecture enforcing trustworthiness in the next generation of mobile networks:

1) The design of an End-to-End system security architecture that capitalises on zero-trust principles to enable a trustworthy 6G service management platform, addressing dynamic network and application-level security requirements.
2) The exploit of AI to detect novel threats from operated assets and generate pertinent cyber threat intelligence enacting their proactive protection.
3) The conception of novel Trust Algorithms (TA) exploiting AI integrated into trust management system (TM) accounting for forensics evidence.
4) The design and implementation of intelligent solutions for AI-driven security orchestration, across extreme edge, edge and public clouds (across the continuum) exploiting programmability models for pervasive enforcement.
5) The specification, development, and integration of intent-based security policies/engine, for explainable and automated E2E security orchestration.

B. High-level Architecture Overview

Figure 1 shows an overview of the iTrust6G framework, where the existing B5G infrastructure is represented in grey, while the value-added components of iTrust6G are highlighted (in blue boxes and black arrows). The framework identifies three main stakeholder roles, i.e., 1) End Users, 2) Infrastructure Providers/Hosts and 3) Service Providers, each belonging to distinct administrative domains. The iTrust6G building blocks span across three domains: infrastructure, network service, and applications. The main architectural pillars of iTrust6G are:

- **Continuous evaluation of trust** is enabled through exploitation of AI/ML techniques to detect and monitor anomalous occurrences and detection of threats despite the complexity of multi-infrastructure and multi-tenant environments in 6G. This concept is integral to the trust evaluation and access control domain process, in the trust management plane of the architecture.
- **Cyber-threat intelligence involvement** will allow an up-to-date threat assessment for the continuous protection of network assets. From a trust perspective, this will enable multiple tenant to collaborate to improve their threat detection and mitigation, enacting a more precise trust assessment and improvement via inter-stakeholders collaboration.
- **End-to-end (E2E) security orchestration** will holistically enable the analysis, planning and enactment of remediation actions, while being accessible to human operators through explainability and intent-based security specification. This materialises in the security management plane and administration plane of the framework architecture.
- **Security programmability** will increase the visibility for resource monitoring and the pervasiveness of countermeasures enforcement on the cloud continuum infrastructure.

III. iTrust6G Foundation & Components

As outlined earlier, and despite steady progress on availability of new security features from 3GPP, ETSI, NGMN etc, a holistic vision of zero-trust within cellular networks has yet to emerge. Although the transition towards zero trust represents a major operational step change for the telecom industry, the new requirements and functionalities introduced in the 5G specifications are already aligned with many of the zero trust tenets. However, existing ZTA approaches may not overcome some specific security challenges faced by 6G networks, such as (i) the massive distribution of assets interacting with the network (e.g. IoT devices) necessitating an massive workload for posture scrutinisation and (ii) the involvement of multiple administrative domains cannot satisfy the current logically centralised trust management and require decentralisation. iTrust6G aims to go beyond the current state of the art of 6G security architecture by building upon current standards and addressing open gaps/security challenges. This will be achieved by enhancing the 6G security framework by embedding ZT architectural and AI components illustrated by Figure 2, and that we describe in the remainder of this section.

a) Continuous Diagnostics and Mitigation (CDM): CDM focuses on dynamically searching for threats and vulnerabilities. It essentially covers four aspects of security: asset management, identity management, network security management and, data protection management. The CDM system is one of the auxiliary systems that the policy engine may use when rendering policy decisions. The dynamic nature of enterprise assets requires a separate system to monitor the current state and ensure that the accessed resources are valid. For example, if a critical OS patch has not yet been applied to a resource, then access will be denied even if the actor is authorised to access the resource.

In iTrust6G, the CDM must evolve by investigating mechanisms that can enhance the overall effectiveness of its approach, improving threat detection, vulnerability management, and incident response capabilities, and adopt:.

- Machine Learning and Artificial Intelligence: Developing and integrating machine learning and artificial intelligence algorithms into CDM systems can significantly improve threat detection and response capabilities. These algorithms can analyse large volumes of data, identify patterns, and adapt to evolving threats, enabling the system to detect and respond to security incidents more effectively than traditional rule-based systems.

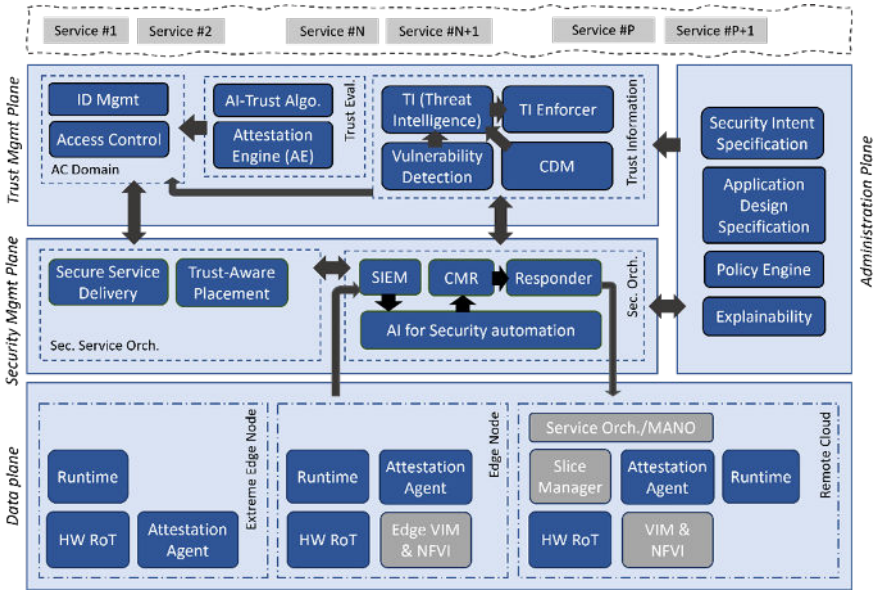

Figure 1. High-level architecture identifying iTrust6G's Security Enablers (blue blocks will be touched by the project)

- User and Entity Behaviour Analytics (UEBA): UEBA technologies can be integrated into the CDM framework to enhance threat detection capabilities. UEBA focuses on monitoring and analysing the behaviour of users, devices, and applications within a 6G infrastructure, identifying anomalous or suspicious activities that may indicate potential security threats
- Security programmability, to collect additional metrics to obtain an increased observability of resources.

b) Security Information and Event Management (SIEM): A SIEM is a tool that analyses data and events gathered from multiple levels of a monitored system to identify potential ongoing cyberattacks or anomalous situations [12]. For critical infrastructure, which presents unique challenges, a customised SIEM solution may be necessary to ensure comprehensive security and threat detection. One of the key challenges that traditional SIEMs can't handle in a Critical Infrastructure scenario is the vast amount of data that the Critical Infrastructure generates, which can overwhelm traditional SIEM systems. Moreover, the heterogeneity of devices and systems within a Critical Infrastructure network poses a significant challenge. These networks can potentially include legacy hardware devices and software that do not support modern security protocols or logging standards, creating a bottleneck to the collection and analysis of data that traditional SIEMs are not equipped to handle.

iTrust6G intends to safeguard the Critical Infrastructure IT ecosystem, which necessitates coping with the large quantity and diversity of cybersecurity events that will record and analyse. For instance, one of the key innovations the iTrust6G SIEM aims for is the handling of encrypted data, which necessitates the development of specific methodologies and solutions. The iTrust6G SIEM system will manage the distributed analysis of enormous volumes of business and Network data including network and systems logs, while effectively addressing data heterogeneity and optimising resource utilisation.

c) Threat intelligence for collaborative risk assessment: The increasing number of cyberattacks against organisations, due to the commoditisation of exploits and the widespread adoption of distributed IT architectures and cloud-based solutions in high-risk scenarios, renders the manual approach to attack reactions by incident response teams infeasible. This is compounded by the chronic shortage of skilled cybersecurity experts in the industry. Human experts are not able to keep track of the overwhelming number of new threats and exploitable vulnerabilities. They are typically required to make split-second decisions without having the necessary information and time to assess the effects of their decisions on the security posture of their managed network. Thus, a collaborative approach to react these issues is desirable. By sharing threats in the security community, security experts would be able to obtain information about new threats and vulnerabilities from trusted sources. A great deal of research has been performed in the last years, producing various projects to define formats, taxonomies, and best practices for threat sharing.

In this context, iTrust6G plans on capitalising on the CACAO standard [13] to exchange actionable procedures as Cyber Threat Intelligence (CTI). This approach will permit the proactive risk management, contributing to maintain a level of shared trustworthiness among collaborative administrative domains.

d) Threat models & Vulnerability detection/scanning: Threat modelling is a systematic process used to identify potential security threats, vulnerabilities, and risks in an information system or network. It involves creating a structured representation of the system's architecture, data flows, and

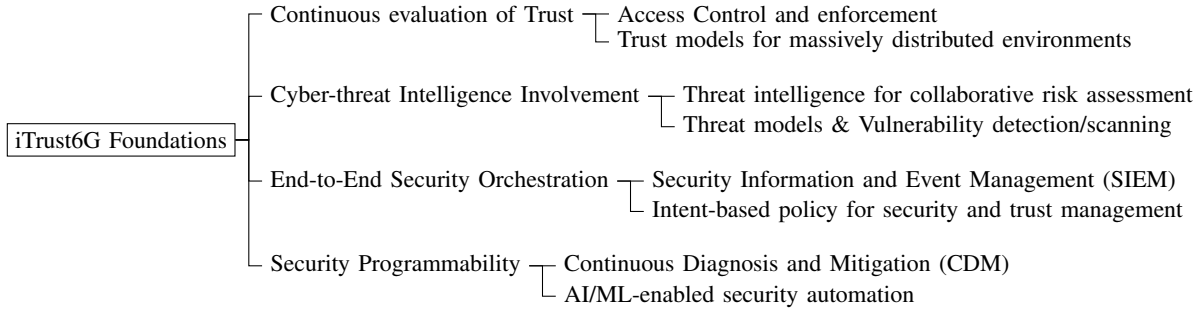

Figure 2. Classification of iTrust6G foundation topics and components

assets, and then using this representation to analyse potential attack vectors and vulnerabilities. Current state-of-the-art threat modelling methodologies include STRIDE [14], PASTA [15], and VAST [16], which focus on identifying threats, vulnerabilities, and mitigations across various stages of the system development lifecycle. Vulnerability detection and scanning are essential components of threat modelling, as they help organisations identify potential weaknesses and security gaps in their systems. State-of-the-art vulnerability detection and scanning solutions involve automated tools that perform static and dynamic analysis of applications, networks, and infrastructure.

iTrust6G will provide advanced solutions for Threat Intelligence in all relevant associated technologies through:

- Design and development of novel decentralised and highly distributed AI algorithms for 6G networks that evolve the classical notion of centralised AI. The proposed algorithms will assist towards threat modelling, classification, and mitigation.
- AI methods to develop association rules between already recorded knowledge bases of cyber-attacks and newly instigated patterns of attack for threat mitigation and remediation, associating properties of incidents like their impact, confidentiality etc. Such mechanisms include the following:
  - Applying anomaly detection and machine learning techniques to stay ahead of evolving cyber threats and ensure the continued operation and safety of mission-critical services.
  - The security behaviour analysis aiming to assess the behaviour analysis on both users and devices.
  - Employing AI-driven Threat Modelling and Vulnerability Detection methodologies and Cross-Domain Threat Modelling that consider the complex interdependencies and relationships between different domains in 6G networks, such as edge computing, network slicing, and cloud services.

e) Access Control (authentication, authorisation, identity management) and enforcement: Access control is considered a critical component in securing network resources and protecting against unauthorised access. With the development of advanced networks, new access control mechanisms are needed to address the unique requirements and challenges of these networks. Currently, access control mechanisms in advanced networks mainly rely on traditional authentication and authorisation techniques, such as username/password and role-based access control (RBAC). However, these mechanisms have limitations in terms of scalability, flexibility, and security.

To address limitations of traditional AC, several new access control mechanisms have been proposed. In iTrust6G, we plan to adopt a Blockchain-based access control approach, which leverages the tamper-proof and decentralised nature of blockchain to provide secure and transparent access control. This approach has the potential to address the challenges of centralised access control and ensure data integrity and authenticity. In blockchain-based access control, access decisions are stored on a blockchain, which is a distributed ledger that records transactions in a tamper-proof and transparent manner. Users can access the blockchain to view their access permissions and audit logs.

f) Trust models for highly distributed environments: Trust models rely on trust algorithm (TA) employed by policy engine (PE) to make a decision/evaluation by considering inputs such as entries in the policy database, user roles, attributes, behavioural information, threat-related information, etc. Once the TA has made the decision as the Policy Decision Point (PDP), the PE passes this to the Policy Administrator (PA) which configures all the corresponding Policy Enforcement Point (PEPs) to either enable or disable the communication. In addition, performance evaluation of the impact of source-dependency of TA mechanism & scoring e.g., MNO vs. tenant, as well as evaluation of various flavours e.g., Criteria-based-TA vs. Score-based-TA vs. Contextual-TA are within scope of activities. Criteria-based TA necessitates a combination of attributes be fulfilled before allowing an action. In score-based TA, the weighted values of input data are used to compute a confidence level which is compared against the threshold value. The concept of Root-of-Trust is typically enabled using hardware-based tools. These known tools include (i) trust anchors comprising Trusted Platform Modules (TPMs) (for software integrity), trusted execution environments (TEEs) (for isolation against the infrastructure provider), hardware security modules (HSMs), (ii) secure identities, crucial to build trust between UE and network and

(iii) secure attestation methodologies, that can be employed for enabling trust at different architectural components. Specifically, secure attestation of virtual network functions is needed to verify isolated execution and ensure that a network function behaves as expected based on the specification of the function.

iTrust6G supports the concept of Level of Trust (LoT) as the key value indicator (KVI) to assess the security of a network service in a particular application environment. Trust evaluation can be based on different principles, some deterministic and some probabilistic. This project aims to integrate these two paradigms. On the deterministic side, we'll adopt well-known software integrity evaluation techniques, based on a root-of-trust, which can be a TPM device, or equivalent features implemented in firmware in a TEE, coupled with remote attestation. This involves performing measured boot and measured operations and compare the measurements against "golden values" provided by developers and security managers. This additionally provides also strong device identity, since the attestation report is digitally signed with a private key securely stored in the TPM. This identity and the attestation result will contribute to the evidence evaluated for zero-trust access control. On the probabilistic side, the project will explore various AI-based approaches to evaluate trust in services and components. This will be mostly based on machine learning applied to the analysis of past incidents and cyber-threats indicators. Some of them are to be enriched with metrics accessible from security programmability.

g) AI/ML-enabled security automation: Security automation is expected to enable the proactive discovery of threats and initiate security function transfers throughout the network. Combining AI/ML techniques with edge computing provides the means for an intelligent edge in 6G. In a 6G zero trust security architecture, zero trust for all North-South (N-S) and East-West (E-W) cloud traffic must be enforced with AI-based ML for threat detection, prevention, and containment. This distributed nature is the key to making the whole computation and resource management scalable towards more complex tasks and larger areas of intelligence. Moreover, with the ability to make network-wide intelligent decisions with a distributed edge-based architecture, AI itself can uncover the patterns within a large volume of data at different levels (intelligent radio, edge, and cloud). Hence, AI-based mechanisms have the potential to uncover vulnerabilities of the network.

iTrust6G will address security automation requirements through development of solutions for:

- Innovative distributed, low-latency federated learning algorithms. These algorithms will run AI processes locally at edge devices, deviating from the classical concept of centralised AI and adapting to the specificities of 6G and IoT. The proposed AI/ML algorithms will contribute towards the automation of security, real-time threat monitoring, and vulnerability assessment.
- Edge-based federated learning algorithms to preserve data privacy by maintaining physical control, keeping data closer to the user. Differential privacy techniques will add random noise to the training data, preventing private information disclosure. Algorithms for collaborative risk mitigation will be proposed to assess the risks of each network node by considering the detected risks of neighbouring nodes. These algorithms will assist users in managing risks by proposing actions and evaluating their effects on neighbouring nodes due to risk propagation rules.
- AI-based techniques to secure the integration of untrusted networks and communication between nodes in 6G networks, focusing on zero-trust architectures. To assess the effectiveness of the developed AI algorithms, which will be part of the security orchestrator module, monitor the mean time to detect threats among other orchestrator KPIs.
- Programmable security mechanism will assist toward the provision of adequate metrics for AI-based decision making, and facilitate enforcement.

h) Intent-based policy for security and trust management: Intent-based management is expected to substantially impact the manual management and reconfiguration of networks. This is proving increasingly difficult, leaving space for human errors that are likely to make networks vulnerable to intrusions and data breaches. Thus, automating the management of networks is desirable. Intent-based networking (IBN) tries to tackle the issue by defining a solution suite whereby network administrators are only required to express the requested reconfigurations of the network in natural language, i.e., their intent. The actual low-level commands for network appliances that are requested to implement the network administrator intents are automatically generated by an ad-hoc artificial intelligence, typically based on a logic inferential engine. IBN gained traction in the industry through several activities in different frontiers, including standard bodies, open-source communities, and R&D projects. In the standardisation landscape, there are workstreams spread across different telco fora. ITU-T has defined scenarios and requirements of intent-based network for network evolution, outlining the touchpoints and extensions for their applicability in sliced networks. TM Forum have specified a framework for intent driven management framework which allows an intent owner to convey the intent to an intent handler, using a well-defined interface that implements a standard set of procedures, this interface is used by Intent Management Function (IMF) to manage the lifecycle of intent objects, in compliance with the IMF operational scope. ETSI has produced different technical reports across different ISGs, including Experiential Networked Intelligence (ENI) and Zero-touch Service Management (ZSM). Of special interest is the future-forwarding view, with focus on 6G-oriented scenarios such as intent model federation and intent conflict handling. Finally, IETF/IRTF has drafted a number of documents related to the applicability of intents, with focus on intent taxonomy and interconnection, as well as intent usage for service assurance and slicing scenarios.

iTrust6G will extend the state of art in Intent-based networking with contributions on i) A novel specification format for

the description of the managed network and the characteristics of the network appliance, security controls, and assets that must be safeguarded along with their security requirements, ii) A cyber-security specialised orchestration framework for intent-based networking, leveraging Deep Learning (DL) and AI-based techniques to generate both configurations for both security controls and network appliances, automatically evaluating the potential increase of the risk exposure of the managed network that would stem from the application of the requested intent, and the compliance of the expressed intents against the network assets security requirements.

IV. iTrust6G use-cases

The iTrust6G vision and concept will be realised and validated through a balanced mix of activities for design and specification of the various solutions, implementation, and demonstrations. The purpose of these use case scenarios is to corroborate the actual value of the project results and their alignment with stakeholder requirements. While iTrust6G results are not specific to any particular vertical industry, the demonstration phase will focus on three use-cases:

- **Use-cases 1:** Dynamic security orchestration and trust establishment in multi-stakeholder and multi-domain environment. The objective is to validate the intent-based security policy enforcement and trust establishment in a multi-stakeholder environment.
- **Use-Case 2:** Operational security and trust re-evaluation. The objective is to validate the robustness of iTrust6G operational security mechanisms in presence of attacks including attack detection, mitigation, and forensics.
- **Use-Case 3:** Programmable security as a service. The objective is to validate the flexibility and agility of the programmability of security mechanisms at multiple levels based on the status of the application service.

V. Conclusion

The paper presented an overview of the iTrust6G Project, which provides "zero-trust" security enablers for future B5G/6G networks. iTrust6G introduces several innovations for strengthening security and privacy in the B5G era, including decentralised and robust security analytics, privacy-aware network slicing and orchestration as well as distributed attestation mechanisms. iTrust6G will contribute towards (i) a security architecture leveraging zero-trust principles for trustworthy 6G service management, (ii) an AI framework for novel threat detection, (iii) trust algorithms leveraging AI to evaluate the security posture from ownership, design and instance integrity factors affecting access control, (iv) AI-driven security orchestration capitalising on programmability models for self-protection, (v) intent-based security management featuring explainable and automated SO and (vi) the dynamic, configurable, and intelligent placement of network functions. Currently, iTrust6G is in the design phase, followed by development, integration and validation phases. The validation phase will include the evaluation of its security framework through three different use-case scenarios.

Acknowledgments

This work is supported by the Smart Networks and Services Joint Undertaking (SNS JU) under the European Union's Horizon Europe research and innovation programme under Grant Agreement No 101139198, iTrust6G project. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or SNS-JU. Neither the European Union nor the granting authority can be held responsible for them.

References

[1] 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 Communications Surveys & Tutorials*, vol. 23, no. 4, pp. 2384–2428, 2021, arXiv:2108.11861 [cs]. [Online]. Available: http://arxiv.org/abs/2108.11861

[2] G. Obrist, O. Okechukwu, A. Cross, D.-T. Do, and A. L. Imoize, "Security threat landscape for 6G architecture," in *Security and Privacy Schemes for Dense 6G Wireless Communication Networks*. IET Digital Library, Jul. 2023, pp. 117–131. [Online]. Available: https://digital-library.theiet.org/content/books/10.1049/pbse021e_ch5

[3] S. Dahmen-Lhuissier, "Securing Artificial Intelligence (SAI)." [Online]. Available: https://www.etsi.org/technologies/securing-artificial-intelligence

[4] ETSI, "GR SAI 001 - V1.1.1 - Securing Artificial Intelligence (SAI)," Tech. Rep. [Online]. Available: https://www.etsi.org/deliver/etsi_gr/SAI/001_099/001/01.01.01_60/gr_SAI001v010101p.pdf

[5] J. V. D'Angelo, M. Battaggia, A. Cammarano, H. Rouzegar, M. Compastie, and J. A. Acosta, "A security threat analysis for unified network orchestration across terrestrial and non-terrestrial," in *2024 IEEE International Mediterranean Conference on Communications and Networking (MeditCom) (IEEE MeditCom 2024)*, Madrid, Spain, Jul. 2024, p. 6.

[6] A. S. Abdalla and V. Marojevic, "End-to-End O-RAN Security Architecture, Threat Surface, Coverage, and the Case of the Open Fronthaul," Apr. 2023, arXiv:2304.05513 [cs, eess]. [Online]. Available: http://arxiv.org/abs/2304.05513

[7] "iTrust6G - Intelligent Trust and Security Orchestration for 6G Distributed Cloud Environments." [Online]. Available: https://www.sns-itrust6g.com/

[8] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero Trust Architecture," National Institute of Standards and Technology, Tech. Rep. NIST Special Publication (SP) 800-207, Aug. 2020. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/207/final

[9] Evan Gilman and Doug Barth, *Zero Trust Networks: Building secure systems in untrusted networks*, o'reilly media, inc. ed. [Online]. Available: https://www.oreilly.com/library/view/zero-trust-networks/9781491962183/

[10] N. MacDonald, "Market Guide for Zero Trust Network Access," Tech. Rep., Jun. 2020. [Online]. Available: https://www.gartner.com/en/documents/3986053

[11] UK NCSC, "Zero trust architecture design principles," Aug. 2024, original-date: 2019-06-26T15:02:21Z. [Online]. Available: https://github.com/ukncsc/zero-trust-architecture

[12] S. Shin, P. A. Porras, V. Yegneswaran, M. W. Fong, G. Gu, and M. Tyson, "FRESCO: Modular Composable Security Services for Software-Defined Networks." in *NDSS*, 2013. [Online]. Available: http://koasas.kaist.ac.kr/bitstream/10203/205914/1/fresco_ndss13.pdf

[13] Bret Jordan and Allan Thomson, "OASIS CACAO Security Playbooks Version 2.0," Nov. 2023. [Online]. Available: https://docs.oasis-open.org/cacao/security-playbooks/v2.0/security-playbooks-v2.0.html

[14] P. Torr, "Demystifying the Threat Modeling Process," *IEEE Security Privacy*, vol. 3, no. 5, pp. 66–70, Sep. 2005.

[15] T. UcedaVelez and M. M. Morana, "Intro to Pasta," in *Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis*. Wiley, 2015, pp. 317–342, conference Name: Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9821030

[16] threatmodeler, "Threat Modeling Methodologies: What is VAST?" Oct. 2018. [Online]. Available: https://threatmodeler.com/threat-modeling-methodologies-vast/