Overview of the security and trust mechanisms in the 5GZORRO project

José María Jorquera Valero*, Pedro Miguel Sánchez Sánchez*, Alexios Lekidis†, James Taylor‡
Javier Fernández Hidalgo§, Adriana Fernández-Fernández§, Paulo Chainho¶, Bruno Santos¶,
Jean-Marie Mifsud‖, Antoine Sciberras‖ M. Shuaib Siddiqui§, Manuel Gil Pérez*,
Alberto Huertas Celdrán*, and Gregorio Martínez Pérez*
*University of Murcia, Murcia, Spain; Email: {josemaria.jorquera, pedromiguel.sanchez, mgilperez, alberto.huertas, gregorio}@um.es
†Intracom Telecom, Athens, Greece; Email: alekidis@intracom-telecom.com
‡Bartr Group, Birmingham, England; Email: jamestaylor@bartr.world
§i2CAT Foundation, Barcelona, Spain; Email: {javier.fernandez, adriana.fernandez, shuaib.siddiqui}@i2cat.net
¶Altice Labs, Aveiro, Portugal; Email: {paulo-g-chainho, bruno-g-santos}@alticelabs.com
‖Malta Communications Authority, Floriana, Malta; Email: {jean-marie.mifsud, antoine.b.sciberras}@mca.org.mt

***Abstract*—In the evolution from 5G to beyond 5G networks, new business models are emerging where multi-domain and multi-stakeholder scenarios will play a paramount role as enablers. In these scenarios, the automated management of the services with minimal human intervention, also known as zero-touch management, is a pivotal requirement to ensure a proper functioning and to enable real-time responses to possible incidents or scalability needs. Nonetheless, these new scenarios and requirements also introduce new security risks that entail a complex threat landscape for beyond 5G networks. Hence, zero-touch management demands new solutions capable of securely controlling network resources into end-to-end scenarios distributed in multiple domains. In this vein, several challenges arise and need to be addressed, such as integrity, non-repudiation, confidentiality, security, and trust. Therefore, the H2020 5GZORRO project proposes new security and trust solutions for multi-domain and multi-stakeholder scenarios in 5G and beyond networks. To deal with the utmost importance security and trust challenges, we introduce different modules to mitigate them, namely, integrity and non-repudiation through Distributed Ledger Technologies, decentralized identity through an Identity and Permission Manager, end-to-end trustworthy relationships via a Trust Management Framework, secure workloads across different tenants and stakeholders via Trusted Execution Environment Security Management, detection and response to internal vulnerabilities and attacks via Network Monitoring, and on-demand secure cross-domain connections via VPN-as-a-Service. Therefore, the built security and trust 5GZORRO mechanisms form a secure environment with zero-touch automation capabilities, minimizing human intervention.**

I. Introduction

The deployment of 5G networks and the development of beyond 5G technologies offer advanced technical capabilities that are enabling the emergence of new network services. These services take advantage of network scenarios located under different administrative entities, each of which can provide part of the required functionality or sell part of its resources on a temporary basis. In this context, the resulting services turn out to be multi-domain and multi-stakeholder services [1], whose resources deployed in different scenarios with different policies and conditions.

Thus, the coordinated management of resources present in different domains introduces a new paradigm to be solved. To this end, technologies such as artificial intelligence (AI) is used to minimize manual intervention, seeking zero-touch services. In this context, new requirements and challenges also appear to be covered from the perspective of security and trust, since advanced cyber-attacks have been gaining prominence in recent years [2].

In this sense, the challenges range from the interrelationship between stakeholders, ensuring that none of them behaves maliciously, to the security of services against external attacks, which could affect multiple domains at the same time. Given this wide variety, solutions are needed that cover the entire lifecycle of multi-domain services while ensuring high security and trust properties.

In order to meet these properties and develop innovative solutions, the H2020 project 5GZORRO (Zero-tOuch secuRity and tRust for ubiquitous cOmputing and connectivity in 5G networks) appeared [3]. Among the project objectives, we can highlight that it seeks to define and prototype a security and trust framework, integrated with flexible and multi-stakeholder combination and composition of resources and services in 5G networks. For this purpose, this project uses three key technologies as fundamental pillars in the present and future of network services: (i) Cloud native technologies [4]; (ii) Distributed Ledger Technologies (DLT) [5]; and (iii) Artificial Intelligence (AI) [6].

Thus, the main contributions of the present work can be divided into two parts. First, an analysis of the security and trust challenges present in multi-domain and multi-stakeholder 5G environments. These challenges serve as a guide to the work performed within the project, motivating the different solutions and technologies employed. And second, the description of how the 5GZORRO ecosystem solves the previous challenges and what security and trust properties it offers for 5G and beyond paradigms.

The remainder of this paper is structured as follows. Section II depicts the main challenges in multi-domain and

multi-stakeholder scenarios that are related to security and trust issues. Section III details the security and trust properties covered in the 5GZORRO ecosystem and how they are enabled. Finally, Section IV dives the conclusions extracted from the work and future directions.

II. Current challenges in 5G multi-domain and multi-stakeholders scenarios

5G-enabled solutions are deployed in multi-domain network environments in which each domain is under the administrative control of a different entity (multi-stakeholder). Such deployments offer numerous advantages in terms of flexibility and performance. However, they also bring new security and trust challenges to be overcome in order to ensure proper service operation.

In particular, the main challenges identified, which are guiding the work in the area of security and trust, are as follows:

A. Integrity and non-repudiation

Data integrity and non-repudiation are essential properties in multi-tenancy environments where resources and services are shared by different customers and organizations. In this regard, new technologies have arisen to cover these security properties. Distributed Ledgers (DLT's) are decentralized digital record systems. Unlike a traditional ledger - managed by a single trusted entity - DLTs are formed of multiple nodes on a peer-to-peer (P2P) network that each replicate and store an identical copy of the ledger state and update themselves independently once consensus has been reached on a ledger update. Crucially, this means that a group of participants are responsible for the maintenance of the valid immutable state of the ledger.

A consensus mechanism is required for network member nodes to agree on ledger updates, a principal element in building trust between transaction participants. This mechanism prevents fraudulent transactions, attacks on the network and ensures entries in the ledger can be trusted by all parties.

Private-permissioned DLTs have evolved to meet enterprise requirements, offering additional privacy guarantees and transaction non-repudiation, with anonymity being sacrificed for well-known participant identities.

Smart Contracts are a DLT feature that encapsulates business logic and potentially real-world contracts or SLAs. Each participant executes a contract's deterministic logic for processing and validating ledger state transitions, sometimes aided by a mutually trusted Oracle services that provide off-chain data or ledger fact attestation. Crucial to the DLT model is that there is no level of entropy in such a transaction, allowing each participant to come to consensus. Smart Contracts give rise to a greater level of trust between parties, reduce the need for trusted intermediaries and help protect against fraud losses and malicious behaviour.

B. Decentralized identity management

Identity management is key to the realisation of trust across 5G domains when it comes to identify, authenticate, and authorize thousands of users, devices, resources, services, organizations, etc. Decentralized identity management (DIdM) is a novel paradigm that is becoming an interesting research area due to its integration with novel distributed ledger technologies (DLTs) such as blockchains. Related to decentralized identity management, Decentralized Identifiers (DIDs) [7] are a novel type of identifiers proposed by W3C that allows associating any subjects such as stakeholders, resources, services, organizations, entities, and so on, with a digital identity. Decentralized Identifiers (DIDs) are global identifiers which enable verifiable and decentralized digital identity, allowing to uniquely identify any subject, e.g. a person, organization, abstract entities, etc. To achieve this purpose, DIDs are associated with cryptographic material, such as public keys, and service endpoints, making each DID globally unique, resolvable with high availability, and cryptographically verifiable. Another concept related to decentralized identity management is Verifiable Credentials, a Verifiable Credential (VC) [8] is a tamper-evident and privacy-preserving credential (set of claims) that can be demonstrated through a cryptographic process. Verifiable Credentials can represent the same information that physical credentials represent in real life such as driving licenses, passports, health insurance card, and so on. Therefore, Verifiable Credentials represent statements made by an issuer in a tamper-evident and privacy-preserving manner.

C. End-to-end trustworthy relationships

5G networks and beyond introduce new pervasive and scalable approaches which tend to contemplate distributed approaches rather than the centralized ones envisaged in previous networks (i.e., 3G and 4G). In this sense, distributed approaches have promoted collaboration between different service/resource consumers and providers. Ergo, many solutions offer end-to-end services provisioning in 5G ecosystem, nevertheless, most of the solutions do not ensure end-to-end trustworthy multi-party relationships [9]. Furthermore, previous trust solutions cannot be considered in 5G and B5G ecosystems on account of the fact that novel requirements and Key Performance Requirements (KPIs) have emerged through 5G-enabled solutions. For instance, since automatization is an essential requirement for 5G and B5G solutions [10], it is required new trust solutions that provide mechanisms for trust automation in multi-domain scenarios on top of a 5G service management framework. Hence, end-to-end trustworthy relationships entail two principal challenges, on the one hand, identifying a set of high-level 5G and B5G requirements that should be fulfilled by trust solutions, and on another hand, adjusting, if possible, or creating emerging 5G and B5G trust solutions.

D. Secure workloads across different tenants and stakeholders

Multi-tenant and multi-stakeholder nature of 5G and B5G ecosystems create scenarios where no inherent trust mechanisms exist. Besides, 5G and B5G also introduce new security risks to data, services and networks [11], which are even higher in multi-tenant and multi-stakeholder scenarios. In this sense, an operator and resource and service provider may assure a set of their machines or services against a perverse tenant using mainstreamed solutions such as virtualization and containerization, nonetheless, few solutions protect tenant services

or applications running under the administrative control of a different entity against perverse stakeholders with root access. Therefore, it is required new approaches that enable critical workloads to go across different tenants and stakeholders with no losses in security, at the same time, they offer zero trust hardware platforms.

E. Detection and response to internal vulnerabilities and attacks

In 5G and beyond networks, sometimes it is required to employ multiple network infrastructures, located at different domains, to reach the required Quality of Service (QoS) targets, and in consequence, create multi-tenant network environments. These environments are principally enabled by network slicing solutions. Nonetheless, network slicing involves its own security threats, as slices are formed by leveraging different parts of the 5G infrastructure. In this regard, each network (i.e. Core, Access Network, Transport Network, and Multi-access Edge Computing) part is subject to specific Tactics, Techniques and Procedures (TTPs) for interrupting its normal behaviour. Hence, the identification and mitigation of the principal threats are vital for a proper 5G infrastructure operation, and hence no prioritization among them is considered. To deal with them, a resilient security architecture should cover all the 5G infrastructure as well as the multi-tenant and multi-domain scenarios. In addition, the detection and protection mechanisms against sophisticated and zero-day threats [12] need the combination of new security solutions at various levels, both within an administrative (i.e. resource owner) domain as well as cross-domains (i.e. the interconnection with other domains).

F. On-demand secure cross-domain connections

One of the most innovative aspects of 5G networks and B5G is the use of network slicing that allows service providers to build virtual end-to-end networks tailored to application requirements. Hence, 5G network slicing is a key enabler to provide end-to-end network communication links across domains. However, network slicing requires integrating isolation mechanisms that guarantee confidentiality and integrity protection of tenant's traffic. Furthermore, such mechanisms should not only ensure on-demand traffic isolation, so data flow of one slice cannot move to and be accessed from another slice, but also facilitate the interconnection of different 5G networks, operators and providers. These mechanisms should follow zero-touch principles in order to automate the overall service lifecycle management. Therefore, new solutions are required for creating secure multi-domain on-demand connections ensuring confidentiality and integrity of the data passing between VNFs in a 5G network slice with seamless use of heterogeneous virtualization platforms.

III. 5GZORRO Security and Trust properties

The 5GZORRO architecture (see Fig. 1) aims at empowering multi-party collaboration in cross-domain 5G environments where operators and service providers often resort to the use of third-party resources to cover for a temporary lack of capabilities in their own domain. To achieve this, 5GZORRO incorporates zero-touch automation solutions to orchestrate high volumes of ubiquitous and pervasive 5G services. Nevertheless, these dynamic and multi-domain scenarios also bring

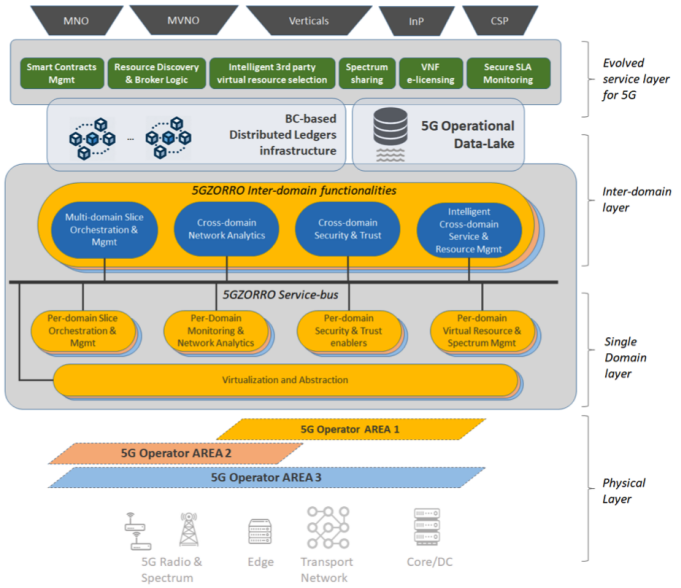

Fig. 1. Conceptual architecture of the 5GZORRO platform [3]

multiple security and trust challenges that should be addressed. In this regard, the 5GZORRO ecosystem will deal with a set of the utmost importance security and trust challenges, previously identified in Section II, through multiple modules.

A. DLT-enabled marketplace

In order to enable the trading of resources and services without the need for a trusted intermediary, a decentralized Marketplace is made available as part of the 5GZORRO architecture. To achieve this, each participant hosts a distributed application (DApp) that interfaces with the domain's DLT node, forming a peer-to-peer (P2P) network consortium. Providers register resources and services into the Marketplace using a standardised data format or schema in order to form a decentralized catalogue of offers available to consumers. These resources and services become tokenised digital assets stored into the blockchain, resulting in an immutable record of ownership and availability on the ledger. By using Smart Contracts that governs any state change, offers stored in the Marketplace are tracked and updated over time (e.g. when leased to a particular consumer). When advertising an offer, a provider will also associate legal prose with its definition. Prose will be generated from templates that are subject to a governance process, defining the legal framework and SLAs for every offer. Smart Contracts, derived from approved legal prose templates, facilitate the autonomous validation of actions made against the digital asset and management of the contract lifecycle in-line with the terms defined within, enforcing its trustworthiness from a business point of view.

B. Identity and Permissions Management based on DIDs and VCs

The goal of Identity and Permissions Management is to supply the mechanisms required for generating unique identifiers in the 5GZORRO ecosystem, recognising communicating endpoints, identifying, and authenticating entities, services,

and organizations, and authorising consumer requests to access a preserved services and resources. The main services provided by Identity and Permissions Management module are identification, authentication, and control access. Firstly, such a module provides an appropriate mechanism to identity entities, services, resources, consumers, providers, and organizations, which allows decentralisation of the system without forgetting the security principles. Secondly, the Identity and Permissions Management proportion a reliable authentication using Decentralised Identifiers, DID Documents securely providing entities metadata (including entities cryptographic metadata like public keys), and Verifiable Credentials. Finally, it guarantees a granular control access mechanism that standardises authorised access to data, resources, and services.

These functionalities are provided by different types of DID Agents, distributed across different domains and securely communicating among each other by using P2P DID Communication protocols. There three main types of DID Agents, each one holding a Governance DLT Wallet to securely handle private keys and credentials:

1) *Admin Issuer DID Agents* have functionalities to issue Verifiable Credentials associated with 5GZORRO entities including stakeholders credentials and Marketplace offers credentials. These functionalities are operated by 5GZORRO stakeholders playing the role of Governance administrator or the Regulator Authority.
2) *Holder DID Agents* communicate with Admin Agents to request the issue of Verifiable Credentials. Issued credentials are stored and maintained by the Holder DID Agent. These functionalities are operated by 5GZORRO stakeholders playing the role of Service Provider or Resource Provider.
3) *Verifier DID Agents* communicate with Holder DID Agents to request presentation proof of Verifiable Credentials. These functionalities are operated by 5GZORRO stakeholders playing the role of Service Consumer, Resource Consumer or Data Lake Operator.

C. 5G Trust Management Framework

Trust is a pivotal element when defining and establishing business relationships between two or more partners, and in particular, when they are trading (leasing or purchasing) services and resources allocated in a third-party infrastructure. Thus, trust plays a crucial role in the selection of partners for business relationships. Nonetheless, trust management also brings a set of challenges, as aforementioned in Section II, which should be tackled. In this regard, 5GZORRO will encompass the design, implementation, and validation of a trust management framework to integrate end-to-end trustworthiness establishment for distributed stakeholder environments. Unlike most of the previous trust management frameworks, it has a decentralized nature, and consequently, the 5GZORRO trust management framework can be deployed in both intra- and inter-domain scenarios. Considering its decentralized nature, the trust management framework allows for end-to-end enforcement differentiating it from other approaches that only assess the trust level for a particular segment of the network. In this respect, the trust management framework may gather reputation information not only from a specific service or slice but also from its resource or service provider. Owing to the fact that the automatization is an essential 5G and B5G requirement and it is also a core design principle of the 5GZORRO project, the trust management framework ensures an automatization for all its steps and modules as well as compatibility with other services based on ETSI ZSM architecture [13]. Lastly, the 5GZORRO trust management framework is also inspired by NIST's Zero Trust Architecture [14] and it contemplates some essential zero trust principles, starting with the basic one of no implicit trust granted to any entity, regardless of whether it is intra- or inter-domain.

D. Trusted Execution Environment Security Management

On account of the fact that fewer solutions can protect a tenant service or application running in an external administrative control domain, novel mechanisms to guarantee secure execution of critical workloads across different tenants and stakeholders are required. In this regard, the 5GZORRO project integrates commercial Trusted Execution Environments (TEEs) in the execution of some 5GZORRO software components, enhancing the security and trust of the software executed under these capabilities. In this way, TEE-based software execution enables critical workloads to go across different tenants and stakeholders with no losses in security, such as VIMs in a third-party infrastructure. By implementing an API for "TEE-as-a-Service", abstracting the low-level details of the commercial TEEs available, any service or application can be executed in a secure enclave on the 5GZORRO platform. Furthermore, such a security management solution not only protects data and software while they are running on the secure enclave but also while data is in transit and at rest. Due to a TEE includes a zero-trust hardware platform, it is as well a key component to establish a root-of-trust and end-to-end secure communications. Thus, the presence of these capabilities in the infrastructure offered by some stakeholders also improves the trust level perceived by service consumers, as this component provides extra security at the hardware level to the resources and services offered by service providers.

E. Network Monitoring

Since the identification and mitigation of threats are an essential security requirement for a proper 5G infrastructure operation, the 5GZORRO project contemplates an intra-domain security module that allows enhancing stakeholders' internal resource and service security. In particular, this module leverages the usage of internal resource and service metrics (such as network communications, resource usage, etc.) and ML techniques to 1) detect attacks and 2) provide mitigation procedures for them before they affect significantly the stakeholder infrastructure. Initially, for the detection part, this module identifies effectively operational (such as failures or malfunctions) and cyber-security (such as malicious activity or abuse of other components) threats based on evidence that originates from network communications. Besides, the detection part is also focused on both known and unknown (zero-day) threats, by employing threat detection mechanisms such as rule-based Intrusion Detection System (IDS), protocol specification, and behaviour analysis, and producing network events and alerts about potential failures or security threats.

Secondly, the mitigation procedures are based on the integration of tools that ensure the protection against unauthorized and malicious entities (e.g., through the configuration of firewall policies) as well as the isolation of infrastructure or 5GZORRO platform components that are compromised (e.g., moving them to a specific VLAN). As a result, mitigation should ensure the continuous operation and reliability of the 5G infrastructure as well as the 5GZORRO platform components. Therefore, this module supplies security against threats but also enriches the external trust from other stakeholders, as these services can be seen as an additional security guarantee for possible delegated resources or services.

F. VPN-as-a-Service

The 5GZORRO platform brings the chance to extend a stakeholder's current capabilities in case it envisages a temporary shortage of those, allowing the stakeholder to lease or purchase certain service/resource available at the Marketplace. In this context, cross-domain security and trusted connectivity establishment play a key role when it comes to performing network slicing and integrating resources located at a third-party infrastructure. Hence, the VPN-as-a-Services module integrates Virtual Private Network (VPN) technologies [15] with the Identity and Permissions Management functionalities offering automated and on-demand VPN-as-a-Service functionalities for the Network Service Mesh Manager (NSMM). The principal novelties provided by the 5GZORRO VPN-as-a-Service are: the integration of DID information [7] stored in a DLT when generating a secure connection at VPN level, and then the generation of secure cross-domain connections on-demand at the slice level. Regarding DID information, the VPN-as-a-Service leverages the Identity and Permission Management service for key distribution process and the authentication between VPN instances, taking advantage of its DLT-based security features. Concerning cross-domain slice stitching requirements, the VPN-as-a-Service designs a gateway-to-gateway service that allows automated interactions and connection setup and decouples the network configuration from VNFs and other delegated resources. Hence, the VPN-as-a-Service module introduces a lightweight approach, ensuring privacy, security, and trust properties, without sacrificing performance, and being agnostic to the underlying virtualization technologies.

IV. Conclusion and future work

The service automation and dynamic adaptation requirements introduced by multi-domain and multi-stakeholders scenarios entail the need to cover new security and trust challenges emerging in 5G networks and beyond. In a bit to enhance next-generation networks, this paper compiles a set of today's most vital security and trust challenges. In addition, this work also presents how the 5GZORRO project seeks to solve such security and trust challenges present in multi-domain and multi-stakeholder 5G scenarios, by leveraging the use of DLTs, DIDs, TEEs, or a Trust Management Framework, among other solutions.

As future work, we plan to continue with the development of the prototype security and trust framework. As main the elements in this development, we consider the integration of the different modular solutions in a common set, completely covering the considered environment. In addition, we plan to validate the different security and trust properties to be covered, verifying that these properties are satisfactorily covered.

Acknowledgment

This work has been supported by the European Commission through 5GZORRO project (grant no. 871533) part of the 5G PPP in Horizon 2020 and by the CERCA Programme / Generalitat de Catalunya. The paper solely reflects the views of the authors. EC is not responsible for the contents of this paper or any use made thereof. Authors thank the 5GZORRO Consortium for useful insights to this work.

References

[1] S. E. Elayoubi, J.-S. Bedo, M. Filippou, A. Gavras, D. Giustiniano, P. Iovanna, A. Manzalini, O. Queseth, T. Rokkas, M. Surridge *et al.*, "5g innovations for new business opportunities," in *Mobile World Congress*. 5G Infrastructure association, 2017.

[2] H. Sedjelmaci, "Cooperative attacks detection based on artificial intelligence system for 5g networks," *Computers & Electrical Engineering*, vol. 91, p. 107045, 2021.

[3] G. Carrozzo, M. S. Siddiqui, A. Betzler, J. Bonnet, G. M. Perez, A. Ramos, and T. Subramanya, "Ai-driven zero-touch operations, security and trust in multi-operator 5g networks: a conceptual architecture," in *2020 European Conference on Networks and Communications (EuCNC)*. IEEE, 2020, pp. 254–258.

[4] S. Sharma, R. Miller, and A. Francini, "A cloud-native approach to 5g network slicing," *IEEE Communications Magazine*, vol. 55, no. 8, pp. 120–127, 2017.

[5] Q. Zhu, S. W. Loke, R. Trujillo-Rasua, F. Jiang, and Y. Xiang, "Applications of distributed ledger technologies to the internet of things: A survey," *ACM computing surveys (CSUR)*, vol. 52, no. 6, pp. 1–34, 2019.

[6] C. Zhang, Y.-L. Ueng, C. Studer, and A. Burg, "Artificial intelligence for 5g and beyond 5g: implementations, algorithms, and optimizations," *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, vol. 10, no. 2, pp. 149–163, 2020.

[7] D. Reed, M. Sporny, D. Longley, C. Allen, R. Grant, M. Sabadello, and J. Holt, "Decentralized identifiers (dids) v1. 0," *Draft Community Group Report*, 2020.

[8] W3C. Verifiable Credentials Data Model 1.0. [Online]. Available: https://www.w3.org/TR/vc-data-model/

[9] C. J. Mitchell, "Who needs trust for 5g?" *arXiv preprint arXiv:2005.00862*, 2020.

[10] C. Benzaid and T. Taleb, "Ai-driven zero touch network and service management in 5g and beyond: Challenges and research directions," *IEEE Network*, vol. 34, no. 2, pp. 186–194, 2020.

[11] M. Barros Lourenço, L. Marinos, and L. Patseas, "ENISA threat landscape for 5G networks," European Union Agency for Cybersecurity, Tech. Rep., 12 2020.

[12] P. Parrend, J. Navarro, F. Guigou, A. Deruyver, and P. Collet, "Foundations and applications of artificial intelligence for zero-day and multi-step attack detection," *EURASIP Journal on Information Security*, vol. 2018, no. 1, pp. 1–21, 2018.

[13] . ETSI GS ZSM 001, "Zero-touch network and service management (zsm); requirements based on documented scenarios," European Telecommunications Standards Institute, Tech. Rep., 2019.

[14] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero trust architecture," National Institute of Standards and Technology, Tech. Rep., 2019.

[15] B. Lipp, B. Blanchet, and K. Bhargavan, "A mechanised cryptographic proof of the wireguard virtual private network protocol," in *2019 IEEE European Symposium on Security and Privacy (EuroS&P)*. IEEE, 2019, pp. 231–246.