Trusted Execution Environment-enabled platform for 5G security and privacy enhancement

José María Jorquera Valero, Pedro Miguel Sánchez Sánchez, Alexios Lekidis, Pedro Martins, Pedro Diogo, Manuel Gil Pérez, Alberto Huertas Celdrán and Gregorio Martínez Pérez

Abstract. With the deployment of 5G networks and the beginning of the design of beyond 5G communications, new critical requirements are emerging in terms of performance, security, and trust for leveraged technologies, such as Software Defined Networking (SDN) and Network Function Virtualization (NFV). One of the requirements at the security and trust level is that when delegating critical tasks and data to the infrastructure deployed in an external domain, the client needs guarantees that the execution has been carried out securely, without data breaches or compromises during computing tasks. To meet this need, this chapter proposes a framework that uses Trusted Execution Environments (TEEs), processing environments isolated from the rest of the system to guarantee the security of the data and tasks processed in them, in order to improve the security of 5G environments. This framework enables the deployment of TEE as a cloud service, also denoted as TEE-as-a-Service or TEEaaS, allowing customers to take advantage of its benefits without having to deal with the configuration of the environment and hardware. Furthermore, this chapter also discusses current trends as well as future challenges related to the deployment of TEEs in 5G environments, providing key aspects for future solutions in the area.

Keywords. 5G cyber-security, Trusted Execution Environments, Multi-Domain Environments, Trustworthy Network Slicing, Cloud infrastructure.

1. Introduction

The modern network paradigm is enabling 5G developments where millions of network elements are connected in real time with scalability and performance far superior to previous versions of the network infrastructure (i.e., 3G and 4G) [20]. In this line, virtualization technologies are emerging as the main drivers for service and resource management due to their flexibility in configuration and deployment. In addition, network resources forming a service can be distributed across domains in different organizations. This situation enables a rapidly changing environment in which network services are created and distributed very dynamically [28].

In this context, there is an ongoing trend for some organizations to offer or share computing services by renting resources that are surplus or close to the end user, offering a better user experience. This allows optimizing the use of resources while offering a better Quality of Service (QoS) to end users, getting faster responses to requests and not exposing information beyond the end user's environment, for example. However, offloading tasks on an external organization infrastructure, especially when they are critical tasks or sensitive data management [34], implies new security risks since direct control of the infrastructure where the software is running is lost. This situation implies additional security measures to ensure reliable execution while maintaining good efficiency and revenue.

To solve the problem, several actions can be taken, such as the use of encrypted communications [15], correct data life cycle handling [59], etc. In addition, some measures are also necessary to guarantee the isolation and security of the processes during their execution. In this sense, the deployment of Trusted Execution Environments (TEEs) becomes one of the most relevant options to guarantee the security of the critical processes executed [61].

A TEE is an isolated processing environment where the code and the data are protected during execution, decoupling its memory area from the rest of the processor and providing confidentiality and integrity properties [49]. To provide such capabilities, the environment should run on a separated kernel whose components (CPU registers, memory, sensitive I/O, etc.) are trustworthy against software and physical attacks. Nevertheless, the usage of TEE in real world deployments comes with given associated problems such as specific code and software adaptations and compiling, specific TEE configuration, or performance degradation [43]. Besides, the integration of these solutions into modern scenarios, such as 5G deployments, brings additional challenges due to the dynamicity and quick deployment time required.

Then, despite the great advances in TEE and 5G virtualization technologies, there are still relevant challenges to tackle, mainly related to their integration. Among them, we highlight the following ones:

- **Application of TEEs on top of existing software solutions**. The fact of adapting pieces of software already developed and compiled to be executed in TEE solutions can be a complex task depending on the used TEE framework.
- **5G core network component execution in TEE frameworks**. 5G network elements have critical performance requirements in terms

of throughput and delay, but also security. Then, it is critical to find a proper balance between security guarantees and service performance.

- **TEE offered as a service for offloaded task execution**. Traditionally, TEE solutions are deployed internally in each domain, without offering these capabilities to potential external customers. However, TEEs offer advanced security and isolation capabilities that, provided as a cloud service, can generate a new service market, just like infrastructure (IaaS), platforms (PaaS), and software (SaaS).

With the goal of improving the security in offloaded task execution on demand, this book chapter proposes a TEEaaS framework for 5G multi-domain networks in which multi-tenancy infrastructures are considered as a key enabler. The proposed framework seeks to guarantee trusted execution of code when offloading critical data and processes into a foreign network domain due to possible performance and system requirements. This framework seeks to decouple possible TEE configuration and deployment tasks from its final usage in actual code, facilitating its use in real environments and generating a new service of security and trust. Thus, the TEEaaS leverages SCONE [9] as a mechanism for abstracting specific implementation details. The present work is developed under the 5GZORRO H2020 project [27], which focuses on the development of solutions for zero-touch service, network, and security management in multi-stakeholder environments operating in a 5G context. Then, the ultimate goal of the proposed framework is to provide TEEaaS solutions in a marketplace shared among several tenants that maintain a commercial relationship based on networked services and resources, where consumers have the possibility to instantiate services or applications on a set of resources that may be, by nature, unreliable.

The rest of the chapter is structured as follows. Section 2 provides the required background on 5G network architecture and TEE technologies, which are useful for the comprehension of the proposed approach, and in particular, Section 2.3 that introduces the current state-of-the-art about TEEs and 5G enforcements. Section 3 details the proposed solution for a TEEaaS platform, focusing on its design and implementation. Then, Section 4 provides an insight into current trends and future challenges on TEE application in modern scenarios. Finally, Section 5 summarizes the presented solution as well as provides some perspectives for future work.

2. Background and related work

In order to understand in depth our TEE-enable solution, it is critical to have a comprehensive view of the 5G paradigm and the main technologies leveraged in it. Besides, it is equally important to provide a background in TEE technologies, with a high-level description and definition of the main types of TEEs. Thus, this section provides the background insights required regarding 5G and TEE technologies.

2.1. 5G network architecture and enablers

5G is expected to be a multi-tenant and multi-service network where technologies play a paramount role as a pillar of digital evolution. Simultaneously, the growth of interconnected devices on 5G networks entails more efficient use of mobile network infrastructures, as well as ensuring enhanced bandwidth, ultra-low latency, network coverage, and high data capacity compared to previous networks. Thus, 5G is designed thinking in a dynamic network environment, where networks are created and modified according to heterogeneous requirements. In this scope, network slices are considered as a necessary mechanism for satisfying the QoS requirements as well as enabling the coexistence of multiple verticals [29].

To solve the previous requirements, advanced networking and virtualization methods, such as Network Function Virtualization (NFV) and Software Defined Networks (SDNs), are regularly contemplated in literature. Thus, flexible virtualization approaches, also known as Virtualized Network Functions (VNFs), are employed as the adoption of techniques that provide not only a high QoS but also a low cost in network environments, thus minimizing operational and capital expenditures (OPEX and CAPEX). Despite the benefits that multi-tenant and multi-service network slices bring, they also introduce a potential attack surface for 5G networks [21]. In this sense, adversaries might eavesdrop on network communications, gain unauthorized access, and finally, carry out spiteful actions such as disrupting swapping data by users or tenants.

In the case of NFV, it possesses a complex architecture [46] that makes it prone to cyber-attacks. In particular, the Virtualized Infrastructure Manager (VIM), which is one of the three functional blocks of ETSI NFV Management And Network Orchestration (NFV-MANO) [44], is a pivotal component as well as one of the most targeted. Among the main tasks of VIM is to coordinate the NFV Infrastructure (NFVI) resources utilized by the VNFs, based on what is needed at any given time, to deliver network services and resources. Therefore, adversaries may discover vulnerabilities that would allow them to steal or tamper with sensitive data [40] and critical processes running within the VIM. To dwindle these types of attacks, the VIM might consider the use of trusted platforms to perform certain critical actions [53]. For the sake of illustration, a possible countermeasure could be the VIM trusted execution by deploying these as containerized systems isolated from the host system. Thus, the VIM life cycle would be executed inside trusted platforms, and therefore, the boot processes, connections and data management, kernel memory, and code integrity may evade buffer overflow and code injection attacks.

Regarding SDN, it encompasses a wide variety of architectures and functionalities such as controllers, northbound and southbound APIs, SDN applications, etc. SDNs promote a dynamic, programmatically, and efficient network administration using software. Nevertheless, the variety of architectures and functionalities together with high customization of the networks lead to the emergence of new security risks in 5G networks. Multiple security threats may be linked to SDNs, among the most well-known we can introduce data forging, memory scripting [7], or DDoS [23, 30], to name but a few. On the one hand, the data forging entails compromising an SDN element such as a switch, router, or controller to falsify network data and launch other attacks as DoS. In this way, data forging has been identified as a threat related to components in the data plane and the controller plane. On the other hand, the memory scripting threat is carried out by an adversary scanning the physical memory of a software component to acquire sensitive data for which he/she/it does not have permission. These threats may cut down the SDN security risks through a trusted executed platform that guarantees not only code integrity to prevent memory or file modification (against memory scripting attacks), but also code confidentiality to ensure code loading (against data forging attack) [42].

Another pivotal enabler that has been boosted by the 5G ecosystem is Distributed Ledger Technologies (DLTs). Having in mind heterogeneous and multi-stakeholder 5G ecosystems, such as a trustworthy end-to-end establishment across multiple domains [27], DLTs facilitate the interaction among multiple stakeholders involved in dynamic 5G environments, the cross-domain sharing of crucial data (Smart Contracts), accelerate settlements that previously involved complex processes, and the decentralized management of the security-related information [35]. In this scope, DLTs are envisioned to play a crucial role in 5G scenarios. Nevertheless, such technology does not depend on pre-established trust between the implicated entities, therefore it also introduces challenges that need to be addressed such as improving the security and the privacy of data being pushed into the DLT or ensuring the nodes against data leakage and injection attacks. In particular, the use of a trusted environment may ensure that sensitive operations, such as the Service Level Agreement (SLA) computation monitoring [22] or authenticity proofs for smart contracts can run inside a tamper-proof environment [58], where neither the off-chain data nor its computation can tamper, and consequently avoiding possible data leakage and injection attacks.

As can be appreciated from the previous examples, there are multiple types of threats affecting swapping, confidentiality and integrity data, or disrupting the normal life cycle of resources. In that sense, 5G network components and enablers need to diminish the attack surface as well as solving or mitigating the feasible threats. Additionally, in the 5G multi-tenant and multi-service environments, these threats may display a higher risk since they may trigger lateral movements targeting other tenant resources. For that reason, we contemplate the use of TEEs as reliable service platforms that enable ensuring [54] the confidentiality and integrity of data managed in distributed, dynamic, and flexible environments, as well as ensuring the non-interruption of the processes carried out in our structures.

2.2. TEE background

TEE is a technology used to provide a tamper-resistant processing environment that runs on a separation kernel. Such a kernel enables systems with different levels of security to coexist on the same platform. The TEE can resist both software attacks and physical attacks performed on the main memory of the system. Furthermore, attacks performed by exploiting backdoor security flaws or system vulnerabilities are also avoided using TEE [49].

With respect to its functionality, the TEE divides the system into trusted and untrusted partitions that are isolated. These partitions use a secured interface for inter-partition communication to ensure that no lateral movement can occur if the untrusted partition is compromised. Currently, the secure interfaces are implemented using three main mechanisms: GlobalPlatform TEE Client API [3]; secure Remote Procedure Call (RPC) of Trusted Language Runtime [51]; and real-time RPC of dual-OS system [50].

Furthermore, three categories of TEE implementations are usually found: at the hardware level, at the software level, and integrated hardware-software solution. Hardware-based TEEs are using enforced isolation that is built into the CPU. A characteristic example is the Arm TrustZone technology [60]. Extensions to this technology allow securing the memory area. On the one hand, a hardware-based TEE allows trusted applications to have complete access to the main processor, resources (e.g., peripherals as sensors, actuators), and memory, while hardware isolation protects them from untrusted applications running on the main operating system.

On another hand, software-based TEEs are providing a normal and secure partition at the device firmware level, where both the kernel and the operating system are encrypted with strong cryptographic mechanisms to protect the data and applications of each device. Access to the keys for encrypting/decrypting the data is provided only to trusted entities through proper authentication or authorization schemes. A characteristic example of software-based TEE is the Open Portable Trusted Execution Environment (OP-TEE) [6]. The main difference with hardware-based TEEs is that they do not provide protection schemes for hardware resources, hence applications may only rely on the trusted kernel and not the processor and resources.

Concerning the integrated hardware-software TEE solution, it is formed as a combination of the hardware- and software-based TEEs to provide protection with multiple security layers. These layers ensure strong encryption mechanisms for applications, system configurations as well as stored data at both hardware and software (i.e., operating system) level.

Several open-source and proprietary TEE platforms are described in the literature as well as are available as market or community solutions. These implementations are separated into the three aforementioned categories as follows:

1. **Hardware-based TEEs**
   - *Arm's TrustZone* (proprietary) [16] offers an efficient system-wide approach to security with hardware-enforced isolation built into the CPU. Genode TEE [1] is based on this technology and extends it through a hypervisor environment that allows switching between secure and normal world.

   - *Intel SGX* (proprietary) [32] provides hardware-based memory encryption that isolates data and application-specific code in memory. Intel SGX allows user-level code to allocate private regions of memory, called *enclaves*, to protect against processes running at higher privilege levels. Besides, it provides a granular level of control and protection.
   - *Intel Trusted Execution Technology (TXT)* (proprietary) [4] provides a root-of-trust and verifies the integrity of a platform by relying on a TEE. During boot, it performs measurements on the platform components (boot loader, firmware, hypervisor, operating system) and verifies them against pre-calculated whitelist values. Hence, it provides mechanisms to protect vital data and processes from being compromised by possible malicious software running on the platform.

2. **Software-based TEEs**
   - *OP-TEE* (open-source) [6] is a TEE solution designed as a companion to a non-secure Linux kernel running on Arm. However, it has been structured to be compatible with any insulation technology suitable for the TEE concept and objectives: isolation, small footprint, and portability.
   - *Trusted Little Kernel* (open-source) [13] is a TEE solution by NVIDIA which defines a software-partitioned environment that provides trusted operations and supports multi-threading, a monitor for switching between the secure and normal environment and finally, a secure storage.
3. **Integrated TEEs**
   - *Trustonic* (proprietary) [12] allows devices to be embedded with a Trusted Identity, combining a secure OS (kernel and memory) along with a hardware-secured environment (e.g., Arm TrustZone chip). Trustonic is focused on mobile, automotive, banking, and IoT sectors and provides key features such as secure boot, secure data storage, secure execution, protecting connected hardware, and secure channels for application delivery.
   - *Solacia SecuriTEE* (proprietary) [11] is a hardware environment that provides security service for processors, peripherals, and storage devices, which is running on top of an Arm TrustZone chip. Additionally, the hardware environment is coupled with a secure kernel, which contains a trusted core environment, trusted function, and an integrated API for communication with the untrusted partition. The API adheres to the GlobalPlatform TEE mechanism.

An overview of the TEE architectural deployment is illustrated in Figure 1. This figure builds on top of existing TEE functional views [49] and extends it with the modules that are included in the existing TEE implementations. The figure depicts an untrusted as well as a trusted area, which

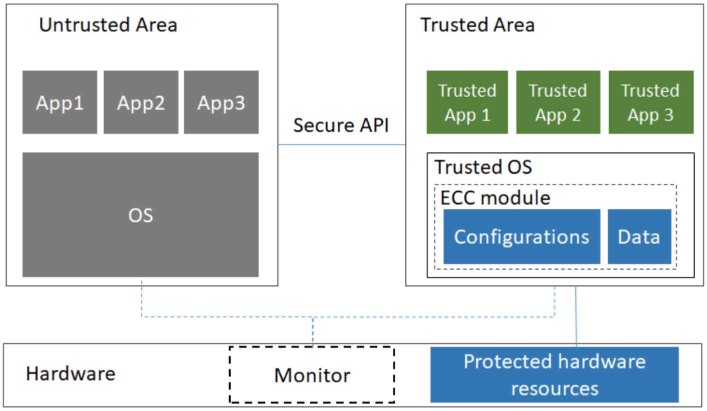

Figure 1. Trusted Execution Environment overview

communicates using the secure API. The Trusted Area uses kernel encryption and Elliptic Curve Cryptography (ECC) primitives to protect the data as well as the application and system configurations inside the operating system. Furthermore, trusted applications are meant to handle confidential information such as credit card PINs, private keys, and Digital Rights Management (DRM) protected media, among others, as well as providing services to the normal world OS to make use of confidential information without compromising it. Finally, dedicated hardware is used to protect the associate hardware resourcesin addition to enabling optional capabilities for switching between a secure and normal (i.e., untrusted) environment.

The offered security level of hardware-based and integrated TEE solution is significantly higher than a software-based TEE, mainly due to the higher safety that is offered by hardware encryption mechanisms. On the other hand, hardware-based encryption usually requires dedicated hardware, which results in a significant cost increase for such solutions. The advantages and disadvantages of each of the presented TEE categories towards the design of a TEEaaS platform are further described in Section 3.

2.3. Related work on TEEs application in 5G

Now, we review the main works combining TEE technologies with 5G and its enablers. Although 5G is a novel technology, there are already some works leveraging TEEs in its networking and solution context.

Ortiz et al. [47] considered TEEs as a game-changing technology in the security of virtualized environments in 5G networks, mainly in integrity and confidentiality perspectives. Here, TEEs are envisioned as a solution for virtual machine or container isolation mechanisms, preventing introspection attacks into the host machine. In [33], Elbashir analyzed how TEEs can be integrated with SDN solutions as a security enabler for 5G mobile networks. Concretely, this work proposed the usage of Intel SGX for TLS connection management (TLSonSGX) between switches deployed using Open vSwitch. In turn, the authors of [42] proposed a TEE abstraction layer for AMD's SEV and Intel's SGX which enables the secure deployment of SDN and NFV solutions. Similarly, [19] considered TEE for VNF (and its hypervisor) isolation and enhancing the security.

From a networking standpoint, Kim et al. [41] proposed the usage of TEEs for enhancing the security and privacy of a confidential networking solution. This approach was designed, deployed, and validated using the TOR's (The Onion Router) networking ecosystem. Besides, the idea of using TEEs for data protection in collaborative networks is explored in [25] in a vehicular network system context. From another perspective, the security architecture for 5G presented in [17] mentioned the TEE possible application in user equipment as a hardware secure layer for certificate and credential management.

As it can be seen, there are many works leveraging TEE technologies in the 5G context. However, none of them envisions the usage of TEEs as a service, offering to the customers additional trust and security properties for their services.

3. Design of the TEEaaS platform

A distributed and virtualized 5G network in a multi-stakeholder and multidomain third-party infrastructure creates a scenario where no inherent trust mechanisms can exist. Therefore, built-in security is paramount at all operational levels, from the hardware to the virtualized layers, but also covering both data and software. TEE-based software execution enables critical workloads to go across different tenants and stakeholders with no losses in security, by providing an isolated processing environment.

In this section, we start detailing how the usage of hardware-based TEEs provides a secure environment for deploying network components, such as VIMs and VNFs, in a third-party infrastructure. Later, we focus on the development of such functionalities by integrating commercial TEEs in the execution of some 5G network virtualized software components, enhancing the security and trust of the software executed under these capabilities. Besides, we also present a TEEaaS solution for 5G multi-domain networks inspired by the 5GZORRO H2020 project [27]. Finally, we end this section by presenting how such secure systems with TEEs can be designed to provide a trustworthy execution environment for 5G applications.

3.1. Secure environments for critical workloads

Protecting a tenant's service or application running on a third-party computing node against a malicious entity, with root and/or physical access, requires a root-of-trust built-in from the hardware. Zero trust hardware platforms, where both data and code are protected even from the infrastructure owner, enforce the necessary security to protect the application from two scenarios:

1. A malicious stakeholder wants to access/manipulate the data or code from a tenant running on its physical infrastructure.
2. A malicious third-party exploits vulnerability in the infrastructure to inadvertently access the computation node which is running the virtualized network modules and tampers with the execution.

TEE-based software execution ensures that only the code running inside the TEE can access its own data. Therefore, critical operations can be executed independently if the system, either hardware, software, or both, has been compromised. The separation between trusted and untrusted areas allows a malicious element to exploit security flaws in software without compromising the critical data and critical operations.

Since a TEE includes a zero trust hardware platform, a key component to establish a root-of-trust and end-to-end secure communications. the presence of these capabilities in the infrastructure offered by some stakeholders also improve the trust level perceived by service consumers, providing extra security at the hardware level to the resources and services offered by service providers.

TEEs are not a new technology by themselves. They are already mainstreamed in contactless payments and biometrics scans on mobile devices. In these scenarios, they enforce a secure enclave: a hardware-enforced separation between the untrusted and the trusted area. This separation allows a third-party application, service, or task to perform operations using critical data without exposing its access to this data or device, nor introducing attack vectors due to security flaws in its design.

The novelty element of the application of TEEs is to expand this concept of secure enclaves from mobile devices to a 5G telecommunications infrastructure, enabling two new use cases:

1. Deployment of network components such as VNFs, VIMs, and orchestration services in a third-party infrastructure [37].
2. Execution of secure oracles, DLTs nodes, authenticity proofs for smart contracts, and other critical operations, where neither the off-chain data nor its computation can be tampered [45, 55].

In the same way that mobile applications thrived when application marketplaces were introduced by mobile device manufacturers, distributed and virtualized telecommunications infrastructure is expected to thrive when similar marketplaces are introduced for VIMs, VNFs, and NFVs [24].

3.2. Suitable TEEs based on cloud infrastructure

In this section, we describe the applicable solutions for the cloud infrastructure-related TEEs, which are built on top of the solutions explained in Section 2 to separate secure from non-secure areas and create an isolated processing environment. These solutions are comprised of hardware, software, or both and can either run x86, Arm, or RISC-V Instruction Set Architecture (ISA).

While IoT devices can be a part of a telecommunication network [38], an Arm-based TEE suffers from a shortcoming: when compared with x86 or

RISC-V based TEEs, they can only have a single secure environment per processor. In a distributed and shared infrastructure, which supports concurrent execution and 5G physical medium access, it is desired that each computation node supports the instantiation of multiple, concurrent secure enclaves, so that multiple tenants can concurrently have a secure enclave allocated to themselves. While RISC-V based microprocessors and microcontrollers have been gaining traction in the last years [5], there are not yet mainstreamed, nor their TEEs modules are mature enough so that we can consider them as a viable commercial solution when compared to x86 solutions.

Therefore, in the context of a virtualized 5G network, x86-based TEEs will still dominate in the forthcoming years. It is worth noting that, due to the virtualization component of networks, the computation node that supports a TEE does not require to be near the edge, therefore, current cloud infrastructure can be used. This realization makes x86 the preferred TEE solution, due to its dominance in the Cloud-as-a-Service market. Since most of the market share for desktop and cloud processors is dominated by Intel, its TEEs are the most prevalent and available cloud-based solutions.

3.3. TEEaaS

Despite market trends, a solution for multi-domain, multi-stakeholder, and distributed 5G networks should be vendor-agnostic and independent of the TEE solution to which the infrastructure has access, as long as the infrastructure can guarantee certain capabilities. Due to the virtualized nature of the infrastructure, abstracting the low-level details of the commercial TEEs available and exposing only high-level tasks to any service or application is not only desired but necessary. By implementing an API for “TEEaaS” to allow the execution of modules in a secure enclave on the distributed 5G network:

- The know-how required to operate with hardware-based TEEs for secure enclaves is not required by the network engineers deploying the containerized network modules.
- New TEE solutions can be added seamlessly to the network infrastructure by different providers, without requiring the upper-level software modules to be ported to different hardware.

Besides, the TEEaaS platform should also offer capabilities to enable the execution of other simpler components and code, such as tasks manipulating critical data, improving the flexibility of the objects that can be deployed leveraging the TEE properties. In the scope of the 5GZORRO H2020 project and other 5G networks, containerized modules can be integrated with the orchestration services, allowing the deployment of critical services on TEE-enabled nodes present in the marketplace. In this regard, SCONE - Secure Linux Containers for Confidential Computing [9] is a framework that has been initially developed in the context of different H2020 projects (mostly Sereca [8] and Secure Cloud [10], while others have been exploiting it and enhancing it [9]). SCONE abstracts specific implementation details of the Intel’s SGX secure enclave, but also provides encryption at rest, in transit, and during runtime without requiring source code changes, supporting most modern program languages. It also has built-in attestation and key provisioning modules, allowing the application developers to focus on the orchestration and configuration of the security management solution and not on the security-solution implementation.

With a focus on the SCONE framework to enable TEE capabilities, the 5GZORRO H2020 project has adopted a hardware-based TEE approach, specifically Intel's SGX, in order to provide a TEEaaS solution for 5G multi-domain networks. When it comes to the instantiation of applications which are ready to be used in a TEE environment (i.e., Intel SGX), this functionality has not been altered, but it is now offered following a Cloud Native way. In other words, such services need only to be instantiated using Kubernetes or Docker with SCONE abstracting the interface within Intel SGX, and therefore, not requiring the definition of specific APIs. Furthermore, from a design point of view, there is no need to change the interface with other components, nor the high-level functional capabilities.

Hence, TEEaaS is expected to enhance 5GZORRO's ability not just to run 5GZORRO core components in a TEE environment (as an SLA monitoring service), but most importantly, the ability to offer consumers the capability to instantiate services in a pool of resources which may be untrusted by nature. For instance, a single and centralized instance of such a component will be enough to feed all subsequent TEE-powered NFVI for attestation and configuration purposes.

3.4. From TEEaaS to full application security

Integrating the TEEaaS with the current ETSI NFV MANO tools for 5G networks requires not only that the orchestrating services can deploy a custom application in a secure enclave, but also that the deployment of the application is performed ensuring end-to-end encryption and secure provisioning of the application, its data, and keys. 5G networks must protect data and software while they are running on the secure enclave, but also while data and code are in transit and at rest.

While multiple secure enclaves and TEE implementations are available, the TEEaaS is used to create a common layer for such secure enclaves. In this scope, a secure enclave on its own is only part of the solution to achieve a complete application-oriented security solution. Moreover, the TEEaaS allows the data and applications to be secure in all system states: during runtime, at rest, and in transit.

Such capabilities require that the application data and files must be encrypted such that they can only be accessed by the application itself. Hence, a TEE-based application should have access to the decryption keys, which implies the following steps:

1. An external module to the application must be responsible for managing the secrets and keys of the application. This module should also be

secured and capable of provisioning the secrets to a genuine application securely.

2. The application and data must be verified and prove to be genuine, i.e., that its code and data have not tampered with.
3. The tenant must be able to verify and attest that the host provided a tamper-free environment (secure enclave inside a TEE) for the tenant to run the application.
4. Secure, end-to-end encrypted communication must be established between the external module described in step 1 and the genuine application, running in a previously attested environment.

The above points must be fulfilled by the orchestration services, in order to ensure that the applications and corresponding data for a 5G network module are secure in all phases of its life cycle.

4. Current trends and future challenges

Given the demonstration of the main types of TEE solutions along with their prevalent properties and limitations, in this section, we focus on the trends and limitations of their offered mechanisms as well as of their adoption on 5G multi-domain environments. These trends reflect the path that the future TEE implementations will have to follow in order to, on the one hand, fill the current gaps associated with performance and integration issues, and on the other hand, meet the security and privacy-preserving challenges of such environments.

4.1. Current trends

A current trend towards the TEE adoption in 5G multi-domain environments is its integration with the VIM or NFVI components of the ETSI NFV MANO architecture [44]. One possible approach in this direction is provided by [53], which describes that a VIM with trusted execution capabilities is achieved by allowing isolation, both at the hardware and the software level for controller nodes. Isolation allows protecting the sensitive data of applications and services that are running on them. Specifically, a trusted VIM usually includes the following services: 1) secure boot process of both the controller and the compute nodes; 2) authentication process initiated by the controller node towards the compute nodes for avoiding man-in-the-middle attacks; and 3) kernel integrity check for both the controller node and the compute nodes to avoid the corruption of the kernel memory. An example of an integration of a trusted OP-TEE environment in the OpenStack VIM platform is illustrated in Figure 2.

TEEs are also used for data protection in 5G multi-domain environments. Specifically, the use of NFV technologies enables resource sharing in multi-tenant network slices, which may also lead to eavesdropping by unauthorized or malicious entities. A consequence of such a cyber-attack would be data leakage across tenant slices or even more severe resource damage (e.g., in

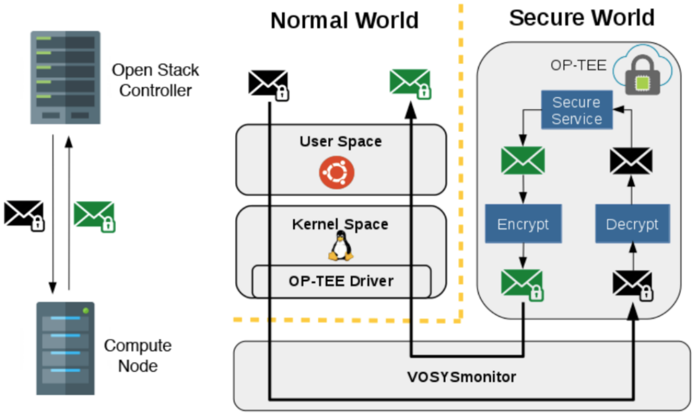

FIGURE 2. Trusted VIM with OpenStack [53]

the 5G Core Network [48]) that would tear down the 5G infrastructure. Furthermore, the use of blockchain mechanisms, such as DLT technologies, makes the 5G multi-domain environment more vulnerable to lateral movements that would propagate the attack across different DLT nodes. The application of a TEE would allow maintaining the transparency of the DLT, whilst ensuring the privacy of data and applications [18]. This is accomplished using the ECC module (see Figure 1) that encrypts the data associated with each transaction and stored locally in each DLT node. Apart from the data, keeping the bids secret is also of primary importance, so that neither another DLT node nor any other party can learn anything about them. Hence, encryption is also added to the transaction bids and the key to decrypt them resides only inside the trusted environment. In this way whenever each DLT node commits a bid in the blockchain, it is always encrypted and only trusted recipients that have the key can decrypt the bid to visualize the underlying transaction. Trust can be established using dedicated authentication or authorization methods. Encryption of the transaction bids ensures both the privacy and trustworthiness of data being exchanged between different DLT nodes.

Based on a literature review of the current trends and implementations, the following TEE mechanisms are feasible in 5G multi-domain environments, such as the one provided by 5GZORRO:

1. *Intra-domain TEE*, in which the functional modules that are related to communication inside an administrative resource domain are executed securely through the presence of a software- or hardware-based TEE. Additionally, such TEE allows the function modules to exchange data in a protected manner. Each domain also includes an untrusted area, which has modules that are not executed inside a TEE component. The interactions between the intra-domain TEE and the untrusted area of a domain take place through secure internal channels to avoid a potential compromise of the intra-domain TEE.

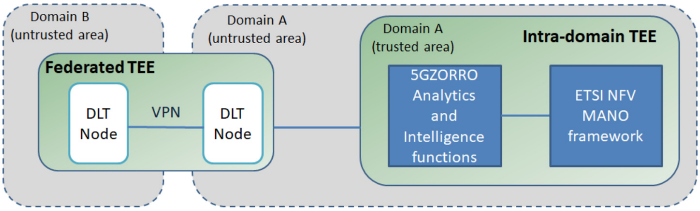

Figure 3. TEE mechanisms for 5G multi-domain environments

2. *Federated TEE*, which focuses on the protection of the communication between different administrative resource domains. Such TEE could extend tunneling mechanisms for the protection of data exchange as well as to prevent eavesdropping from malicious entities.

These mechanisms are illustrated with an example within the scope of 5GZORRO in Figure 3. Specifically, the Intra-domain TEE includes Analytics and Intelligence functions that are used for the automation of complex resource management procedures, such as the proactive scaling mechanism to increase or decrease the mobile infrastructure capacity through third-party resources based on tenant or user demands. These functions usually reside in the same administrative domain with the ETSI NFV MANO framework and inform it of any updates on the existing 5G network slices. On the other hand, DLT nodes of a blockchain environment are distributed across different domains offered services and hence are using Federated TEE mechanisms to communicate, such as the VPN mechanism that is shown in Figure 3. The presence of a VPN ensures that the data remains protected when they are transmitted from one domain to another.

Even if the TEE mechanisms are already used for increasing the cyber-resilience in various application domains, their implementation on 5G multi-domain environments faces challenges as it does not cover the entire mobile network infrastructure. This is due to the hesitant nature of Mobile Network Operators (MNOs) towards changes that would interrupt the normal operation of their network and the services offered to their customers. Furthermore, if these changes occasionally involve the presence of new hardware as with hardware-based TEEs this hesitation becomes even greater. Moreover, even with the presence of TEEs a 5G infrastructure and the multi-domain environment is not adequately secure as additional challenges are also involved. These challenges are presented in the following section.

4.2. Future challenges

The wide variety of 5G scenarios, where TEE may be applied, brings with it numerous challenges to be fulfilled through enriching current solutions with advanced technological approaches and features. In particular, the next challenges are principally centered on potential threats associated with TEE solutions, the impediment of employing TEE solutions in certain environments or contexts due to the performance, and finally, the agnosticism required by TEE solutions to be deployed or instantiated in multiple 5G enablers.

- **Pivotal threats and vulnerabilities**. One of the most significant challenges of TEE solutions is the threats related to microarchitectural attacks. Concretely, some of these paramount threats arise since TEE solutions intend to maximize performance gains. That is the case of side-channel attacks, one of the most well-known as identified in [39]. By means of this attack, an adversary may acquire user sensitive meta-information since it intends to discover the memory access patterns, and then, these patterns are exploited to infer target information. In fact, outstanding solutions such as Intel SGX [26] and Arm TrustZone [60] are not completely exempt from this attack. Another reiterated attack on TEEs is the transient execution [57], in which an adversary exploits the out-of-order execution of CPUs to leak actual data. In contrast to the side-channel attack, the transient execution attack is mostly applied to Intel SGX solutions [52]. Finally, two further cyber-attacks are related to fake secure enclaves [31] and fault attacks [52], which are both associated with Intel SGX approaches. The first attack occurs when enclaves are not able to withstand memory corruption errors, and therefore, an attacker may partially execute arbitrary code inside the enclave. The second one is linked to tampering computations for deflecting data or control flow, as well as to the disruption of code or data.
- **Performance**. Due to the additional operations required to securely execute the tasks in the TEEs, the performance of the execution can be considerably downgraded. The impact is conditioned by the number and complexity of additional processing steps inside the TEE, so minimizing them without losing security properties is a key challenge in TEE applicability. Besides, TEE usage can require specific configuration and optimization, so it is critical to facilitate these steps. In this sense, Akram et al. analyzed in [14] how high-performance computing related to scientific tasks is affected when running on hardware-based TEEs (Intel SGX and AMD SEV). They showed how execution performance is considerably degraded when using default configurations. However, a proper configuration can secure the computing tasks without significant performance degradation, mainly in AMD SEV.
- **Agnostic solutions**. Since the use of TEEs ranges from embedded sensors to cloud servers, while considering a range of security risks [56], power constraints, and cost choices, it is crucial to abstract the complexity of TEE designs from their integration in dynamic environments. In this regard, vendors should analyze the feasibility of hardware-based, software-based, and integrated TEEs to facilitate their deployment and/or integration in multiple 5G enablers such as SDNs, NFVs, and DLTs. Thus, an organization named GlobalPlatform [2] is working on developing and publishing standards for TEE-related interfaces and implementations. At the software level, there are solutions such

as OP-TEE [6] (using the TrustZone technology) that has support for the GlobalPlatform TEE Client API. In addition, this approach is being addressed in several areas of current literature, to name a few, the trusted VIM in the cloud and edge environments [53] or IoT devices [36]. Nonetheless, while there are many hardware solutions that can support a TEE, there are not enough agnostic approaches to apply a software-based TEE solution to multiple hardware-based TEE solutions.

Inasmuch as the above-mentioned trends and challenges, it is possible to gather a set of research lines that should be considered for future developments of TEE solutions. In that sense, the forthcoming investigations will mainly focus on the TEE consideration in 5G multi-domain and multi-stakeholder environments, as well as its integration with existing NFV MANO architectures and their crucial components such as VIMs and NFVIs.

5. Conclusions and future work

The present chapter has shown a proposal for integrating the use of a hardware-based TEE solution, like SCONE, with 5G technologies, which enables the deployment of network components in third-party infrastructures. The proposed TEEaaS framework attempts not only to cover security and trust aspects under 5G core network components such as VIMs or VNFs, but also to consider pivotal performance and delay requirements. Thus, the proposed boosts the trustworthy execution of offloading critical data and processes on demand. In particular, the TEEaaS framework is developed considering the 5GZORRO H2020 project requirements and properties, where the trading of heterogeneous resources among stakeholders is contemplated to make easier the establishment of thoroughly pervasive services across different domains. Furthermore, a set of current trends and future challenges has been recognized during the state-of-the-art review and design phase, which will be considered during the development phase.

As future work, we plan to finish the implementation of the TEEaaS framework, since it should enable its deployment and integration with other 5GZORRO resources such as SLA monitoring. Additionally, the framework design will be aligned with the trends and challenges that have been discussed in this book chapter. To validate the suitability of the proposed solution, we plan to carry out a Proof-of-Concept (PoC) which will protect not only data and software while running on the secure enclave, but also while data is in transit and at rest. Finally, we plan to use the PoC to measure the resilience of well-known threats and vulnerabilities, and on the other hand, the fulfillment of performance requirements in 5G multi-domain networks.

Acknowledgment

This work has been supported by the European Commission through 5GZORRO project (grant no. 871533) part of the 5G PPP in Horizon 2020. 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] Genode - An exploration of Arm TrustZone technology. https://genode.org/documentation/articles/trustzone. Accessed: 2021-05-04

[2] GlobalPlatform. https://globalplatform.org/. Accessed: 2021-05-04

[3] GlobalPlatform device technology. TEE client API specification. https://globalplatform.org/specs-library/tee-client-api-specification/. Accessed: 2021-05-04

[4] Intel Trusted Execution Technology (Intel TXT) overview. https://www.intel.com/content/www/us/en/support/articles/000025873/technologies.html. Accessed: 2021-05-04

[5] Multizone security for RISC-V. https://hex-five.com/multizone-security-sdk/. Accessed: 2021-05-04

[6] Open Portable Trusted Execution Environment (OP-TEE). https://github.com/OP-TEE. Accessed: 2021-05-04

[7] SDN 5G threat analysis: An ENISA case study. https://www.charisma5g.eu/wp-content/uploads/2016/07/SDN5G-Threat-Analysis-An-ENISA-case-study.pdf. Accessed: 2021-05-04

[8] Secure Enclaves for Reactive Cloud Applications (SERECA) project. https://www.serecaproject.eu. Accessed: 2021-05-04

[9] Secure Linux Containers (SCONE). https://sconedocs.github.io/aboutScone/. Accessed: 2021-05-04

[10] SecureCloud. https://www.securecloudproject.eu/. Accessed: 2021-05-04

[11] Solacia SecuriTEE. https://www.insidesecure.com/Company/Press-releases/Inside-Secure-AND-SOLACIA. Accessed: 2021-05-04

[12] Trusted Executed Environment (TEE), Trustonic. https://www.trustonic.com/technical-articles/what-is-a-trusted-execution-environment-tee/. Accessed: 2021-05-04

[13] Trusted Little Kernel. https://trustedfirmware-a.readthedocs.io/en/latest/components/spd/tlk-dispatcher.html. Accessed: 2021-05-04

[14] Akram, A.: Performance analysis of scientific computing workloads on general purpose TEEs. In: 35th IEEE International Parallel & Distributed Processing Symposium (IPDPS). IEEE (2021)

[15] Alrawais, A., Alhothaily, A., Hu, C., Xing, X., Cheng, X.: An attribute-based encryption scheme to secure fog communications. IEEE Access **5**, 9131–9138 (2017)

[16] Amacher, J., Schiavoni, V.: On the performance of arm trustzone. In: IFIP International Conference on Distributed Applications and Interoperable Systems, pp. 133–151. Springer (2019)

[17] Arfaoui, G., Bisson, P., Blom, R., Borgaonkar, R., Englund, H., Félix, E., Klaedtke, F., Nakarmi, P.K., Näslund, M., O'Hanlon, P., et al.: A security architecture for 5G networks. IEEE Access **6**, 22466–22479 (2018)

[18] Ayoade, G., Karande, V., Khan, L., Hamlen, K.: Decentralized IoT data management using blockchain and trusted execution environment. In: 2018 IEEE International Conference on Information Reuse and Integration (IRI), pp. 15–22. IEEE (2018)

[19] Baldoni, G., Cruschelli, P., Paolino, M., Meixner, C.C., Albanese, A., Papageorgiou, A., Khalili, H., Siddiqui, S., Simeonidou, D.: Edge computing enhancements in an NFV-based ecosystem for 5G neutral hosts. In: 2018 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), pp. 1–5. IEEE (2018)

[20] Bangerter, B., Talwar, S., Arefi, R., Stewart, K.: Networks and devices for the 5G era. IEEE Communications Magazine **52**(2), 90–96 (2014)

[21] Barros Lourenço, M., Marinos, L., Patseas, L.: ENISA threat landscape for 5G networks. Tech. rep., European Union Agency for Cybersecurity (2020)

[22] Bendriss, J., Yahia, I.G.B., Chemouil, P., Zeghlache, D.: AI for SLA management in programmable networks. In: DRCN 2017-Design of Reliable Communication Networks; 13th International Conference, pp. 1–8. VDE (2017)

[23] Bhushan, K., Gupta, B.B.: Distributed denial of service (DDoS) attack mitigation in software defined network (SDN)-based cloud computing environment. Journal of Ambient Intelligence and Humanized Computing **10**(5), 1985–1997 (2019)

[24] Bondan, L., Franco, M.F., Marcuzzo, L., Venancio, G., Santos, R.L., Pfitscher, R.J., Scheid, E.J., Stiller, B., De Turck, F., Duarte, E.P., et al.: FENDE: marketplace-based distribution, execution, and life cycle management of VNFs. IEEE Communications Magazine **57**(1), 13–19 (2019)

[25] Boos, P., Lacoste, M.: Networks of trusted execution environments for data protection in cooperative vehicular systems. In: Vehicular Ad-hoc Networks for Smart Cities, pp. 99–109. Springer (2020)

[26] Brasser, F., Müller, U., Dmitrienko, A., Kostiainen, K., Capkun, S., Sadeghi, A.R.: Software grand exposure: SGX cache attacks are practical. In: 11th USENIX Workshop on Offensive Technologies (WOOT) (2017)

[27] Carrozzo, G., Siddiqui, M.S., Betzler, A., Bonnet, J., Perez, G.M., Ramos, A., Subramanya, T.: 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), pp. 254–258. IEEE (2020)

[28] Celdran, A.H., Perez, M.G., Clemente, F.J.G., Perez, G.M.: Enabling highly dynamic mobile scenarios with software defined networking. IEEE Communications Magazine **55**(4), 108–113 (2017)

[29] Celdrán, A.H., Pérez, M.G., Clemente, F.J.G., Pérez, G.M.: Towards the autonomous provision of self-protection capabilities in 5G networks. Journal of Ambient Intelligence and Humanized Computing **10**(12), 4707–4720 (2019)

[30] Chhabra, M., Gupta, B., Almomani, A.: A novel solution to handle DDOS attack in MANET (2013)

[31] Cloosters, T., Rodler, M., Davi, L.: TeeRex: Discovery and exploitation of memory corruption vulnerabilities in SGX enclaves. In: 29th USENIX Security Symposium (USENIX Security 20), pp. 841–858 (2020)

[32] Costan, V., Devadas, S.: Intel SGX explained. Cryptology ePrint Archive, Report 2016/086 (2016). `https://eprint.iacr.org/2016/086`

[33] Elbashir, K.: Trusted execution environments for open vswitch: A security enabler for the 5G mobile network (2017)

[34] Elgendy, I.A., Zhang, W., Tian, Y.C., Li, K.: Resource allocation and computation offloading with data security for mobile edge computing. Future Generation Computer Systems **100**, 531–541 (2019)

[35] Esposito, C., Ficco, M., Gupta, B.B.: Blockchain-based authentication and authorization for smart city applications. Information Processing & Management **58**(2), 102468 (2021)

[36] Göttel, C., Felber, P., Schiavoni, V.: Developing secure services for IoT with OP-TEE: a first look at performance and usability. In: IFIP International Conference on Distributed Applications and Interoperable Systems, pp. 170–178. Springer (2019)

[37] Guerzoni, R., Vaishnavi, I., Perez Caparros, D., Galis, A., Tusa, F., Monti, P., Sganbelluri, A., Biczók, G., Sonkoly, B., Toka, L., et al.: Analysis of end-to-end multi-domain management and orchestration frameworks for software defined infrastructures: an architectural survey. Transactions on Emerging Telecommunications Technologies **28**(4), e3103 (2017)

[38] Gupta, B., Quamara, M.: An overview of internet of things (IoT): Architectural aspects, challenges, and protocols. Concurrency and Computation: Practice and Experience **32**(21), e4946 (2020)

[39] Jauernig, P., Sadeghi, A.R., Stapf, E.: Trusted execution environments: properties, applications, and challenges. IEEE Security & Privacy **18**(2), 56–60 (2020)

[40] Jiang, F., Fu, Y., Gupta, B.B., Liang, Y., Rho, S., Lou, F., Meng, F., Tian, Z.: Deep learning based multi-channel intelligent attack detection for data security. IEEE Transactions on Sustainable Computing **5**(2), 204–212 (2020). DOI 10.1109/TSUSC.2018.2793284

[41] Kim, S., Han, J., Ha, J., Kim, T., Han, D.: Enhancing security and privacy of Tor's ecosystem by using trusted execution environments. In: 14th USENIX Symposium on Networked Systems Design and Implementation (NSDI), pp. 145–161 (2017)

[42] Lefebvre, V., Santinelli, G., Müller, T., Götzfried, J.: Universal trusted execution environments for securing SDN/NFV operations. In: 13th International Conference on Availability, Reliability and Security, pp. 1–9 (2018)

[43] Liu, Y., An, K., Tilevich, E.: RT-Trust: Automated refactoring for different trusted execution environments under real-time constraints. Journal of Computer Languages **56**, 100939 (2020)

[44] Mijumbi, R., Serrat, J., Gorricho, J.L., Latré, S., Charalambides, M., Lopez, D.: Management and orchestration challenges in network functions virtualization. IEEE Communications Magazine **54**(1), 98–105 (2016)

[45] Nour, B., Ksentini, A., Herbaut, N., Frangoudis, P.A., Moungla, H.: A blockchain-based network slice broker for 5G services. IEEE Networking Letters **1**(3), 99–102 (2019)

[46] Ordonez-Lucena, J., Ameigeiras, P., Lopez, D., Ramos-Munoz, J.J., Lorca, J., Folgueira, J.: Network slicing for 5G with SDN/NFV: Concepts, architectures, and challenges. IEEE Communications Magazine **55**(5), 80–87 (2017)

[47] Ortiz, J., Sanchez-Iborra, R., Bernabe, J.B., Skarmeta, A., Benzaid, C., Taleb, T., Alemany, P., Muñoz, R., Vilalta, R., Gaber, C., et al.: INSPIRE-5Gplus: Intelligent security and pervasive trust for 5G and beyond networks. In: 15th International Conference on Availability, Reliability and Security, pp. 1–10 (2020)

[48] Park, S., Choi, B., Park, Y., Kim, D., Jeong, E., Yim, K.: Vestiges of past generation: Threats to 5G core network. In: International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, pp. 468–480. Springer (2020)

[49] Sabt, M., Achemlal, M., Bouabdallah, A.: Trusted execution environment: what it is, and what it is not. In: 2015 IEEE Trustcom/BigDataSE/ISPA, vol. 1, pp. 57–64. IEEE (2015)

[50] Sangorrín, D., Honda, S., Takada, H.: Reliable and efficient dual-OS communications for real-time embedded virtualization. Information and Media Technologies **8**(1), 1–17 (2013)

[51] Santos, N., Raj, H., Saroiu, S., Wolman, A.: Using Arm TrustZone to build a trusted language runtime for mobile applications. In: 19th International Conference on Architectural Support for Programming Languages and Operating Systems, pp. 67–80 (2014)

[52] Schwarz, M., Gruss, D.: How trusted execution environments fuel research on microarchitectural attacks. IEEE Security & Privacy **18**(5), 18–27 (2020)

[53] Sechkova, T., Barberis, E., Paolino, M.: Cloud & edge trusted virtualized infrastructure manager (VIM)-security and trust in OpenStack. In: 2019 IEEE Wireless Communications and Networking Conference Workshop (WCNCW), pp. 1–6. IEEE (2019)

[54] Stergiou, C.L., Psannis, K.E., Gupta, B.B.: IoT-based big data secure management in the fog over a 6G wireless network. IEEE Internet of Things Journal (2020)

[55] Swapna, A.I., Rosa, R.V., Rothenberg, C.E., Sakellariou, I., Mamatas, L., Papadimitriou, P.: Towards a marketplace for multi-domain cloud network slicing: Use cases. In: 2019 ACM/IEEE Symposium on Architectures for Networking and Communications Systems (ANCS), pp. 1–4. IEEE (2019)

[56] Tewari, A., Gupta, B.: Security, privacy and trust of different layers in internet-of-things (IoTs) framework. Future Generation Computer Systems **108**, 909–920 (2020)

[57] Van Bulck, J., Minkin, M., Weisse, O., Genkin, D., Kasikci, B., Piessens, F., Silberstein, M., Wenisch, T.F., Yarom, Y., Strackx, R.: Foreshadow: Extracting the keys to the intel SGX kingdom with transient out-of-order execution. In: 27th USENIX Security Symposium (USENIX Security 18), pp. 991–1008 (2018)

[58] Xiao, Y., Zhang, N., Li, J., Lou, W., Hou, Y.T.: PrivacyGuard: Enforcing private data usage control with blockchain and attested off-chain contract execution. In: European Symposium on Research in Computer Security, pp. 610–629. Springer (2020)

[59] Xu, S., Qian, Y., Hu, R.Q.: Privacy-preserving data preprocessing for fog computing in 5G network security. In: 2018 IEEE Global Communications Conference (GLOBECOM), pp. 1–6. IEEE (2018)

[60] Zhang, N., Sun, K., Shands, D., Lou, W., Hou, Y.T.: TruSpy: Cache side-channel information leakage from the secure world on Arm devices. Cryptology ePrint Archive, Report 2016/980 (2016). https://eprint.iacr.org/2016/980

[61] Zhu, J., Hou, R., Wang, X., Wang, W., Cao, J., Zhao, B., Wang, Z., Zhang, Y., Ying, J., Zhang, L., Meng, D.: Enabling rack-scale confidential computing using heterogeneous trusted execution environment. In: 2020 IEEE Symposium on Security and Privacy (SP), pp. 1450–1465 (2020). DOI 10.1109/SP40000.2020.00054

José María Jorquera Valero
Department of Information and Communications Engineering
University of Murcia
30100 Murcia
Spain
e-mail: josemaria.jorquera@um.es

Pedro Miguel Sánchez Sánchez
Department of Information and Communications Engineering
University of Murcia
30100 Murcia
Spain
e-mail: pedromiguel.sanchez@um.es

Alexios Lekidis
Intracom Telecom
190 02 Athens
Greece
e-mail: alekidis@intracom-telecom.com

Pedro Martins
Ubiwere
3800-075 Aveiro
Portugal
e-mail: pmartins@ubiwhere.com

Pedro Diogo
Ubiwere
3800-075 Aveiro
Portugal
e-mail: pdiogo@ubiwhere.com

Manuel Gil Pérez
Department of Information and Communications Engineering
University of Murcia
30100 Murcia
Spain
e-mail: mgilperez@um.es

Alberto Huertas Celdrán
Department of Information and Communications Engineering
University of Murcia
30100 Murcia
Spain
e-mail: alberto.huertas@um.es

Gregorio Martínez Pérez
Department of Information and Communications Engineering
University of Murcia
30100 Murcia
Spain
e-mail: gregorio@um.es