The Roadmap to 6G Security and Privacy

Pawani Porambage*, *Member, IEEE,* Gürkan Gür, *Senior Member, IEEE,* Diana Pamela Moya Osorio, *Member, IEEE,* Madhusanka Liyanage, *Senior Member, IEEE,* Andrei Gurtov, *Senior Member, IEEE* and Mika Ylianttila, *Senior Member, IEEE*

***Abstract*—Although the fifth generation (5G) wireless networks are yet to be fully investigated, the visionaries of the 6th generation (6G) echo systems have already come into the discussion. Therefore, in order to consolidate and solidify the security and privacy in 6G networks, we survey how security may impact the envisioned 6G wireless systems, possible challenges with different 6G technologies, and the potential solutions. We provide our vision on 6G security and security key performance indicators (KPIs) with the tentative threat landscape based on the foreseen 6G network architecture. Moreover, we discuss the security and privacy challenges that may encounter with the available 6G requirements and potential 6G applications. We also give the reader some insights into the standardization efforts and research-level projects relevant to 6G security. In particular, we discuss the security considerations with 6G enabling technologies such as distributed ledger technology (DLT), physical layer security, distributed AI/ML, visible light communication (VLC), THz, and quantum computing. All in all, this work intends to provide enlightening guidance for the subsequent research of 6G security and privacy at this initial phase of vision towards reality.**

***Index Terms*—6G, Security, Security threats, AI/ML security, DLT, Physical Layer Security, Privacy, Quantum computing.**

I. Introduction

The evolution of wireless communication technologies started from the first generation cellular networks (1G) in the 1980s. By then, significant advancements have been added to the telecommunication and networking industries during 2G, 3G and 4G cellular networks. The era of fifth generation (5G) wireless technologies has been already in deployment phase since 2020, and it is yet to be evolved mostly on software-based till the 2025 with the full coverage. The most remarkable feature in 5G is the cloudification of networks with the microservice-based architecture. This provides and abstraction of physical resources to virtual and logical environments introducing on-demand automated learning management functions.

Sixth generation (6G) of mobile communication is already envisioned by the researchers despite the fact that 5G coverage is not yet being fully provided. Although it is expected that 6G standardization will start somewhere 2026, the research community has already started looking for novel research directions towards materializing 6G vision. Networking and communication scientific community envisage that 6G wireless networks will be driven by entirely intelligent network orchestration and management [2], [3]. This is going to be achieved with multiple technologies such as reconfigurable intelligent surfaces (RIS), visible light communications (VLC), electromagnetic–orbital angular momentum, cell-free communications, and quantum computing [4]. The driving elements of 5G evolution such as virtual radio access networks (vRANs) and cloudified core network are projecting the basis of 6G architectural framework. As stated in [5], 6G architecture is evolving in terms of platform, functional architecture, specializations and orchestration. Regarding the platform, heterogeneous cloud infrastructure are expected in 6G architecture to achieve optimal Network Function (NF) execution [6]. This needs the capability to discover the service that multiple clouds are offering and the dynamic function placement. The functional architecture requires new functionalities including, not limited to, RAN-core convergence, cell free radio and information collection for AI at physical and management layers. Novel means of specialization are also anticipated such as personal subnetworks, extreme slicing and flexible workload offloading [7]. In the management of 6G cognitive networks, the orchestration is based on the cognitive closed loop and automation.

The security and privacy considerations in the envisioned 6G networks need to be addressed with respect to many areas. There are specific security issues that may arise with the novel 6G architectural framework as stated above. In addition to that, there are many hypes on blending novel technologies such as blockchain, VLC, TeraHertz (THz), and quantum computing features in 6G intelligent networking paradigms in such a way to tackle the security and privacy issues. Therefore, 6G security considerations need to be also discussed with respect to the physical layer security (PLS), network information security, application security and deep learning related security [1], [8].

A. Evolution of Mobile Security

The early generations of mobile networks (i.e., 1G, 2G, 3G) encountered with significant security and privacy challenges including cloning, illegal physical attacks, eavesdropping, encryption issues, authentication and authorization problems, and privacy issues [9]. Then, the security threat landscape has been evolved with more advanced attack scenarios and powerful

Pawani Porambage*, Diana Pamela Moya Osorio and Mika Ylianttila are with the Centre for Wireless Communications, University of Oulu, Finland. email: firstname.lastname@oulu.fi

Gürkan Gür is with the Zurich University of Applied Sciences (ZHAW), Institute of Applied Information Technology (InIT), Switzerland, email: gueu@zhaw.ch

Madhusanka Liyanage is with the School of Computer Science, University College Dublin (UCD), Ireland and the Centre for Wireless Communications, University of Oulu, Finland. e-mail:madhusanka@ucd.ie, madhusanka.liyanage@oulu.fi

Andrei Gurtov is with Department of Computer and Information Science, Linköping University, Sweden, email: andrei.gurtov@liu.se

*Corresponding author

This work is an extension of the short paper (6 pages) which is accepted to 2021 Joint EuCNC & 6G Summit. The conference paper is entitled as "6G Security Challenges and Potential Solutions" [1].

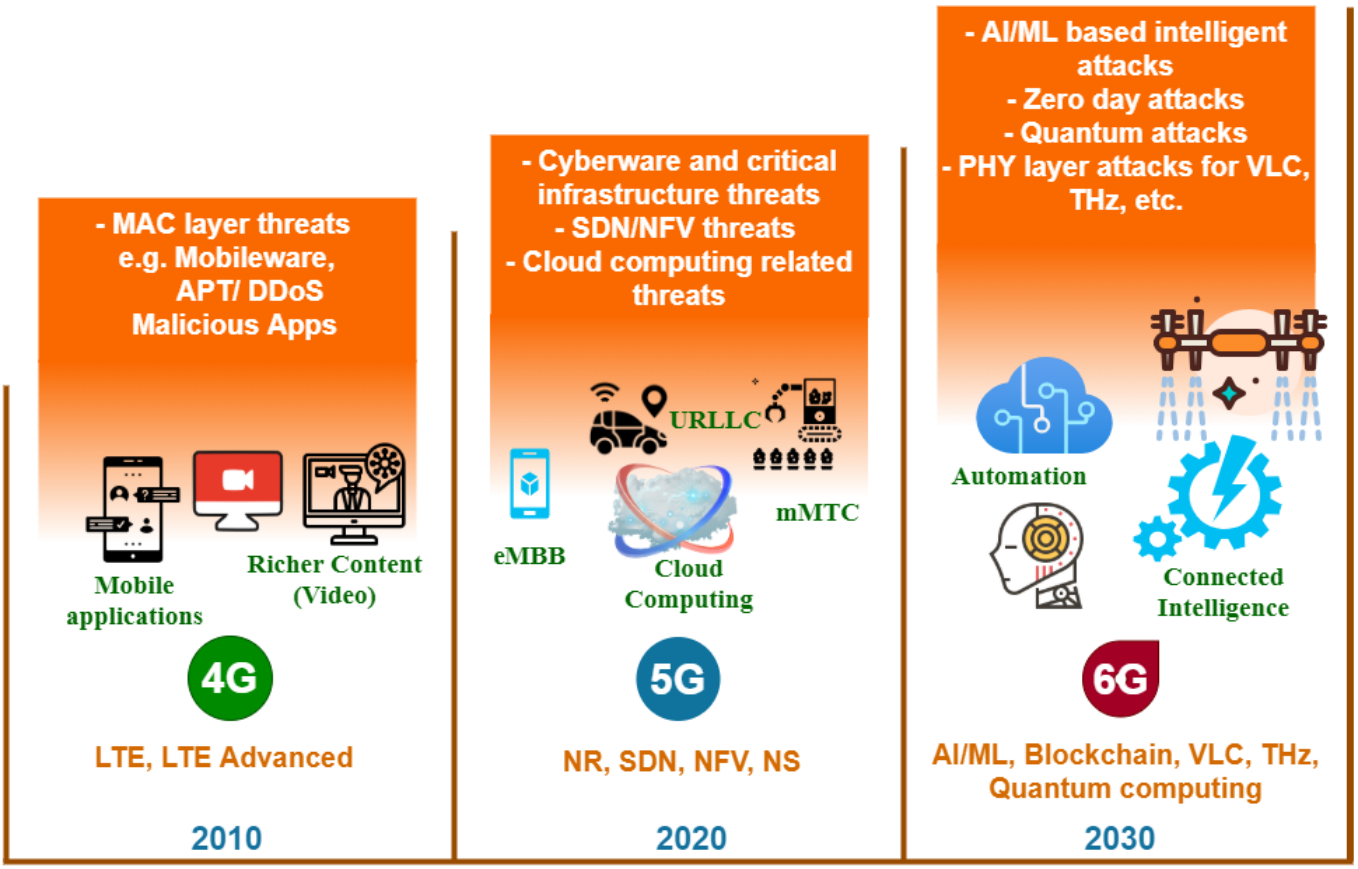

Fig. 1: Evolution of Mobile Security Landscape from 4G towards 6G

attackers. The evolution of security landscape of telecommunication networks, from 4G towards the envisioned 6G era, is illustrated in Figure 1. 4G networks faced security and privacy threats mainly due to the execution of wireless applications. The typical examples include Media access control (MAC) layer security threats (e.g., denial of service (DoS) attacks, eavesdropping, replay attacks) and malware applications (e.g., viruses, tampering into hardware).

In the 5G architecture, security and privacy threats are causing at access, backhaul and core networks [10]. Cyberware and critical infrastructure threats, Network Functions Virtualization (NFV) and Software-Defined Networking (SDN) related threats, and cloud computing related threats are the most common security issues in 5G [11]. There are numerous occasions that SDN may create security threats, such as by exposing critical Application Programming Interfaces (APIs) to unintended software, the inception of OpenFlow, and centralizing the network control (i.e., subject to DoS attacks) [12]. Above all, the most significant driving force in 6G vision is the added connected intelligence in the telecommunication networks accompanied with advanced networking and AI/ML technologies. However the alliance between AI and 6G may also be a double edge sword in many cases while applying for protecting or infringing security and privacy [13].

B. Motivation

Irrespective of the advancements of networking and communication technologies, security is always a paramount feature to consider to ensure the resilience and reliability of networks. Therefore, it will be useful to the research community to identify the security related research directions in the envisioned 6G networks. Since the standard functions and specifications of 6G are yet to be defined, still there is a limited number of literature that provides security and privacy insights of beyond 5G networks. Furthermore, it is necessary to build on 5G research in a methodical way and consolidate existing emerging research towards 6G security realization. Already there are many 6G vision papers available [14]–[17], however, as summarized in Table I, only a handful of surveys have been released with the key focus on 6G security and privacy. In the existing surveys, none of the articles cover the holistic picture of 6G security with respect to the expected novelties and advancements that 6G intends to bring in terms of architectural and technological aspects, and application areas. Therefore, our main motivation is to shed the light on how security may impact on the envisioned 6G wireless systems with the possible challenges and the potential solutions while identifying the future research areas.

C. Our Contribution

Given the fact that 6G networks are yet to be discovered around ten years ahead, it is interesting to study the security

TABLE I: Surveys on 6G security and privacy

Ref.	Contribution
[18]	This white paper provides a high-level discussion on the role of of trust, security, and privacy in the 6G networks and the respective research challenges.
[9]	Presents a concise survey on new research areas and challenges in security and privacy with respect to four key aspects of 6G networks such as real-time intelligent edge computing, distributed artificial intelligence, intelligent radio, and 3D intercoms. Discusses the security and privacy issues on emerging technologies including AI-based software, blockchain, quantum communications, TeraHertz (THz) technology, Visible Light Communication (VLC) technology, and molecular communications.
[19]	Provides a comprehensive survey of ML and privacy in 6G, with a view to further promoting the development of 6G and privacy protection technologies.
[20]	Provides a comprehensive road-map on important relevant results on physical layer security (PLS) and discusses open issues on the applicability of PLS in 6G systems.

and privacy aspects of 6G networks in different angles. Therefore, throughout the entire article we try to compile the future research directions in 6G security and relate how they may evolve with the current research works. Our key contributions in this article are as follows:

- **To explore driving trends, visions, applications, requirements and key enabling technologies related to 6G security and privacy:** This paper provides a brief survey mentioning the security and privacy challenges that may encounter with the expecting 6G requirements, security key performance indicators (KPIs), novel network architecture, new applications and enabling technologies.
- **To identify threat landscape and possible solutions related to 6G security:** The paper surveys the potential security solutions for 6G in terms of distributed ledger technology (DLT), physical layer security, quantum communication, distributed AI/ML.
- **To present a road map for materializing 6G security visions into a reality:** The paper introduces the standardization efforts and renowned research projects that are leading towards 6G security visionaries putting into practice.

D. Outline

The remainder of the paper is organized as follows: Section II presents the 6G security requirements and challenges in general. This section also discusses the potential 6G security KPIs and the security issues with respect to different 6G architectural components. Section III describes the security related issues that may encounter with the main 6G applications. Section IV focuses on security impact on novel 6G technologies. Respectively, Section V and VI respectively provide an overview on 6G privacy issues/possible solutions and security standardization efforts. Finally, Section VII provides the discussion and Section VIII concludes the paper.

II. 6G Security Requirements and Challenges

In this section, we first provide an overview about novel 6G requirements in general. Then we discuss the security considerations, 6G security vision and the potential security KPIs. The last subsections describe the security landscape for the envisioned 6G architecture which is classified into four key areas such as functional architecture (i.e., intelligent radio and radio-core convergence), edge intelligence and cloudification, specialized subnetworks, and network management and orchestration.

A. New 6G Requirements

Future 6G applications will pose stringent requirements and require extended network capabilities compared with the currently developed 5G networks. These requirements are summarized in Figure 2. They are established to enable the wide range of key 6G use cases and thus can be categorized accordingly. For **Further enhanced Mobile Broadband (FeMBB)**, the mobile connection speed has to reach the peak data rate at Tbps level [21]. With **Ultra massive Machine Type Communication (umMTC)**, the connection density will further increase in 6G due to the novel concept of Internet of Everything (IoE) as the next phase of Internet of Things (IoT). These devices will have to communicate with each other and the infrastructure, and provide collaborative services in an autonomous and self-driven manner [22]. For new latency extremely-sensitive 6G applications in the **Enhanced Ultra-Reliable, Low-Latency Communication (ERLLC/eURLLC)** use case, the E2E latency in 6G should be reduced down to μs level [23]. 6G will require the network energy efficiency to be improved by 10x than 5G and 100x than 4G. It is also expected to enable extremely low power communications for the resource constrained devices [23]. Moreover, intelligent and proactive mobility management systems will support seamless and instant mobility beyond 1000 kmph speeds [21].

For ERLLC, the latency impact of security workflows will be considered to ensure service quality. Similarly, high reliability requirements calls for very efficient security solutions protecting availability of services and resources. With FeMBB, extreme data rates will pose challenges regarding traffic processing for security such as attack detection, AI/ML pipelines, traffic analysis and pervasive encryption. That issue can be alleviated with distributed security solutions since traffic should be processed locally and on-the-fly in different segments of the network, ranging from the edge to the core service cloud [24]. At this point, DLT will be instrumental with transparency, security and redundancy attributes. umMTC will serve critical use-cases which impose much more stringent security requirements compared to 5G. In particular, IoE with very diverse capabilities will challenge the deployment and operation of security solutions such as distributed AI/ML and privacy concerns. An important aspect is how to integrate novel security enablers in an abundance of resource constrained devices. Nevertheless, the security enforcement will be more complex since network entities will be much more mobile, changing their edge networks frequently and getting services in different administrative domains.

Fig. 2: 6G applications, requirements and security.

B. 6G Security Vision and KPIs

The vision of 6G networks is formed with many novelties and advancements in terms of architecture, applications, technologies, policies, and standardization. Similar to the generic 6G vision which has the added intelligence on top of the cloudified and softwarized 5G networks, 6G security vision also has a close fusion with AI which leads to security automation (Figure 3). At the same time, the adversaries also become more powerful and intelligent and capable of creating new forms of security threats. For instance, the detecting zero-day attacks is always challenging whereas prevention from their propagation is the most achievable mechanism. Therefore, the necessity will become more important than ever to incorporate intelligent and flexible security mechanisms for predicting, detecting, mitigating, and preventing security attacks and limiting the propagation of such vulnerabilities in the 6G networks. It is also equally significant to ensure privacy and trust in the respective domains and among the stakeholders. Especially, security and privacy are two closely-coupled topics where security relates the safeguarding of the actual data and privacy ensures the covering up of the identities related to those data. While security on its own is exclusive from privacy, the vice versa is not valid: Essentially, to assure privacy, there should be always security mechanisms that protect data. In the coming sections, we discuss how security and privacy complement each other for different aspects of 6G.

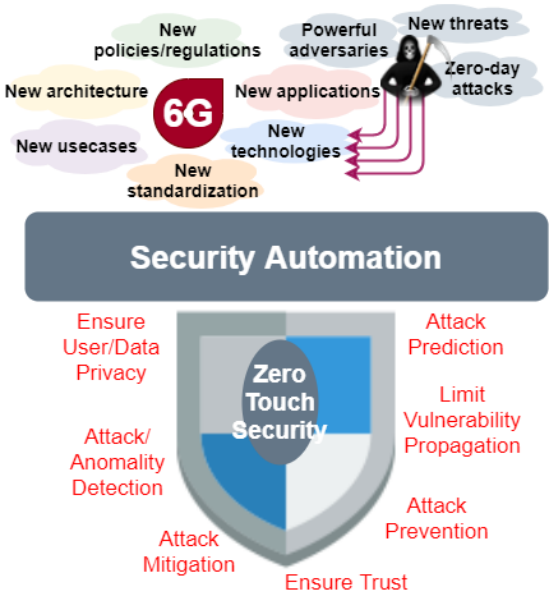

Fig. 3: 6G Security Vision

To set the scope of 6G, we also think that Key Performance Indicators (KPIs) and Key Value indicators (KVI) will help

TABLE II: Security KPIs and 6G vision.

KPI	Description	6G impact
Protection level	The guaranteed level of protection against certain threats and attacks	More stringent due to the pervasive utility of 6G and burgeoning risk level
Time to Respond (mean, max, ...)	Time for security functions to counteract in case of malicious activity	Much smaller due to compressed timescale of 6G networks, e.g., an attack can cause havoc at an order or faster
Coverage	The coverage of security functions over the 6G service elements and functions	More challenging due to diverse 6G technologies and ultra-distributed functions
Autonomicity level	A measure of how autonomic security controls can act	Expected to be easier to implement with pervasive AI, but also may be counter-beneficial due to AI security issues
AI robustness	The robustness of AI algorithms in the network hardened for security	More difficult to maintain consistently system-wide but more critical due to AI's role in 6G
Security AI model convergence time	Time for learning models working for security to converge	Although more advanced AI/ML models are emerging and hardware capabilities are improving, the data availability and complexity are challenging factors for this KPI.
Security Function Chain round-trip-time	Time for chained security functions to process for ingest, analyse, decide and act (related to "Time to respond" KPI)	Security architecture in 6G supposed to be more distributed, leading to challenges. But at the same time, device-centric and edge-centric solutions will help.
Cost to deploy security functions (mean, max, ...)	Various cost metrics for measuring the cost of deployment	Substantially increases due to complexity, thus harder to meet target KPI values

to take the dimensions of impact that go beyond the scope of deterministic performance measures into full account [25]. It is expected that 6G systems will incorporate novel aspects, such as integrated sensing, artificial intelligence, local compute-and-storage, and embedded devices [26]. These aspects will both lead to enhancements to existing KPIs, as well as require a whole new set of KPIs and KVIs which have not traditionally been associated with mobile networks, such as sensing accuracy, computational round-trip-time, and AI model convergence time. The KVIs will quantify the value of the new 6G related technologies from the perspective of sustainability, security, inclusiveness, and trustworthiness stemming from the UN sustainable development goals [27], [28].

Therefore, we believe that the new aspects will have a significant impact on how security KPIs are designed and measured (as shown in Table II). Various aspects should be considered for characterizing security, such as PLS, network information security, and AI/ML related security [8].

C. Security Threat Landscape for 6G Architecture

Undoubtedly, the massive emergence of connections in the future 6g networks will increase the security and privacy vulnerabilities. Considering the foreseen technological, architectural and application specific aspects and their advancements in the future 6G networks, the threat landscape of 6G security is summarized in Figure 4. Since the attacks can be generalized based on the architecture rather than the technologies or the applications, we are taking this step forward to give the reader an insight about the security threat landscape on top of the envisioned 6G architecture.

Among various visionary 6G architectures proposed by the industrial and academic research community, we have identified the vision from Nokia Bell Labs as a realistic yet ambitious proposal to facilitate our security landscape analysis for 6G architecture [5]. As stated by Ziegler et al. in [5], after investigating the potential 6G architectural innovation, they decompose the data and information architecture into four segments, namely, *platform*, *functions*, *orchestration* and *specialization*. In the infrastructure "platform" of 6G architecture, heterogeneous clouds need to create agnostic, open and scalable run-time environment to accelerate the hardware and improve data flow centrality. The "functional" architecture component includes the topics such as RAN core convergence and intelligent radio. The "specialized" part represents the architectural enablers of flexible off-load, sub-networks and extreme slicing. The "orchestration" component includes the intelligent network management and the cognitive closed loop and automation of 6G networks. In the rest of the section, we discuss the security considerations of these four 6G architectural components and how they are related at the consumer end.

However, in addition to the 6G architectural evolution, the advent and advancements of technologies may also pave the way to generate more powerful attackers who can create sophisticated attacks. For instance, while detecting AI based malicious activities, distributed learning based attack prediction methods give promising potential solutions within the constantly changing environments [8].

1) Intelligence Radio and RAN-Core Convergence: The recent advances in the state-of-the-art circuits, antennas, meta-material-based structures, and the dramatic evolution of AI techniques, including ML, data mining, and data analysis, have shed light on a novel path for the challenges expected in radio networks towards 6G. In this sense, providing intelligence beyond the already known intelligent spectrum access for cognitive radio networks is of interest for addressing novel radio network challenges. Thus, the envisioned intelligent radio (IR) will involve cutting-edge AI/ML techniques in order to address accurate channel modeling and estimation, modulation, beamforming, resource allocation, optimal spectrum access, automated network deployment and management. Hence, the introduction of IR towards 6G will lead to a reduced implementation time and a significant reduction in the cost of new algorithms and hardware [29]. With all this promising

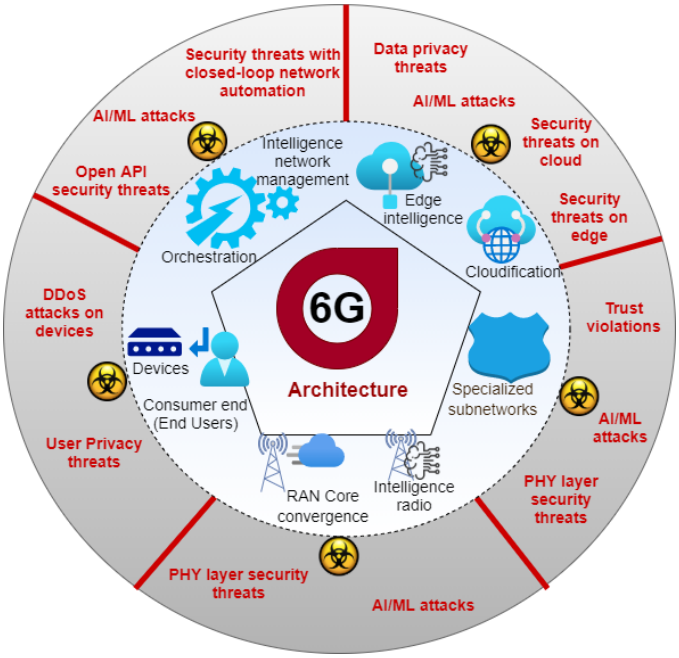

Fig. 4: 6G Security Threat Landscape

benefits of IR, security and privacy are becoming more and more critical in wireless networks, specially for the increasing demands for mission-critical services. For example, AI training can be manipulated in a spectrum access system by inserting fake signals, so that a malicious party can take advantage of a large portion of spectrum by denying the spectrum to other users. Also, attacks through the wireless channel, such as denial-of-service, spoofing, and malicious data injection, could affect the AI. Therefore, efficient detection of malicious training is critical for the proper performance of IR [30].

Besides, new network architecture paradigms are expected for 6G by harmonizing RAN and core functions. Given that different core functions are being distributed and virtualized to be implemented closer to RAN, which benefits low-latency services, while higher-layer RAN functions are being centralized, RAN and core functions can be combined (RAN-Core convergence) in order to simplify the network and facilitate the implementation of some services [31]. Thus, security and privacy challenges and opportunities from this convergence should be addressed towards 6G.

2) Edge Intelligence and Cloudification of 6G Era: The union between AI and edge computing is instinctive since there is a close interaction [32]. In certain 6G wireless applications, it is imperative to shift the computation towards the edge of the network. Whether AI/ML algorithms are used to acquire, storage or process data at the network edge, it is referred to as edge intelligence (EI) [33]. In EI, an edge server aggregates data generated by multiple devices that are associated with it. Data is shared among multiple edge servers for training models, and later used for analysis and prediction, thus devices can benefit from faster feedback, reduced latency and lower costs while enhancing their operation. However, as data is collected from multiple sources, and the outcome of AI/ML algorithms is highly data-dependant, EI is highly prone to several security attacks. Under such circumstance, trust is also required in EI services which are critical to ensure user authentication and access control, model and data integrity, and mutual platform verification [23]. In [34], it is demonstrated how Blockchain is used to secure distributed edge services to prevent resource transactions vulnerable to malicious nodes. Blockchain ensures the consistency of decomposed tasks and the chunks of learning data required in AI implementation.

Attackers can exploit the distributed nature and the respective dependencies on edge computing to launch different attacks like data poisoning, data evasion, or a privacy attack, thus affecting the outputs of the AI/ML applications and undermining the benefits of EI [35]. Moreover, EI may require novel secure routing schemes and trust network topologies for EI service deliveries. Security in EI is closely coupled with privacy since the edge devices may collect privacy sensitive data which contain user's location data, health or activities records, or manufacturing information, among many others. Federated learning is one approach for privacy-friendly distributed data training in edge AI models which enables local ML models. In addition to that, secure multiparty computation and homomorphic encryption for designing privacy-preserving AI model parameter-sharing schemes in EI services are also considered by researchers.

The key architectural change in 5G which has a cloud native and microservice architecture is expected to evolve with heterogeneous aspects in the cloud transformation towards 6G [5]. The heterogeneous clouds related to numerous service delivery platforms including public, private, on-premises and edge cloud may require proper co-ordination of communication resources and distributed computing through orchestration and network control. The security considerations may also differ based on the nature of each cloud environment and the stakeholders. Mainly the most common security issues include the violation of access control policies, data privacy breaches, information security issues, insecure interfaces and APIs, denial of service (DoS) attacks, and loss of data [36].

3) Specialized 6G Networks: As introduced in [5], the trend of having vertical industries in 5G for industrial automation will continue to 6G as sub networks. These specialized 6G networks are expected to operate as stand-alone miniaturized networks for multiple application verticals (e.g., in-body, in-car, in-robot, sub-network of drones). When the wireless interfaces enable sub-network owners or infrastructure to use novel applications, those external communication interfaces may impose security vulnerabilities. To avoid the unauthorized persons remotely take control of the sub-network functions, it will be important to use strong as well as lightweight authentication and encryption algorithms together with methods for monitoring network security by means of intrusion detection systems. Hierarchical and dynamic authorization mechanism will be more suitable to handle trust boundaries between the large networks and the miniaturized sub-networks. Use of trusted execution environments (TEE) may also guarantee the confidentiality and integrity of such closed sub-network environments.

4) Intelligence Network Management and Orchestration: The extreme range of 6G requirements such as massive de-

mand for increased capacity, extremely low latency, extremely high reliability and support for massive machine-to-machine communication will demand a radical change in network service orchestration and management in 6G. With the support of AI, new 6G architecture is expected to offer intelligent end-to-end automation of network and service management. The upcoming ETSI ZSM (Zero-touch network and Service Management) [45] architecture is paving the path towards such intelligence network management deployment in beyond 5G network. Below we discuss the key security challenges in such intelligence network management deployments under three aspects and summarize in Table III.

Open API's security threats: 6G network is expected to support open APIs by continuing the trend developed in 5G networks [37], [38]. There are mainly three variants of open API attacks we identify in the current literature. 1. Parameter attacks lead to unauthorized exploitation of the data transferred through the API. The improper validation of API parameters may also lead to inject attacks on cross-domain data services. 2. Identity attacks allow the attackers to exploit flaws in authentication and authorization process. For instance, extraction of API keys and using them as credentials can result in identity-based attacks. Moreover, unencrypted transmission of API messages may lead to 3. man-in-the-middle attack. An attacker can intercept the unencrypted API messages and capture confidential information. In addition, these open API's can be vulnerable to DoS/DDoS attacks as well. Here an attacker or a group of attackers can manipulate an API out of order by submerging it with a massive amount of requests.

Closed loop network automation: 6G networks may allow closed-loop network automation for the zero touch management capabilities of the network such as monitoring the network to identify the fault and congestion occurrence. Then, it analyzes the data and acts accordingly to eliminate the identified issues. Thus, it creates a feedback loop of communication between monitoring, identifying, adjusting and optimizing the performance of the network to enable self-optimization. Closed loop network automation in 6G will create security threats such as DoS, Man-In-The-Middle and Deception attacks [37].

Intent-Based Interfaces: Intent-based networking (IBN)

TABLE III: Security Challenges in Intelligence Network Management and Orchestration of 6G Networks

Aspect	Issue	Description	Solutions
Open API's security threats [37]–[39]	Parameter attacks	- Improperly validated parameters may lead to injection attacks on cross-domain data services. - Data injection, data manipulation and logic corruption. - Manipulating network topology data to insert fake links, malicious nodes. - Continuous injection of false parameters may leads DoS attack to make the data services unresponsive.	- Input validation and user authentication. - Access Control and rate limiting.
	Identity attacks	- Exploit flaws in authentication and authorization. - Extraction of API keys and using them as credentials. - Attack insecure E2E domain orchestration service to change configurations to fail SLAs, create new instances demanding more resources to exhaust the network.	- Authentication (Signed JWT tokens, OpenID connect) - Authorization (Role based Access Control, Attribute based access control, Access control lists)
	Man-in-the-middle attack	- Obtain information from unencrypted transmission of API messages between the API consumer and provider. - Interception of API messages and revealing confidential information	- Use secure encrypted communication - Use of VPNs (e.g. IPsec, SSL/TLS and HIP)
	DoS/DDoS attacks	- Make an API out of order by submerging it with a massive amount of requests	- Throttling/rate limiting the usage of APIs - Deployment of API gateways and microgateways - AI based API security for proactive monitoring
Closed loop Automation [37]–[41]	DoS attacks	- Fake heavy load on VNFs to increase the capacity of VM, which may. Lead to DoS	- Throttling/rate limiting on resources for VMs - AI based resources level prediction
	Man-in-the-Middle attacks	- Triggering a fake fault event and intercept the domain control messages to reroute traffic via a malicious switch	- Use secure encrypted communication - Use of VPNs (e.g. IPsec, SSL/TLS and HIP)
	Deception Attacks	- Intends to tamper transmitted data	- Use Integrity validation mechanisms (e.g Blockchain)
Intent-based Interfaces [37], [42]–[44]	Information Exposure	- Intercepting information of intents by an unauthorized entities to compromise system security objectives (e.g., privacy, confidentiality). This may lead to the launch of other attacks.	- Authenticating between intent producer and consumer (Signed JWT tokens, OpenID connect) - Controlled access via authorization controls (Role based Access Control, OAuth 2.0) - Secure communication via transport protocols (TLS 1.2)
	Undesirable configuration	- Changing the mapping from intent to action. Setting the security level from "High" to "Low"	- Input validation via user authentication.
	Abnormal behaviors	- Malformed intent could change the behavior, causing network outage	- AI based proactive monitoring for abnormality detection
	Malinformed intent	- Changing the intent reduce the service quality.	- Intent format validation

is a novel concept which is originally proposed to introduce AI into the 6G mobile networks. The main idea of IBNs is to directly transform users' business intent into network configuration, operation, and maintenance strategies using AI technologies. By using IBN concepts, 6G can effectively mitigate the typical limitations in the traditional networks in terms of efficiency, flexibility, and security. The key security security vulnerabilities with IBN may include information exposure, undesirable configuration and abnormal behaviors.

5) Consumer End (Terminals and Users): From the beginning of the advanced portable communication in early generations of wireless systems, they are dependent on a physical placing of symmetric keys in a Subscriber Identity Module, which is also known as SIM card. Although the encryption computations are moved from undisclosed to universal guidelines, the alternative cryptographic instruments are introduced for the shared verification process [18]. In accordance with the general standards, 5G security model is still dependent on the SIM cards [46]. Although the SIM cards are getting smaller into nanoscale, they still need to be inserted into device/gadgets. This may limit the appropriateness of foreseen IoE paradigm in 6G. In a way, this challenge can be tackled with using eSIMs, however, introducing some issues with physical measures. Another solution will be iSIMs which will a part of System-on-Chip in future gadgets. This will also face challenging due to the possible resistance coming from the telecom operators due to conceivable loss of control.

Typically, SIM cards rely on proven symmetric key encryption, which scaled well up to millions to billions of users. However, it has some serious issues with user privacy, IoT, network authentication and fake base stations. Therefore, 6G need to consider a significant shift from symmetric crypto to asymmetric public/private keys and even to the post-quantum keying mechanisms. Already 5G plans to support authentication through a public-key infrastructure (PKI) and a set of microservices communicating over HTTPS. The authentication, confidentiality and integrity for such communication is provided by Transport Layer Security (TLS) using elliptic curve cryptography (ECC). Experiences that come from the use of these technologies in 5G, will shape the user and device authentication approaches in 6G.

III. Security Challenges with 6G Applications

6G is emerging as the network facilitator to a wide range of new applications which will drastically reshape the human society of the 2030s and beyond. However, these applications and services come with very challenging performance requirements as well as extremely stringent security levels due to their critical nature and the need of high trust level. The interplay between the general performance expectations and security requirements becomes even more complicated with the emergence of very capable and ubiquitous attackers and nefarious activities. The envisaged capabilities of 6G could enable a myriad of possible novel applications and use cases. Among them, we extensively select the widely discussed ones and also identify as most influential 6G applications (i.e., summarized in Figure 5 and Table IV) to elaborate on the security considerations. This set of applications are regarded

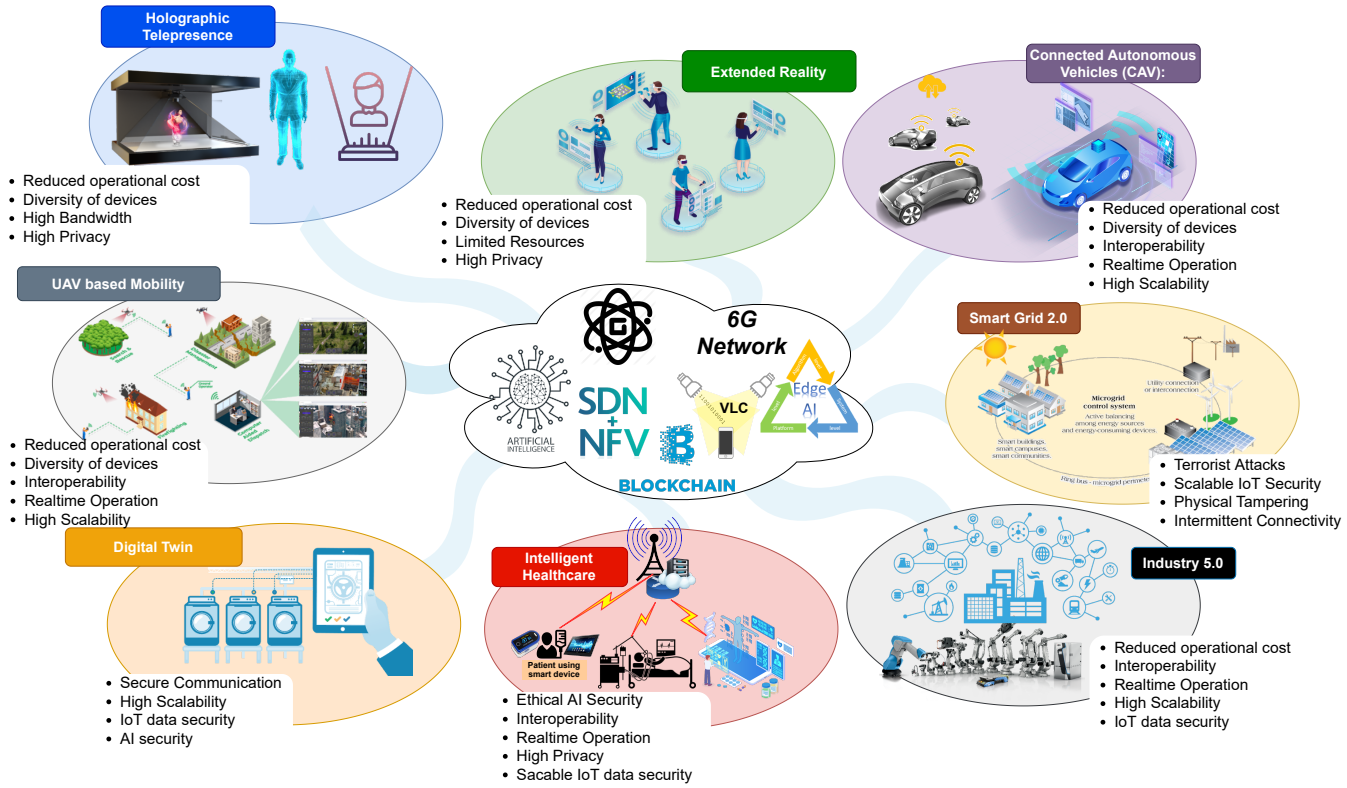

Fig. 5: Key Security Requirements of Prominent 6G Applications

as early deployment use cases and applications of 6G within the current research literature [14], [16], [47], [48].

A. UAV based Mobility

Since 5G, Unmanned Arial Vehicles (UAVs) are getting popular to use in various application domain. With the support of 6G and AI based services, UAV technologies will be used in new use cases such as passenger taxi, automated logistics, and military operations [49], [50]. Due to the limited available resources (i.e. processing and power) and latency critical applications in UAVs they should use lightweight security mechanisms which should satisfy the low latency requirements. Moreover, factors such as high scalability, diversity of devices and high mobility have to be considered while developing the security mechanisms for UAVs. Since 6G will support AI and Edge-AI based UAV functions such as collision avoidance, path planing, route optimization, and swarm control, it is important to deploy mechanism to mitigate AI related attacks as well. Specially, protected integrity of control data is a vital requirement for proper operation. Due to the unmanned nature of UAVs, they are highly vulnerable for physical attacks. An adversary can physically capture the UAVs by jamming control signal or use physical equipment, then steal the important data contained within the UAVs. Moreover, UAVs will have advanced computational and communication capabilities compared to other smart devices. Thus, a swarm of drones can be used to perform organized attacks. Such attacks can be range from cyber-attacks to physical terrorist attacks [51], [52].

B. Holographic Telepresence

Holographic telepresence is a 6G application which can project realistic, full-motion, real-time three-dimensional (3D) images of distant people and objects with a high level of realism rivaling of the physical presence [53] (e.g.,3D video conferencing and news broadcasting [54]). An extremely large bandwidth is required to enable holographic communication. When the number of holographic communication devices are increasing, the bandwidth requirements are also increasing proportionally. Thus, the security mechanisms used for holographic communication should not bring an extra burden on already overwhelmed bandwidths. Moreover, factors such as reduced operational cost and diversity of devices have to be considered while developing the security mechanisms for holographic communication. However, most critical challenge related to holographic telepresence is the protection of the privacy [55]. Specially, providing the required level of privacy when a holographic image is projected to a remote location is also important aspect to consider. Since the remote presenter can not control the environmental settings of the projected location, additional privacy protection mechanisms should implemented, so that users can ensure the privacy.

C. Extended Reality

Extended reality (XR) is a term used to refer all real and virtual combined environments which cover Augmented Reality (AR), Virtual Reality (VR), Mixed Reality (MR), and everything in between [56], [57]. 6G will support the advancements of XR by providing opportunity to use in various use cases including virtual tourism, online gaming, entertainment, online teaching, healthcare and robot control. Managing personal data is an important security aspect of XR which will include not only people's credit card numbers or purchase histories, but also more personal information such as feelings, behaviors, judgments, and physical appearance. Thus, offering the required level of data responsibility is a critical requirement of 6G networks in terms of collection, storage, protection, and also sharing of personal data. Moreover, if fake or forged data are used in XR applications, the quality of user experience (QoE) in XR will fail. The factors such as high

TABLE IV: 6G Applications: Security requirement and Possible Challenges.

	Security Requirements						Expected Security and Implantation Challenges									
Potential 6G Applications	Ultra Lightweight Security	Zero-touch Security	High Privacy	Proactive Security	Security via Edge	Domain specific security	Limited resources	Diversity of Devices	High Mobility	Physical Tempering	Terrorist Attacks	Intermittent Connectivity	Localized environment	Lack of Security Standards	E2E Security orchestration	Energy Efficiency
UAV based mobility	M	H	L	M	H	L	H	M	H	M	H	L	L	L	H	H
Holographic Telepresence	M	L	H	L	M	L	H	M	L	M	L	L	M	M	H	H
Extended Reality	H	M	H	L	H	L	H	M	M	H	L	L	L	H	H	H
Connected Autonomous Vehicles	L	H	M	H	H	H	L	M	H	M	H	L	L	L	H	M
Smart Grid 2.0	H	M	M	H	L	H	H	L	L	H	H	H	L	L	L	M
Industry 5.0	M	H	L	H	H	H	H	H	M	L	M	L	H	M	H	H
Hyper-Intelligent Healthcare	H	M	H	M	H	H	H	H	M	M	L	M	H	M	H	H
Digital Twin	M	H	L	L	M	M	L	M	L	L	H	M	L	L	H	M

L Low Level Requirement/Impact M Medium Level Requirement/Impact H High Level Requirement/Impact

scalability, low overhead, and diversity of devices should be considered while developing the security mechanisms for XR. Depending on the application, the security level or enforced security methods in XR application can fluctuate significantly. For instance, military applications may need the highest level of security (i.e. strong multi-factor authentication, data encryption, user access control) while entertainment applications may require a lower level of security.

Another critical security issue related specifically to XR is the fake experiences. If fake or forged data been used in XR applications, total XR experience will fail. Such incidents can even cause fatal results. For instance, use of fake experience in critical XR environments such as surgery or military operation may lead to life-or-death consequences.

D. Connected Autonomous Vehicles (CAV)

Nearly 50 leading automotive and technological companies are heavily investing in autonomous vehicle technology. The world moves forward to experience truly autonomous, reliable, safe, and commercially viable driver-less cars in near future [58]. With the advent of Connected Autonomous Vehicles (CAV) technologies, a new service ecosystem will emerge such as driver-less taxi and driver-less public transport [48], [59]. The security issues in complex CAV ecosystem can be categorized into three categories as vehicle level, CAV supply chain and data collecting. The vehicle level attacks can happen by hijacking vehicle sensors, V2X communications and taking over physical controls. Similar to UAVs, autonomous nature without human involvement will lead to possibility of physical hijacking. However, autonomous vehicles have more advanced capabilities than UAVs. Therefore, emergency security measures can be integrated within a car. For instance, automatic stop of car during a terrorist attack is possible. 6G network can analyze the situation and deliver the emergency signals to vehicles.

Moreover, new types of cyber attacks due to V2X communications in CAV ecosystem are possible. Advance CAVs have communication link with the car manufacturer, so they can constantly monitor and make instant transmission of software-related patches to mitigate any foreseen troubles over the air. However, vulnerabilities in the communication channels or forging the data downloaded from manufacturer cloud services can compromise the safety and security of the vehicles and its passengers.

The CAV ecosystem has a complex supply chain with different third-party service providers such as CSPs (Communication Service Providers), Road Side Equipment (RSE), cloud service providers and regulators. Enabling common standard of security requirements and enabling the inter-operability is challenging. Privacy issue may arise when CAVs collect data about the travel routes, control sensor data and also about their owners and passengers. Such data becomes a honeypot for malicious attackers. According to the National Institute of Standards and Technology (NIST), CAV security framework should target on providing device security, data security, and individuals' privacy.

Specially, when public transport modes such as trains, flights and buses are used, protection of individual privacy while delivering 6G services such as XR, holographic telepresence will be challenging. Therefore, 6G security framework for CAVs has to consider security convergence by combining of physical security and cybersecurity along with the concept of Privacy by Design.

E. Smart Grid 2.0

With the development of smart devices and advanced data analytical techniques, the grid networks are getting smarter and evolving from Smart grid 1.0 to Smart grid 2.0. Smart grid 2.0 may offer features such as automated meter data analysis, intelligent dynamic pricing, intelligent line loss analysis, distribution grid management automation and reliable electric power delivery with self-healing capabilities [60]. In smart grid 2.0, it is important to offer network information and cybersecurity to ensure confidentiality, integrity and availability of the energy network. The most common security vulnerabilities may include different type of attacks such as physical attacks, software related threats, threats targeting control elements, network based attacks and AI/ML related attacks [61]. The critical components and services such as data access points, control elements (SCADA) [62] and the EMS of the cyber-physical system [63], metering, billing and information exchange are heavily targeted in these attacks.

Moreover, the improvement of trust management of trading mechanisms is a critical requirement of smart grid 2.0. One of the key features envisaged by Smart grid 2.0 is the trading of energy between unknown parties in a P2P manner. Such trading could occur in variations of prosumer-to-prosumer and prosumer-to-consumer due to popularity of solar PV based small scale energy production and electrical cars [64]. Due to the scale of number of such occurrences, the trust should be established with minimal intervention of an intermediary. Moreover, the radical shift in smart grid management from centralized to distributed mode has also created the necessity of instating trust between the buyer and the seller, which has been the role of the third party intermediary (i.e., Distribution Systems Operator) in a vertical grid arrangement [65].

F. Industry 5.0

Industry 5.0 is identified as the next innovation in industrial revolution which means people working alongside robots and smart machines to add a personal human touch to the Industry 4.0 pillars of automation and efficiency [66]. 6G plays a vital role in enabling the advancements of automated industrial environment. Similar to other 6G enabled applications, Industry 5.0 will also face critical security threats and also they need to provide basis security needs such as integrity, availability, authentication, and audit aspects. Factors such as reduced operational cost, diversity of devices, high scalability have to be considered while developing the security mechanisms for Industry 5.0. 6G will mainly responsible for The data security and integrity protection [67] in Industry 5.0 as controlling commands and monitoring data will be transferred over the 6G networks. Therefore, 6G era should also provide highly scalable and automated access control mechanisms and audit systems to restrict the access to the sensitive resources such as intellectual properties related to Industry 5.0.

G. Intelligent Healthcare

Digital healthcare or e-health care services are evolving for new dimensions. Within few years, AI-driven intelligent healthcare will be developed based on various new methodologies including Quality of Life (QoL), Intelligent Wearable Devices (IWD), Intelligent Internet of Medical Things (IIoMT), Hospital-to-Home (H2H) services, and novel business models [21], [68]. The growth elderly population may create the increase the importance of e-health than every before. Body Area Networks (BANs) with the integrated intelligent health systems are advancing towards personalized health monitoring and management. Such personalized BANs can collect health information from multiple sensors, dynamically exchange the collected information with the environment and interact with networking services including social networks [69].

6G will be the main communication platform to interconnect the intelligent healthcare services in the future. Thus, enabling the secure communication, device authentication and access control for billions of IoMT and wearable devices will be critical security challenges to solve in 6G era.

Privacy protection and ensuring of the ethical aspects of user data or electronic health records will be a critical issue in future healthcare system. As explained above, the utilization of AI is mandatory to manage billions of IoMT devices and process the health related information. However, current AI model are mainly focused on performance optimization rather than the ethical aspects. Specially, AI models should follow strict ethical rules on data collection and use of user data for the model training [70]. Moreover, AI models should comply with privacy rules and regulations enforced by the regulation bodies. As the main communication infrastructure for future healthcare systems, 6G networks should protect both privacy and integrity aspects of the patient information and records.

H. Digital Twin

The digital twin is a novel industrial control and automation systems concept which is identified as a key 6G application. A digital twin is defined as a digital or virtual copy of a physical object, an asset or a product [71], [72]. Digital twin interconnects virtual and physical worlds by collecting real-time data by using IoT devices which are connected to the physical system. These collected data will be stored in locally decentralized servers or centralized cloud servers. Then, the collected data will be analyzed and evaluated in the virtual copy of the assets. After obtaining the results form the simulations, the parameters are applied to the real systems. The integration of data in real and virtual representations will help in optimizing the performance of the physical assets. Digital twin can be used in other use cases such as Industry 5.0, Automation, healthcare, utility management and contractions.

The biggest security challenge in the digital twin system is that an attacker can intercept, modify, and replay all communication messages between the physical and digital domains. With the popularity of digital twin systems in future, 6G should support highly scalable secure communication channels. Another issue in digital twin systems is that the attacker can modify or alter the IoT data and make privacy attacks. When 6G is used to enable digital twin system, IoT data integrity and privacy protection mechanisms should be utilized. For instance, blockchain can be used as a candidate technology to enable such features in 6G networks.

IV. Security Impact on New 6G Technologies: Requirements, Threat Landscapes and Possible Solutions

Considering the security requirements and application specific aspects of the future 6G networks which are presented in the previous sections, here we discuss the threat landscape and possible security solutions related to few 6G technologies that have already gained the most attention. Although many other emerging technologies show their potential of relevance to 6G, their security and privacy considerations are not yet discovered in the state-of-the-art. In contrast, certain topics such as network softwarization and cloudification are already discussed with respect to 5G security. Based on the current literature, we identified that technologies such as DLT, distributed and scalable AI/ML and quantum computing, and some PLS related topics (THz, VLC, RIS, MC) are quite relevant and have substantial amount of work and new research directions related to security and privacy in 6G. Therefore, we extensively discuss those listed topics in the remainder of the section. In brief, we discuss the possible security solutions for the key security issues in 6G networks, how the available and evolving technologies can mitigate such security threats, state-of-the-art of security mitigation techniques for the given technologies, and beyond the state-of-the-art vision.

A. Distributed Ledger Technology (DLT)

Among DLTs, today Blockchain technology has gained the highest attention in the telecommunication industry. The advantages of blockchain such as disintermediation, immutability, non-repudiation, proof of provenance, integrity and pseudonymity are particularly important to enable different services in trusted and secure manner in the 6G networks [73].

In addition to the advantages of AI in 6G, the use of AI/ML, and other data analytic technologies, can be a source for new attack vectors in 6G. It has been proven that ML techniques are vulnerable to several attacks [74] targeting both training phase (i.e., poisoning attacks) and the testing phase (i.e., evasion attacks). Since data is the fuel for AI algorithms, it is crucial to ensure their integrity and their provenance from trusted sources [75]. DLT can achieve the trust dimensions, such as protect the integrity of AI data via immutable records and distributed trust between different stakeholder, which will enable the confidence in AI-driven systems in a multi-tenant/multi-domain environment.

Furthermore, DLT/blockchain show the potential of using as a facilitating technology to evolve the 5G service models to support 6G. These services may include, however not limited to, secure VNF management, secure slice brokering, automated Security SLA management, scalable IoT PKI management, secure roaming and offloading handling and user privacy protection, to comply with 6G requirements [76].

1) Threat Landscape: Due to the foreseen alliance of DLT and 6G, the security vulnerabilities of Blockchain and smart contracts may also implicitly impact the 6G networks [77]. Most of these attacks are occurred due to the reasons such as software programming errors, restrictions in the programming languages, and security loopholes in network connectivity [78]. Moreover, these security issues can be occurred in both public and private blockchain platforms. They lead to complications such as loss of accuracy, financial losses in terms of cryptocurrency and reduced availability of the system. Some of the critical security attacks in blockchain and smart contract systems are listed below (Figure 6).

Fig. 6: Key Security Vulnerabilities of Blockchanized 6G Services.

Majority attack / 51% attack: If malicious users capture the 51% or more nodes in the blockchain, they could take over the control of the blockchain. In a majority attack, the attackers could alter the transaction history and prevent the confirmation of new legitimate transactions from confirming [79]. Blockchain systems which use majority voting consensus [80] are usually vulnerable for majority attacks.

Double spending attacks: The spending of the cryptographic token is a key feature of most the blockchain platforms [81]. However, there is a risk that a user can spend a single token multiple times [82] due to lack of physical notes. Such attacks are called the double spending attacks [83] and blockchain systems should have a mechanism to prevent such double spending attacks.

Re-entrency Attack: The re-entrancy vulnerability can be occurred when a smart contract invokes another smart contract iterative. Here, the secondary smart contract which has invoked can be malicious. For instance such an attacks was performed to hack Decentralized Autonomous Organization (DAO) in 2016 [84]. An anonymous hacker stole USD50M worth Ethers.

Sybil attacks: Here, an attacker or a group of attackers are trying to hijack the blockchain peer network by conceiving fake identities [85]. The blockchain systems which have minimal and automated member addition systems are typically prone to Sybil attacks [86].

Privacy Leakages: Blockchains and smart contracts are vulnerable to several privacy threats such as leakage of transaction data privacy [87], leakage of smart contract logic privacy [88], leakage of user privacy [89] and privacy leakages while execution of smart contracts [90]. Some of the blockchain nodes may follow the strict privacy roles and support too much transparency which may leads to reveal some sensitive information such as trade secrets and pricing information [87]. Moreover, business logic of the organization required to be incorporated in the blockchain. The sensitive business logic information such as commissions and bonuses may need be included smart contracts and these information can be revealed to the competitors [88].

Other attacks: Apart from the above, blockchains and smart contracts are vulnerable to several other security threats such as destroyable contracts [91], exception disorder [92], call stack vulnerability [93], bad randomness [94], underflow/Overflow errors [95] [96], broken authentication [97], broken access control [98], security misconfiguration [99] and unbounded computational power intensive operations [100].

2) Possible Solutions: Obviously, when the DLT/blockchain solutions are adopted in 6G networks, they should always comply with possible mechanisms to mitigate the above security attacks. However, the deployment of some of the security mechanisms can be momentous in the public blockchains than in the private blockchains. For instance, the debugging or any correction of smart contracts might be a cumbersome process [101] since the smart contracts are adopted by all the nodes in a blockchain network. Since the smart contracts are playing a vital role in DLT/blockchain systems to enable the automation, ensuring the accuracy of the smart contract is necessary. Moreover, the proper validation of correct functionality of the smart contract is required before deploying it in thousands of blockchain nodes. The accurate functionality of smart contacts can be checked by ***identifying semantic flaws*** [102], [103], using ***security check tools*** [104], [105] [106] and performing ***formal verification*** [107]–[110].

Moreover, proper access control and authentication mechanisms should be utilized to identify the malicious bots and AI-agent based blockchain nodes. Such mechanisms can prevent the majority and Sybil attacks. The additional privacy preservation mechanisms such as privacy by design [111], [112]

and TEE [113], [114] can be integrating to prevent privacy leakages in blockchain based 6G services [115], [116].

Moreover, blockchain/DLT support different architecture types such as (i) public, (ii) private, (iii) consortium and (iv) hybrid blockchain [117]. The impact of above security attacks naturally vary for different architectures. For example, the 51% attacks are highly impacting on public blockchains. In such cases, a consortium or private blockchains can be suitable for certain 6G services (e.g., spectrum management, roaming) which has less number of miners [76]. Therefore, selecting the proper blockchain/DLT type according to the 6G application and services can eliminate the impact of certain attacks.

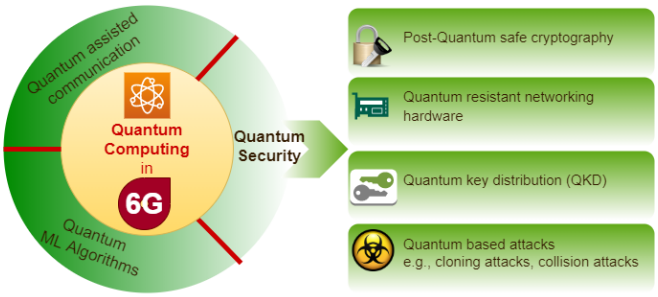

Fig. 7: Role of quantum computing in 6G.

B. Quantum Computing

With in the next couple of years, it is expected that quantum computing will be commercially available and will impose a huge threat on the current cryptographic schemes. As stated in the current state-of-the-art, quantum computing is envisioned to use in 6G communication networks for detection, mitigation and prevention of security vulnerabilities. Quantum computing assisted communication is a novel research area that investigates the possibilities of replacing quantum channels with noiseless classical communication channels to achieve extremely high reliability in 6G. Moreover, with the advancements of quantum computing, it is foreseen by the security researchers that quantum-safe cryptography should be introduced in the post-quantum world. The discrete logarithmic problem, which is the basis of current asymmetric cryptography, may become solvable in polynomial time with the development of quantum algorithms (e.g., Shor) [118].

Since quantum computing tends to use the quantum nature of information, it may intrinsically provide absolute randomness and security to improve the transmission quality [4]. Integrating post-quantum cryptography schemes with physical layer security schemes may ensure secure 6G communication links [119]. Moreover, new eras may open up by introducing ML-based cyber-security and quantum encryption in communication links in 6G networks. Quantum ML algorithms may enhance security and privacy in communication networks with the quantum improvements in unsupervised and supervised learning for classification and clustering tasks. There are promising 6G applications where there are potentials in applying quantum security mechanisms. For instance, many 6G applications such as ocean communication, satellite communication, terrestrial wireless networks, and TeraHertz communications systems have potentials of using quantum communication protocols such as quantum key distribution (QKD) [120]. QKD is applicable in the conventional key distribution schemes by providing quantum mechanics to establish a secret key between two legitimate parties. Figure 7 demonstrates the envisioned roles of quantum computing and quantum security in the 6G era.

1) Threat Landscape: Within the threat landscape in quantum-based attacks, the adversaries are also considered to have quantum powers. Although quantum computers are yet to be evolved in the long run, the threat it may generate on IoT devices needs to be carefully considered already. Since cryptography is the key security factor in IoT networks and IoT devices, they require light-weight cryptographic solutions. It is always challenging to incorporate post-quantum crypto solutions which are resisting quantum-based attacks in IoT devices. Therefore, device independent quantum cryptography is a challenge in the post-quantum era in 6G paradigm.

The oblivious transfer (OT) in classical information sharing allows sender to transfer one of potentially many pieces of information to a receiver while remaining oblivious as to which piece has been transferred. However, this feature is unable to maintain in quantum information since any leakage may create huge damage to whole two-party communication.

As a fundamental law, the quantum computers have no-cloning property which makes impossible to maintain the exact copy of quantum state (i.e., rewinding not achievable). In quantum cloning attacks, an adversary has to take a random quantum state of an information and make an exact copy without altering the original state of the information. Although perfect quantum state copies are prohibited, in [121], it is proven that a quantum state can be copied with maximal accuracy via various optimal cloning schemes. Quantum cloning attacks may even occur in high-dimensional QKD schemes as quantum hacking in a secure quantum channel. Moreover, quantum collision attacks can also occur when two different inputs of a hash function provide the same output in a quantum setting.

2) Possible Solutions: In order to be ready with the threat due to quantum computing in the future 6G era, the scientists have already started investigating quantum resistant hardware and encryption solutions. There are few post-quantum cryptographic primitives identified as lattice-based, code-based, hash-based and multivariate-based cryptography [122]. In the current context, lattice computational problems show better performance in IoT devices. Due to the smaller key-length, they fit better in 32-bit architecture. However, these categories are yet to be evolved and are recommended for the IoT devices with respect to their performance and memory constraints and communication capabilities. As post-quantum cryptography will be no longer protected with the classical random oracle model, it may need to verify security in the quantum-accessible random oracle model where the adversary can query the random oracle with quantum state [123].

C. Distributed and Scalable AI/ML

6G envisions autonomous networks that can perform *Self-X* functions (self-monitoring, self-configuration, self-optimization and self-healing) without any human involvement [124]. The ongoing ZSM architecture specifications entailing intent-based interfaces, closed-loop operation and AI/ML techniques to empower full-automation of network management operations including security are steps towards that goal. Since the pervasive use of AI/ML will be realized in a distributed and large-scale system for various use cases including network management, distributed AI/ML techniques are supposed to enforce rapid control and analytics on the extremely large amount of generated data in these networks. As demonstrated in Figure 8, 6G security is mainly revolving around AI in two aspects such "AI for security" and "Security for AI".

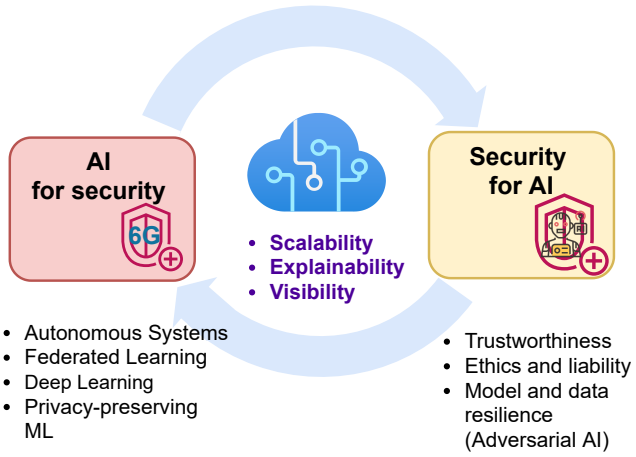

Fig. 8: 6G security and AI.

Distributed AI/ML can be used for security for different phases of cybersecurity protection and defense in 6G. The utility of AI/ML driven cybersecurity lies on the advantages in terms of autonomy, higher accuracy and predictive capabilities for security analytics. Following are some challenges regarding the AI/ML in 6G systems as defined in [125]:

- Trustworthiness Are ML components trustworthy? This is a more important question when critical network functions including security are AI-controlled.

- Visibility For controllability and accountability, visibility is crucial. A research question is how to monitor timely for security-violating AI incidents.

- AI Ethics and Liability Could some AI based optimization starve some users or applications? Do AI driven security solutions protect all users the same? Who is liable if AI controlled security functions fail?

- Scalability and feasibility For federated learning, data transmissions should be secured and preserve privacy. For AI/ML controlled security functions, scalability in terms of required computation, communication and storage resources is challenging. For instance, FeMMB leads to huge data flows. Integrated with AI/ML, these flows may cause significant overhead.

- Model and data resilience Models should be secured and robust in the learning and inference phases (e.g., against poisoning attacks). However, more attacks are being developed with increasing variety and proficiency in recent years [126], e.g. on federated learning [127].

1) Threat Landscape: It is expected that 6G will heavily rely on AI and ML technologies. However, the use of AI and ML will lead to 6G intelligence network management system to become a victim of AI/ML related attacks. Such attacks can target the training phase (poisoning attacks) as well as the test phase (evasion attacks) [128], [129]. During a poisoning attack on the training phase, the attacker can tamper the training data by injecting carefully crafted malicious samples, to influence the outcome of the learning method [130]. Such injection of crafted samples may lead to intelligence services supporting the E2E services to mispredict the resource requirements and misclassifying the services. Evasion attacks during the test phases attempts to circumvent the learned model by introducing disorders to the test data. Moreover, model inversion aims to derive the training data, utilizing the outputs of the targeted ML model while model extraction attacks steal the model parameters to replicate (near-)equivalent models. Infrastructure-targeting physical attacks essentially strive for communication tampering, and intentional outages and impairments in the communication and computational infrastructure for impairments in decision-making/data processing and may even put entire AI systems in offline.

At the AI middleware layer, a significant threat is the compromise of AI frameworks to exploit vulnerabilities in those artefacts or traditional attack vectors towards their software, firmware and hardware elements. For another type of attack, API-based attacks, an adversary queries and attack an API of a ML model to obtain predictions on input feature vectors. This may lead to model inversion (recover training data), model extraction (reveal model architecture compromising model confidentiality) and membership inference (exploit model output to predict on training data and ML model) attacks.

2) Possible Solutions: There are different solutions against these threats for AI/ML. Adversarial training injects perturbed examples similar to attacks into training data to increase robustness [131]. Defensive distillation is another defensive strategy that is based on the concept of knowledge transfer from one neural network to another via soft labels, which are the output of a previously trained network and represent the probability of different classes. They are used for the training instead of using hard labels mapping every data to exactly one class) [132]. These two solutions are both effective ones against evasion attacks and adversarial attacks.

Against poisoning attacks in the training phase, protection of data integrity and authentication of the data origin is instrumental. In that regard, blockchain provides a distributed, transparent and secure data sharing framework perspective [133]. Similarly, moving target defense [134], [135] and input validation [136] are used. The latter is also beneficial against adversarial attacks. To mitigate model inversion attacks, an effective defense is to control information provided by ML APIs to the algorithms to prevent them. This approach is also effective against adversarial attacks. Another countermeasure

against model inversion attacks is to add noise to ML prediction [137]. Noise injection, but to the execution time of the ML model, is also used against model extraction attacks.

D. Physical Layer Security

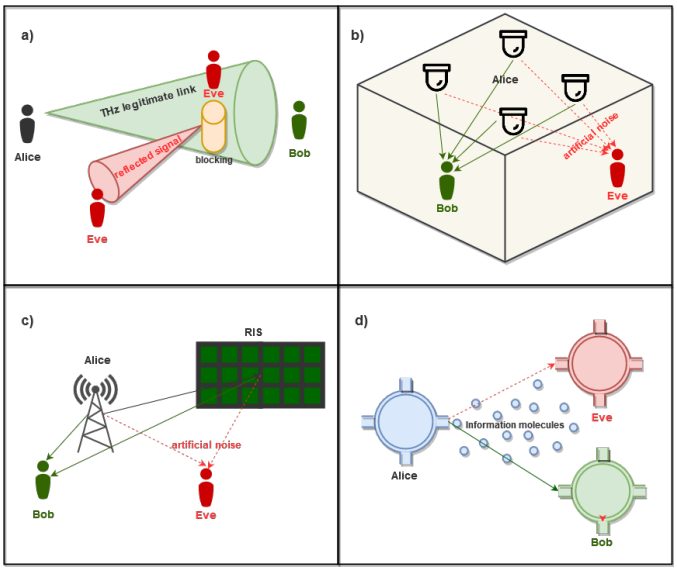

Fig. 9: Illustrative PLS scenarios in 6G era: a) THz communications in the presence of eavesdroppers, b) Secure MIMO VLC systems with artificial noise, c) RIS-aided secure wireless communication, d) Eavesdropping in molecular communications.

Physical layer security (PLS) mechanisms rely on the unique physical properties of the random and noisy wireless channels to enhance confidentiality and perform lightweight authentication and key exchange. The flexibility and adaptability of PLS mechanisms, specially for resource-constrained scenarios, joint with the opportunities provided by disruptive 6G technologies may open a new horizon for PLS in the time frame of 6G. Figure 9 shows illustrative scenarios for PLS regarding key technologies expected for 6G, which are described next.

1) TeraHertz technology: In 6G, it is expected to move further to higher carrier frequencies, in the terahertz range (1 GHz to 10 THz), to improve spectral efficiency and capacity of future wireless networks as well as provide ubiquitous high-speed Internet access. In those frequencies, the transmitted signals are highly directional and the propagation environment is harsh, thus the interception of signals is mostly limited to illegitimate users that are located in the same narrow beam of the legitimate user.

Threat Landscape: Even with the use of extremely narrow beams, an illegitimate receiver can intercept signals in line-of-sight (LoS) transmissions. Thus, THz communications are prone to data transmission exposure, eavesdropping, and access control attacks.

Possible Solutions: In [138], the authors prove that an illegitimate user can intercept signals by placing an object in the path of the transmission, so that the radiation is scattered towards him. In that paper, it is proposed to perform a characterization of the backscatter of the channel in order to detect some, although not all, eavesdroppers. Moreover, in [139], the authors proposed to explore the multipath nature of THz propagation links to enhance the information-theoretic security. Therein, by sharing data transmission over multiple paths, the authors showed that the message eavesdropping probability can be significantly reduced, even when several eavesdroppers are cooperating, at a cost of a slight decrease on link capacity. That solution can be explored for transmitting sensitive data or performing secure key exchange in THz networks. Moreover, in [140], a study is conducted for performing authentication at the physical layer in vivo nano networks at THz frequencies, where a distance-dependent-pathloss based authentication is performed. The authors showed that pathloss can be used as a device fingerprint from a THz time-domain spectroscopy setup. All in all, new PLS solutions, as electromagnetic signature of THz frequencies for performing authentication at the physical layer [9], would benefit THz wireless joint with the incorporation of new countermeasures on the transceiver designs.

2) Visible Light Communication technology: VLC is an optical wireless technology that has gained significant attention due to its advantages compared with radio frequency (RF) systems, such as high data rates, large available spectrum, robustness against interference, and low-cost for deployment. VLC also has great potential to complement RF systems in order to exploit the benefits of both networks [141].

Threat Landscape: VLC systems are intrinsically more secure compared with RF systems due to light cannot penetrate walls. However, due to the broadcast nature of VLC systems (as in RF), when communication takes place on public zones or with large windows in the coverage, VLC systems are prone to eavesdropping attacks, thus confidentiality may be potentially compromised [142]. Moreover, VLC systems present different characteristics than RF systems that should be considered for the design of PLS mechanisms. For instance, VLC channels are quasi-static and real-valued channels, and VLC systems present a peak-power constraint that impedes unbounded inputs, e.g. Gaussian inputs. Therefore, these operating constraints should be revisited for the performance evaluation and the optimization of PLS strategies in VLC systems [143]. Besides, according with the study conducted in [144], VLC systems are more vulnerable at locations that present strong reflections.

Possible Solutions: In [142], the enhancement of the secrecy performance, in terms of the achievable secrecy rate, of a multiple-input multiple-output (MIMO) VLC system is demonstrated by using linear precoding. Therein, the peak-power constraint is considered for the transmitted signal, and only discrete input signaling schemes are used. Also, in [145], a scheme of watermark-based blind PLS was investigated, where red, green and blue LEDs and three color-tuned photodiodes are employed to enhance the secrecy of a VLC system by implementing a jamming receiver joint with the spread spectrum watermarking technique.

3) Reconfigurable Intelligent Surface: With the evolution of metamaterials and micro electro-mechanical systems, RIS

have emerged as a promising option to tackle the challenges of intelligent environments regarding security, energy and spectral efficiency. RIS is a software-controlled metasurface composed by a planar array of a large number of passive and low-cost reflecting elements, which are capable of dynamically adjust their reflective coefficients, thus controlling the amplitude and/or phase shift of reflected signals to enhance the wireless propagation performance.

Threat Landscape: Traditional PLS techniques, such as the deployment of active relays or friendly jammers that use artificial noise (AN) for security provisioning, may incur on increased hardware cost and energy consumption. Moreover, in adverse wireless propagation environments, an adequate secrecy performance cannot be always guaranteed even with the use of AN. Therefore, it would be desirable to adaptively control the propagation properties of wireless channels to ensure secure wireless communications, which is impossible to attain with traditional communication technologies.

Possible Solutions: By controlling the phase shifts of RIS in an intelligent manner, the reflected signals can either be added coherently at the intended receiver to enhance the quality of the received signal, or be added destructively at a non-desired receiver to enhance security [146]. In this sense, RIS-assisted PLS has become a promising technology for secure and low-cost 6G networks. For instance, in [147], it is shown the importance of RIS technology for enhancing security, even if the eavesdropping link is in better conditions than the legitimate link. Moreover, the secret key generation problem for RIS-assisted wireless networks has also been investigated, where each element of the RIS is an individual scatter to enhance the secret key capacity [148].

4) Molecular communication (MC): In MC, bionanomachines communicate using chemical signals or molecules in an aqueous environment [149]. This technology is appealing for enabling important applications and use cases related to helthcare innovations in the context of 6G.

Threat Landscape: This kind of communications will handle highly sensitive information with several security and privacy challenges on the communication, authentication and encryption process.

Possible Solutions: It is extremely important to tackled security issues in MC from the very early stages of its practical development in order to guaranteed the promising benefits of this technology, thus PLS mechanisms would have an impact on providing security for MC. For instance, the notion of biochemical cryptography was introduced in [150], where a biological macro-molecule composition and structure are used as a medium to achieve information integrity. Moreover, in [151], the fundamental benefits and limits of PLS are investigated for diffusion-based channels, where the secrecy capacity is derived to obtain insights on the number of secure symbols that can be transmitted over a diffusion-based channel.

V. Privacy

The faster the world is moving towards a digital reality, the higher the risk people may put their privacy, which is more precisely called digital privacy. The data is collected for many applications to improve their service performance. Such processed data or the information leakage always create huge privacy issues which require well balanced privacy preserving techniques. When more and more end devices tend to share local data to the centralized entities, the storage and processing of this data pile with the added privacy protection mechanisms will be difficult. As 6G systems may have simultaneous connectivity up to about 1000 time greater than in 5G, privacy protection should be considered an important performance requirement and a key feature in wireless communication in the envisioned era of 6G [9]. However, in the current process of data collection and analysis, privacy protection has not received the enough attention and priority level. Therefore, there are many research opportunities for finding the correct balance between increasing data privacy and maintaining them with lower computation load which may reduce the speed and accuracy of the computation. In Figure 10, we describe illustrate a summary of 6G privacy with respect to privacy types, privacy violation, privacy protection, and related technologies.

The issue in 6G with data privacy will be more challenging when the number of smart devices are increasing and tracking every move of a person with lack of transparency about what is exactly collected. Specially, in the big data era of decentralized systems, adding privacy protection mechanisms will further increase the communication and computational costs which already show a rapid growth [152].The current European Union's General Data Protection Regulation (GDPR) for privacy assurance should be also subject to change with the evolving 6G applications and specifications. Mainly, there are three key challenges that encounter while protecting privacy in 6G:

- The extremely large amounts of data exchange require in 6G may impose a greater threat on peoples' privacy with an extensive attention attracted by the governmental and other business entities. This may occur as a large number of small chunks of data accumulations. The easier the data is accessible and collectable in the 6G era, the greater risk they may impose on protecting user privacy and causing regulatory difficulties.
- When the intelligence is moving to the edge of the network, more sophisticated applications will run on mobile devices are increasing the threats of attacks. However, incorporating privacy protecting mechanisms in resource-constrained devices in the edge of the network will be again challenging. This arises the requirement of introducing lightweight privacy preserving mechanisms.
- Keeping the correct balance between maintaining the performance of high-accurate services and the protection of user privacy is also noteworthy. Location information and identities are required to realize many smart applications. Therefore, it is necessary to carefully consider data access rights and ownership, supervision and regulations for protecting privacy.

Considering privacy in the context of statistical and machine learning analysis, Differential Privacy (DP) is another budding privacy-preserving technology which is also likely to appear in future 6G wireless applications [18], [153]. DP may provide

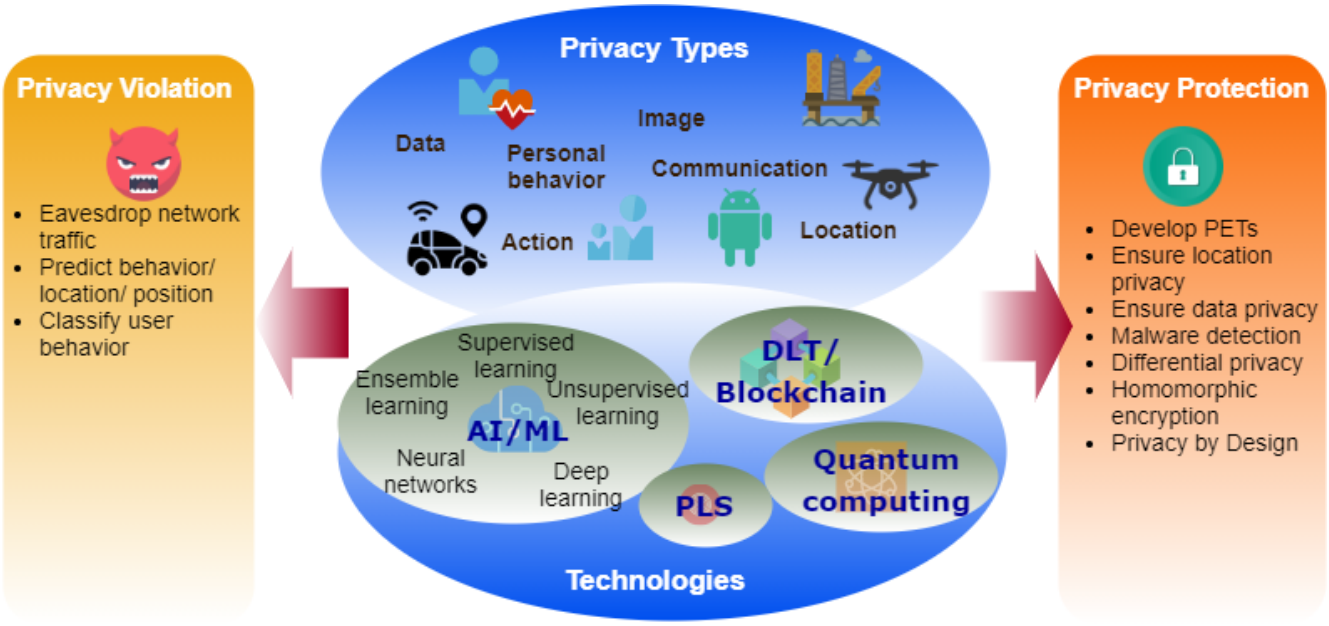

Fig. 10: Summary of 6G privacy.

mathematically provable privacy protection against certain privacy attacks such as differencing, linkage and resonstruction attacks. As stated in [153], DP has interesting properties to enhance privacy protection while analyzing personal information: quantification of privacy loss permits comparisons among different computation techniques; composition allows the design and analysis of complex privacy enhancing algorithms starting from simple building blocks; allow group privacy; immunity to post-processing of the privacy concerned algorithms. Rather than using conventional data encryption methods, novel mechanisms can be incorporated with the development of lightweight privacy preserving techniques such as using homomorphic encryption (HE) [154].

The role of Blockchain in 6G may have pros and cons in terms of privacy aspects. On one hand, data privacy in 6G will likely involve Blockchain for the ultra-massive and ultra-dense networks. For instance, Blockchain technology can be used as a key candidate for privacy preservation in content-centric 6G networks. Having a common communication channel in blockchain may allow network users to be identified by pseudo names instead of direct personal identities or location information. Moreover, blockchain can be improved by introducing new block header structures to protect privacy in high sensitive tasks and actors. On the other hand, since Blockchain is a DLT which is intrinsically transparent, it may disclose private information to all participants by creating privacy violations. When the 6G is expected to host a zero trust architecture that assure embedded trust in the devices and the network. While Blockchain is gaining higher reputation to ensure trust among highly decentralized and distributed applications, it also brings the biggest issue on data privacy and advanced connectivity. As pointed out in [155], such privacy risks can be addressed by solutions including, risk signatures, zero-knowledge augments and coin mixing.

The fast growing AI technology in the 6G vision has a close associative with ML technology where privacy is showing a greater impact in two ways [19]. In one way, the correct application of AI/ML can protect privacy in 6G. In another way, privacy violations may occur as AI/ML attacks. Different ML types (e.g., neural network, deep learning, supervised learning) can be applied for privacy protection in terms of data, image, location, and communication (e.g. Android, intelligent vehicles, IoT). As summarized in [19], privacy attacks can occur ML models while training (e.g., poisoning attack) and testing phases (e.g., reverse, membership interference, adversarial attacks). When AI is used to emulate human brain capability with collaborative/cooperative robots (cobots), they use learning tools to train those digital entities. However, the question is, whether the cobots will be ethical, transparent and accountable for preserving privacy concerns while using data sets during this constant learning and real-time decision making process.

While developing more robust and efficient privacy preservation solutions, the properties of quantum mechanics can be also exploited for high security and high efficiency levels. Such approaches will be very much useful in a post-quantum era of 6G networks in the long run. For instance, in [156] the authors propose an encryption mechanism based on controlled alternate quantum walks for privacy preserving of healthcare images in IoT. Moreover, the work in [157] presents a lattice-based conditional privacy preserving authentication mechanism for post-quantum vehicular communication. Adding quantum noise to protect quantum data will lead the security concept of DP towards quantum differential privacy. In [158] the author demonstrate this by including depolarization noise in quantum circuits for classification.

On the other hand, critical applications and massive scenarios expected in 5G/6G have raised the importance of novel privacy-related requirements, such as anonymity, unlinkability, and unobservability of the nodes in a network. Thus, from

the information theoretic point of view, a common approach to guarantee privacy is based on the perturbation of data attained by means of a privacy mechanism that performs a randomized mapping to control private information leakage. Quantifying this information leakage is important in order to limit this. Different notions of privacy leakage have been proposed to capture the capacity of adversaries to estimate private information, for example, Shannon's mutual information, differential privacy, among others [159], as well as different leakage measures. In that sense, privacy can, under careful control, tolerate some leakage to get some utility. There is no a general privacy vs. utility trade-off, thus the amount of leakage required to get some utility depends on the application [160].

VI. Security Standardization and Projects

As a critical aspect of next generation networks and digital services, the security domain has a very active standardization and project landscape. In this section, we highlight and delineate the key research projects and standardization efforts which have a prospective impact on 6G security[1]. At the end of the section we present Table V to show the summary of contribution of global-level ongoing projects, initiatives, associations and SDOs on 6G.

A. Standardization

Various Standards Developing Organizations (SDOs) which are relevant to 6G security as shown in Figure 11.

1) ETSI: As a multi-pronged effort, ETSI has launched multiple Industry Specification Groups (ISG) to examine 5G component technologies, including NFV (ETSI NFV), AI (ETSI ISG Securing Artificial Intelligence-SAI, ETSI ISG Experiential Network Intelligence - ENI) and network automation (ETSI ISG Zero touch and service management - ZSM). NFV-SEC is a WG under ISG NFV that produces industry specifications on security-related matters of NFV technology. Since 2014, the NFV SEC WG has produced multiple Group Specifications (GS) and Group Reports (GR). Work during releases 3 and 4 of ETSI NFV has increased the focus on security specifications as the scope and features of NFV platforms are expanding.

ETSI ISG ENI was also launched in 2017 to define a Cognitive Network Management architecture, using AI techniques and context-aware policies to adjust offered services based on changes in user needs, environmental conditions, and business goals. The ISG has produced a set of use cases, including network security, where the ENI system can detect various attacks and trigger a reaction by the network. Another group, ETSI ISG SAI, was formed in 2019 and aims to develop technical specifications to alleviate threats emerging from deploying AI and threats targeting AI systems originating from other AI systems and typical attack sources. This ISG has undertaken the tasks of defining AI threats, provide relevant use cases, recommend mitigation measures against such threats, and propose possible recommendations regarding data sharing.

[1]Please note that although there is a much wider spectrum of Beyond 5G or 6G projects and standardization activities, we focus on the ones with a significant security component or impact.

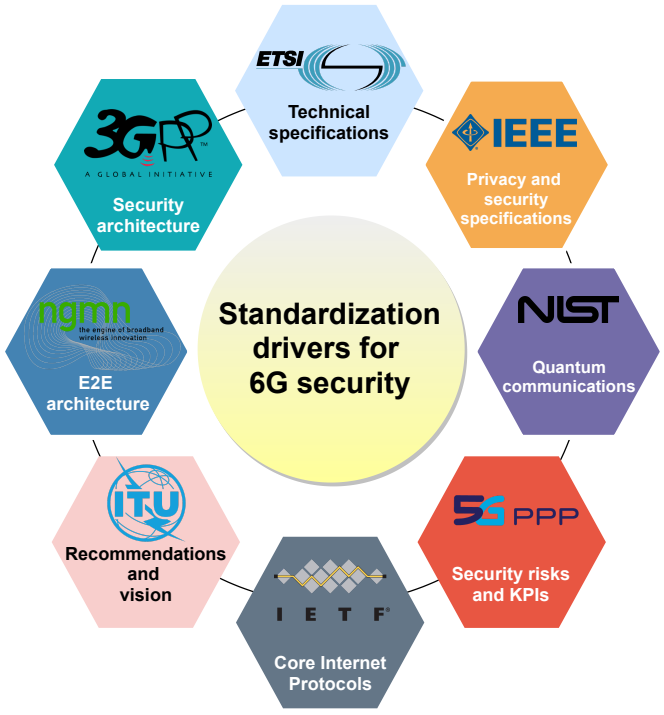

Fig. 11: Standardization landscape relevant for prospective 6G security standards.

2) ITU-T: At a global level, ITU has established the ITU-T Focus Group on ML for Future Networks (FG-ML5G) working on technical specifications for machine learning for future networks, including interfaces, network architectures, protocols, algorithms, and data formats [161]. ITU-T FG-NET2030 – Focus Group on Technologies for Network 2030 is elaborating on new drivers, requirements and gaps to propose use cases for applications including augmented and virtual reality and holograms. The developments will also have an impact on security aspects of 6G networks [162].

3) 3GPP: Similarly, 3GPP has already addressed the use of AI/ML in the 5G Core Service Based Architecture (SBA), by introducing the Network Data Analytics Function. This function provides analytics and notifications to other network functions regarding the users' behavior and the network's status. 3GPP SA3 is currently working on a draft TR by identifying the security issues, requirements, and solutions regarding Network Slicing and the use of the Network Data Analytics Function in selected use cases [163].

4) NIST: Standardization of post-quantum cryptographic algorithms is performed by National Institute of Standards and Technology (NIST) [164]. The ongoing work by NIST's Post-Quantum Cryptography Program is working to solicit candidates and then specify quantum-resistant algorithms each for digital signatures, public-key encryption and cryptographic key-establishment. The process is now at Round 3 following the completion of the second round in July 2020. The selected algorithms will constitute the first standard developed to

counter threats due to quantum decryption.

5) IETF: On the IETF front, IETF Security Automation and Continuous Monitoring (SACM) Architecture RFC defines an architecture enabling a cooperative SACM ecosystem based on entities, or components, which communicate by sharing information [165]. One or more components are consumers of information in a given flow while some are providers of information. A key component is an *orchestrator* which facilitates the automation of various functions such as configuration, coordination, and management for the SACM components. There can be also various *repositories* such as policy repositories, vulnerability definition data repositories, and security information repositories.

6) 5G PPP: 5G PPP has established 5G PPP Security Work Group as a joint effort on tackling 5G security risks and challenges and providing insights into 5G security and how it should be addressed [166]. It elaborates on 5G security architecture and how it fits with that of the 3GPP, access control, privacy, trust, security monitoring and management and standardisation on 5G security. Although it has a focus on 5G, the outcomes of the group have direct implications on Beyond 5G networks such as intelligent network security, security KPIs, emerging risks, threats and countermeasures.

7) NGMN: NGMN 5G End-to-End Architecture Framework v4.3 (2020) describes the requirements in terms of network entities and functions for the capabilities of an end-to-end framework which also includes security [167]. It considers the security for the end-to-end protection of the various network features and enabling capabilities in a forward-looking 5G service paradigm.

8) IEEE: IEEE P1915.1 Standard for Software Defined Networking and Network Function Virtualisation (SDN/NFV) Security works to provide a framework to build and operate secure SDN/NFV environments. It aims for different stakeholders such as end users, network operators, and service/content providers. To this end, it specifies a security framework for SDN/NFV with related system models, analytics, and requirements [168]. Similarly, IEEE P1917.1 Standard for Software Defined Networking and Network Function Virtualisation Reliability focuses on reliability requirements and develops a framework for reliable SDN/NFV service delivery infrastructure [169].

For the quantum communications, IEEE P1913.1 (Draft) Standard for Software-Defined Quantum Communication (SDQC) defines the SDQC protocol that enables configuration of quantum endpoints in a communication network [170]. It allows dynamic creation, modification, or removal of quantum protocols or applications in a software-defined setting. This is possible with the availability of a well-defined interface to quantum communication devices, which can be reconfigured to implement a variety of protocols and measurements. The SDQC protocol functions at the application layer and communicates over TCP/IP. The protocol design considers future integration with network softwarisation related standards.

B. Key Projects

1) 6G Flagship: The 6G Flagship [47] is a 8-year research project for "6G-Enabled Wireless Smart Society and Ecosystem" and funded by the Academy of Finland. 6G Flagship aims at the development of the new 6G standard for future digital societies. It will target security and privacy among other areas to develop essential technology components of 6G mobile networks. The research will focus on communication between people, devices, processes and objects, which implies a multitude of security and privacy questions. This will contribute to enabling a highly automated, smart society, which will penetrate all areas of life in the future. Finally, 6G flagship project will also carry out the large pilots with a test network with the support of both industry and academia.

2) INSPIRE-5Gplus: INSPIRE-5Gplus as an EC H2020 Research and Innovation (RIA) project aims to improve security of 5G and Beyond networks for various aspects such as the security vision, novel enablers, security assets, and learning models [38]. It will develop an integrated security management architecture using relevant frameworks, ZSM paradigm, Trusted Execution Environment (TEE), and address the key security challenges of vertical applications such as connected mobility, smart energy and aerial networks. Moreover, it will integrate trustworthiness and liability into the developed security approach for a holistic architecture [171].

3) 5GZORRO: 5GZORRO is an EC H2020 RIA project which will develop solutions for a system level architecture combining zero-touch automation and DLT in distributed multi-stakeholder environments. It will use Smart Contracts for intelligent resource discovery, brokerage and selection (e.g., spectrum and pervasive virtualized CDN services) and enable required agility [172]. Accordingly, it has a specific focus on security in future wireless networks.

4) Hexa-X: The Hexa-X project [173] targets to develop novel key enablers in 6G for

- radio access technologies at high frequencies
- high-resolution localization and sensing
- connected intelligence through AI-driven air interface
- 6G architectural elements for network disaggregation and dynamic dependability

For the security perspective, Hexa-X focuses on trustworthiness, namely the confidentiality and integrity of end-to-end communications, and guaranteed security, data privacy, and operational resilience. The final E2E Hexa-X architecture will include the developed security architecture and relevant security guidelines.

5) AI@EDGE: The AI@EDGE project aims to develop general-purpose frameworks for the creation, utilization, and adaptation of secure, reusable, and trustworthy AI/ML models. Those frameworks will support flexible and programmable pipelines and will be wielded for closed-loop network automation. Moreover, the project will work on a converged connect-compute platform for creating and managing resilient and secure network slices for various AI-enabled network applications [174].

6) ATIS/Next G Alliance: The Next G Alliance is an initiative formed for 6G development with for North American preeminence considering an evolutionary 5G path [175]. It has stemmed from the ATIS' "Call to Action Promoting U.S. Leadership on the Path to 6G". Therefore, the prospective 6G ecosystem will be key to defining the Next G vision.

Therefore, the Next G Alliance has determined three initial strategic actions to focus:

- Development of a 6G national roadmap that will lead North America to a global leader position in R&D, standardization, and manufacturing of Next G technologies while addressing the changing competitive landscape
- Alignment of the North American technology industry by converging on a core set of priorities to influence public policies and funding for 6G
- Identification of the early steps and strategies for rapid commercialization of Next G technologies across new markets and business sectors while promoting widescale adoption domestically and globally

7) South Korea MSIT 6G research program: The government of South Korea expects 6G services could be commercially available in Korea between 2028 and 2030 [176]. First deployment of 6G networks will be available in 2028 and mass scale commercial deployment will happen in 2030. The preliminary goal of their strategy includes launching a 6G pilot by 2026. Five major areas (digital healthcare immersive content, self-driving cars, smart cities and smart factories) are identified for these pilot projects.

The South Korean Ministry of Science and ICT (MSIT) has also formed the "6G R&D Strategy Committee" which consists of the three major mobile network operators, small and large scale equipment manufacturers, government agencies and public universities in South Korea. It will be responsible for management of 6G related projects. The 6G research program is also calling for proposals (led by 5G forum and 6G TF) to perform pilot projects to realize 6G vision. The goals of the 6G research program are 1)to reach the rate of 1 Tbps, 2)to reduce the wireless latency up to 0.1ms, 3)to extend the connectivity coverage range up to 10 km from the ground, 4)to utilize AI with entire network to cover all the segments, and 5) to use Security by design concept to protect the network.

8) Japan 6G/B5G Promotion Strategy: The Japanese government initiated Japan 6G/B5G promotion strategy in 2020 to promote research and development on 6G wireless communications services [177]. The Japanese government creates a fund to support the research and development and to build a 6G test-bed facility for academia and companies for testing their developed technologies. This funding scheme also plans to improve the collaboration between public-private sectors in 6G research and development. The 6G vision includes ultra-low power consumption, ultra-security and reliability, autonomy,

TABLE V: Contribution of global-level ongoing projects, initiatives, associations and SDOs on 6G.

	6G Architectural/ Technological/ Security Aspects									6G Applications							
	Intelligence Radio and RAN-Core Convergence	Edge Intelligence and Cloudification	Specialized 6G Networks	Blockchain/DLT	AI Security	Intelligence Network Management/ Orchestration	Privacy	Consumer end (terminal and users)	Quantum Security	UAV based Mobility	Holographic Telepresence	Extended Reality	Collaborative Autonomous Driving	Smart Grid 2.0	Industry 5.0	Digital Twin	Intelligent Healthcare
6G Projects																	
6G Flagship	✓	✓	✓	✓				✓		✓		✓	✓		✓		✓
Hexa-X	✓	✓	✓				✓			✓					✓	✓	
INSPIRE-5Gplus		✓		✓	✓	✓							✓				
5GZORRO		✓	✓			✓											
AI@EDGE		✓	✓		✓	✓								✓	✓		
ATIS/Next G Alliance	✓	✓	✓					✓		✓		✓	✓	✓	✓	✓	✓
South Korea MSIT 6G	✓	✓			✓		✓					✓	✓	✓	✓	✓	✓
Japan 6G/B5G Strategy	✓	✓			✓		✓		✓	✓		✓	✓	✓	✓	✓	✓
SDOs and Associations																	
ETSI	✓	✓		✓		✓			✓	✓		✓	✓	✓	✓		✓
NGMN	✓	✓		✓					✓	✓	✓	✓	✓	✓	✓		✓
NIST							✓		✓								✓
IETF			✓	✓		✓	✓		✓								
5G PPP	✓	✓	✓			✓				✓			✓	✓	✓		✓
IEEE	✓			✓	✓		✓		✓	✓			✓	✓			✓
3GPP	✓	✓	✓			✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
ITU-T	✓	✓	✓	✓	✓		✓		✓	✓	✓	✓	✓	✓	✓		✓

and scalability, in addition to the further advancement of 5G's characteristic features such as high speed and high capacity, low latency, and multiple simultaneous connections. Moreover, this 6G/B5G promotion strategy is aiming to establish and showcase the core technologies for the 6G system by 2025 and put the new technologies into practical use by 2030.

VII. Discussion

There is obviously a long journey to get to 6G, while current 5G will continue to evolve over the next few years. Every new generation brings a big leap with respect to previous generation. However, in the long run 6G will be a revolution rather than an evolution due to the self managing networks and will drive towards a more sustainable and trustworthy society.

The goal of 6G networks is to fulfill the connectivity requirements of the 2030s and beyond human society. 6G will be the key communication infrastructure to satisfy the demands of future needs of hyper-connected human society in the 2030 and beyond [25]. The development of new technologies such as smart surfaces, zero energy IoT devices, advance AI techniques, possible quantum computing systems, AI-powered automated devices, AI driven air interfaces, humanoid robots, self sustained networks, and future trends of digital societies' such as massive availability of small data, increasing elderly population, convergence of communication, sensing, and computing, gadget-free communication will demands new applications. Thus, 6G will support new applications such as UAV based mobility, Connected Autonomous Vehicles (CAV), Smart Grid 2.0, Collaborative Robots, Hyper-Intelligent Healthcare, Industry 5.0, Digital Twin and Extended Reality.

In this paper, we have identified mainly four key technological domains which may bring the highest impact on 6G security and privacy. In Table VI we summarize the benefits and challenges with using Blockchain/DLT for security, quantum security, distributed AI/ML security, and PLS. The security, surveillance, accountability, and governance of the network can be implemented through blockchain and DLT in general. As DLT allows to store immutable and transparent logs for each event which can be utilized in the auditing of events, it may introduce trust among unknown entities in the system. However, DLTs may introduce lots of issues with the user and data privacy and extra computation and storage overhead when they try to achieve this trust level. With quantum security algorithms and their implications in network protocols and related security procedures, such as post-quantum cryptography and quantum key distribution, should be considered in the design of next-generation networks. AI/ML has two aspects regarding security: It can enable security as well as suffer from threats and vulnerabilities as a founding element of 6G networks. In 6G, AI/ML will be pushed closer to the source of data for ultra-low latency while distributing ML functions over the network to attain performance gains due to optimized models and ensemble decision making. However, overcoming practical constraints of some network elements (e.g., IoT) will be challenging with AI security. PLS mechanisms are expected to advocate and develop relying on the unique characteristics and properties of wireless channels to secure wireless communication. This may include the list of security operations such as authentication, encryption, and key exchange.

As described in Section III, 6G applications will support different stakeholders and demand different levels of network requirements including security. Since these applications are arising with 6G and pre-6G security models will not be applicable or sufficient enough to provided required level of security for 6G applications. Moreover, a new set of security attacks can be arises via these new applications. Therefore, 6G networks have to address the security issues due to novel 6G applications. The main security threats and possible defense mechanisms related to key 6G technologies and 6G applications which are discussed in the previous sections are summarized in Table VII.

VIII. Conclusion

In parallel to the deployment of 5G wireless systems, the scientific community is setting the stage for next wireless evolution towards 6G. Driving the vision of 6G security towards a reality has already initiated from the research level. In this paper, we presented one of the first surveys of 6G security and privacy which covers all the possible areas that could be touched with 6G security considerations. It has its

TABLE VI: Solutions and Technologies.

Technology	**Benefits and utility for security**	**Challenges**
Blockchain/ DLT for security	- Provisioning of transparency - Allow trustless trading among unknown entities	- Preserving privacy - High overhead
Quantum security	- Provide unbreakable quantum-safe security	- Lack of existing processing power with current networking devices. - Marginal availability of standardization.
Distributed AI/ML security	- Higher accuracy - Autonomous security management - Optimized security enforcement - Omnipresent operation - Feasibility	- Scalability - Distribution management - Securing of models and data pipes - Computational infrastructure protection - Explainability
Physical layer security	- Provides a first line of defense - Requires little or no additional computing resources, and does not rely on the computational robustness of attackers - Particularly attractive for umMTC and eURLLC	- Integration with higher layer solutions - Trade-off between security performance, energy efficiency, latency, and reliability - Regulatory and standardisation aspects are still to be addressed

TABLE VII: Summary of security attacks and their impact on 6G architecture, key technologies and applications.

		6G architectural blocks					Key 6G applications							
Security attacks	**Possible defense mechanisms**	Int. Radio/RAN-Core Convergence	Edge Intelligence and Cloudification	Specialized 6G Networks	Int. Net. Management/ Orchestration	Consumer end (terminals and users)	UAV	Holographic Telepresence	Extended Reality	Connected autonomous vehicles	Smart Grid 2.0	Industry 5.0	Hyper-intelligence health	Digital Twin
AI/ML														
Poisonous attacks	Moving target defense/ Input validation	✓	✓	✓	✓	✓	✓			✓		✓	✓	
Evasion attacks	Defensive distillation/ Adversarial training	✓	✓	✓	✓	✓	✓			✓	✓	✓		
Infrastructure physical attacks & communication tampering	Use tamper-proof hardware	✓	✓	✓	✓	✓	✓			✓	✓	✓	✓	✓
Compromise of AI frameworks	Security solutions for software, firmware and hardware.	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓
ML API-based Attacks	Control information provided by ML APIs		✓		✓		✓			✓	✓	✓	✓	
Model inversion attacks	Noise injection		✓		✓		✓			✓	✓	✓	✓	
Model extraction attacks	Control information provided by ML APIs/ Noise injection		✓		✓		✓			✓	✓	✓	✓	✓
Adversarial attacks	Defensive distillation/ Adversarial training/ Input validation		✓		✓		✓			✓	✓	✓	✓	
Privacy attacks	Differential privacy/ Homomorphic encryption.		✓			✓		✓					✓	✓
Blockchain														
Majority/ 51% attack	Select proper DLT architecture.		✓	✓	✓		✓			✓	✓	✓	✓	✓
Double-spending attacks	Protect transactions.			✓			✓		✓	✓	✓		✓	
Re-entrency attack	Use security check tools.			✓	✓		✓			✓		✓	✓	
Sybil attacks	Use strong authentication and access control mechanisms.	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Authentication access control attacks	Use robust authentication and access control mechanisms.	✓		✓		✓	✓	✓	✓	✓	✓	✓	✓	✓
Security misconfigurations	Identify semantic flaws.	✓		✓			✓	✓	✓	✓	✓	✓	✓	✓
Privacy attacks	Privacy by design approach.		✓			✓		✓	✓	✓	✓		✓	✓
Quantum computing														
Quantum cloning attack	Uncloneable encryption mechanisms					✓		✓						✓
Quantum collision attack	Quantum resistant encryption solutions					✓		✓						✓
VLC														
Authentication/ access control attacks	Location-based authentication	✓		✓		✓				✓		✓		
Eavesdropping	Artificial noise-assisted visible light MIMO beamforming	✓								✓		✓		
Jamming and data modification attacks	ML techniques to learn the environment in real time	✓		✓						✓		✓		
THz														
Authentication access control attacks	Electromagnetic signatures for physical layer authentication	✓		✓		✓	✓			✓		✓		
Eavesdropping	Characterization of the backscatter channel / Exploting multipath.	✓					✓			✓		✓		
Molecular communication														
Authentication access control attacks	Biochemical cryptography.			✓		✓							✓	
Privacy attacks	Information-theoretic privacy /Camouflage of DNA-based messages					✓							✓	
RIS														
Authentication access control attacks	RIS-assisted secret key generation.	✓		✓		✓	✓			✓		✓		
Eavesdropping	Controlling of phase shifts of RIS to improve secrecy performance.	✓					✓			✓		✓		

roots in a first white paper written by a group of telecommunication security experts. 6G is still in initial phases and 3GPP has not yet started the standardization with deployment around 2030. Still, this survey tried to identify the relevant security technologies and threat landscape based on future use scenarios of 6G. We described security issues related to the most renowned 6G potential use cases such as Industry 5.0, digital twin, Unmanned Aircraft and Autonomous Vechicle control, Extended reality and SmartGrid 2.0. In addition to that, we discussed the threat landscape and possible solutions with respect to the key 6G technologies including AI/ML, DLT, Quantum Computing, VLC and THz communication. We also presented the significance of privacy in the 6G vision towards reality. Finally, we summarized the ongoing research projects on 6G which have the closest alliance with security and privacy. As a whole, our intention was to compile this survey to serve as an enlightening guideline for the future research works on 6G security.

ACKNOWLEDGMENT

This work has been performed under the framework of 6Genesis Flagship (grant 318927) and 5GEAR projects. The research leading to these results partly received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 871808 (5G PPP project INSPIRE-5Gplus). The paper reflects only the authors' views. The Commission is not responsible for any use that may be made of the information it contains. A. Gurtov was partly supported by CENIIT project 17.01 and by Excellence Center at Linköping-Lund in IT (ELLIIT).

REFERENCES

[1] P. Porambage, G. Gür, D. P. M. Osorio, M. Liyanage, and M. Ylianttila, "6G Security Challenges and Potential Solutions," in *2021 Joint European Conference on Networks and Communications (EuCNC) and 6G Summit*. IEEE, 2021, pp. 1–6.

[2] C. de Alwis, A. Kalla, Q. V. Pham, P. Kumar, K. Dev, W. J. Hwang, and M. Liyanage, "Survey on 6G Frontiers: Trends, Applications, Requirements, Technologies and Future Research," *IEEE Open Journal of the Communications Society*, pp. 1–1, 2021.

[3] X. You, C.-X. Wang, J. Huang, X. Gao, Z. Zhang, M. Wang, Y. Huang, C. Zhang, Y. Jiang, J. Wang *et al.*, "Towards 6G wireless communication networks: Vision, enabling technologies, and new paradigm shifts," *Science China Information Sciences*, vol. 64, no. 1, pp. 1–74, 2021.

[4] S. J. Nawaz, S. K. Sharma, S. Wyne, M. N. Patwary, and M. Asaduzzaman, "Quantum machine learning for 6G communication networks: State-of-the-art and vision for the future," *IEEE Access*, vol. 7, pp. 46 317–46 350, 2019.

[5] V. Ziegler, H. Viswanathan, H. Flinck, M. Hoffmann, V. Räisänen, and K. Hätönen, "6G architecture to connect the worlds," *IEEE Access*, vol. 8, pp. 173 508–173 520, 2020.

[6] H. Viswanathan and P. E. Mogensen, "Communications in the 6G era," *IEEE Access*, vol. 8, pp. 57 063–57 074, 2020.

[7] S. Wijethilaka and M. Liyanage, "Survey on network slicing for internet of things realization in 5g networks," *IEEE Communications Surveys & Tutorials*, 2021.

[8] G. Gui, M. Liu, F. Tang, N. Kato, and F. Adachi, "6G: Opening new horizons for integration of comfort, security and intelligence," *IEEE Wireless Communications*, 2020.

[9] M. Wang, T. Zhu, T. Zhang, J. Zhang, S. Yu, and W. Zhou, "Security and privacy in 6G networks: New areas and new challenges," *Digital Communications and Networks*, vol. 6, no. 3, pp. 281–291, 2020.

[10] M. Liyanage, I. Ahmad, A. B. Abro, A. Gurtov, and M. Ylianttila, *A comprehensive guide to 5G security*. Wiley Online Library, 2018.

[11] M. Liyanage, A. B. Abro, M. Ylianttila, and A. Gurtov, "Opportunities and challenges of software-defined mobile networks in network security," *IEEE security & privacy*, vol. 14, no. 4, pp. 34–44, 2016.

[12] R. Khan, P. Kumar, D. N. K. Jayakody, and M. Liyanage, "A survey on security and privacy of 5g technologies: Potential solutions, recent advancements, and future directions," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 196–248, 2019.

[13] B. Schneier, "Artificial intelligence and the attack/defense balance," *IEEE security & privacy*, vol. 16, no. 2, pp. 96–96, 2018.

[14] W. Saad, M. Bennis, and M. Chen, "A vision of 6G wireless systems: Applications, trends, technologies, and open research problems," *IEEE network*, vol. 34, no. 3, pp. 134–142, 2019.

[15] S. Dang, O. Amin, B. Shihada, and M.-S. Alouini, "What should 6G be?" *Nature Electronics*, vol. 3, no. 1, pp. 20–29, 2020.

[16] S. Chen, Y.-C. Liang, S. Sun, S. Kang, W. Cheng, and M. Peng, "Vision, requirements, and technology trend of 6G: How to tackle the challenges of system coverage, capacity, user data-rate and movement speed," *IEEE Wireless Communications*, vol. 27, no. 2, pp. 218–228, 2020.

[17] T. Huang, W. Yang, J. Wu, J. Ma, X. Zhang, and D. Zhang, "A survey on green 6G network: Architecture and technologies," *IEEE Access*, vol. 7, pp. 175 758–175 768, 2019.

[18] M. Ylianttila, R. Kantola, A. Gurtov, L. Mucchi, I. Oppermann, Z. Yan, T. H. Nguyen, F. Liu, T. Hewa, M. Liyanage *et al.*, "6G white paper: Research challenges for trust, security and privacy," *arXiv preprint arXiv:2004.11665*, 2020.

[19] Y. Sun, J. Liu, J. Wang, Y. Cao, and N. Kato, "When machine learning meets privacy in 6G: A survey," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 4, pp. 2694–2724, 2020.

[20] M. Shakiba-Herfeh, A. Chorti, and H. V. Poor, "Physical layer security: Authentication, integrity, and confidentiality," in *Physical Layer Security*. Springer, 2021, pp. 129–150.

[21] S. Nayak and R. Patgiri, "6G communication technology: A vision on intelligent healthcare," *arXiv preprint arXiv:2005.07532*, 2020.

[22] F. Jameel, U. Javaid, B. Sikdar, I. Khan, G. Mastorakis, and C. X. Mavromoustakis, "Optimizing blockchain networks with artificial intelligence: Towards efficient and reliable iot applications," in *Convergence of Artificial Intelligence and the Internet of Things*. Springer, 2020, pp. 299–321.

[23] Z. Zhang, Y. Xiao, Z. Ma, M. Xiao, Z. Ding, X. Lei, G. K. Karagiannidis, and P. Fan, "6G wireless networks: Vision, requirements, architecture, and key technologies," *IEEE Vehicular Technology Magazine*, vol. 14, no. 3, pp. 28–41, 2019.

[24] P. Ranaweera, A. D. Jurcut, and M. Liyanage, "Survey on multi-access edge computing security and privacy," *IEEE Communications Surveys & Tutorials*, 2021.

[25] M. Latva-Aho and K. Leppänen, "Key drivers and research challenges for 6G ubiquitous wireless intelligence (white paper)," *Oulu, Finland: 6G Flagship*, 2019.

[26] A. Pouttu, F. Burkhardt, C. Patachia, L. Mendes, G. R. Brazil, S. Pirttikangas, E. Jou, P. Kuvaja, F. T. Finland, M. Heikkilä *et al.*, "6g white paper on validation and trials for verticals towards 2030's." [Online]. Available: https://www.6gchannel.com/wp-content/uploads/2020/04/6g-white-paper-validation-trials.pdf

[27] United Nations (UN) #Envision2030 Sustainable Development Goals, "United Nations (UN)." [Online]. Available: https://sdgs.un.org/goals

[28] V. Ziegler and S. Yrjola, "6g indicators of value and performance," in *2020 2nd 6G wireless summit (6G SUMMIT)*. IEEE, 2020, pp. 1–5.

[29] K. B. Letaief, W. Chen, Y. Shi, J. Zhang, and Y. A. Zhang, "The roadmap to 6G: Ai empowered wireless networks," *IEEE Communications Magazine*, vol. 57, no. 8, pp. 84–90, 2019.

[30] M. Yao, M. Sohul, V. Marojevic, and J. H. Reed, "Artificial intelligence defined 5g radio access networks," *IEEE Communications Magazine*, vol. 57, no. 3, pp. 14–20, 2019.

[31] H. Viswanathan and P. E. Mogensen, "Communications in the 6G era," *IEEE Access*, vol. 8, pp. 57 063–57 074, 2020.

[32] S. Deng, H. Zhao, W. Fang, J. Yin, S. Dustdar, and A. Y. Zomaya, "Edge intelligence: the confluence of edge computing and artificial intelligence," *IEEE Internet of Things Journal*, vol. 7, no. 8, pp. 7457–7469, 2020.

[33] G. Plastiras, M. Terzi, C. Kyrkou, and T. Theocharidcs, "Edge intelligence: Challenges and opportunities of near-sensor machine learning applications," in *2018 IEEE 29th International Conference on Application-specific Systems, Architectures and Processors (ASAP)*, 2018, pp. 1–7.

[34] S. Xu, Y. Qian, and R. Q. Hu, "Edge intelligence assisted gateway defense in cyber security," *IEEE Network*, vol. 34, no. 4, pp. 14–19, 2020.

[35] M. Mukherjee, R. Matam, C. X. Mavromoustakis, H. Jiang, G. Mastorakis, and M. Guo, "Intelligent edge computing: Security and privacy challenges," *IEEE Communications Magazine*, vol. 58, no. 9, pp. 26–31, 2020.

[36] R. Kalaiprasath, R. Elankavi, and R. Udayakumar, "Cloud security and compliance-a semantic approach in end to end security." *International Journal on Smart Sensing & Intelligent Systems*, vol. 10, 2017.

[37] C. Benzaid and T. Taleb, "ZSM security: Threat surface and best practices," *IEEE Network*, vol. 34, no. 3, pp. 124–133, 2020.

[38] J. Ortiz, R. Sanchez-Iborra, J. B. Bernabe, A. Skarmeta, C. Benzaid, T. Taleb, P. Alemany, R. Muñoz, R. Vilalta, C. Gaber *et al.*, "Inspire-5gplus: Intelligent security and pervasive trust for 5g and beyond networks," in *Proceedings of the 15th International Conference on Availability, Reliability and Security*, 2020, pp. 1–10.

[39] Y. Siriwardhana, P. Porambage, M. Liyanage, and M. Ylianttila, "AI and 6G Security: Opportunities and Challenges," in *2021 Joint European Conference on Networks and Communications (EuCNC) and 6G Summit*. IEEE, 2021, pp. 1–6.

[40] 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.

[41] I. Sanchez-Navarro, P. Salva-Garcia, Q. Wang, and J. M. A. Calero, "New immersive interface for zero-touch management in 5g networks," in *2020 IEEE 3rd 5G World Forum (5GWF)*. IEEE, 2020, pp. 145–150.

[42] M. Hyder and M. Ismail, "Inmtd: Intent-based moving target defense framework using software defined networks," *Engineering, Technology & Applied Science Research*, vol. 10, no. 1, pp. 5142–5147, 2020.

[43] Y. Han, J. Li, D. Hoang, J.-H. Yoo, and J. W.-K. Hong, "An intent-based network virtualization platform for sdn," in *2016 12th International Conference on Network and Service Management (CNSM)*. IEEE, 2016, pp. 353–358.

[44] Y. Wei, M. Peng, and Y. Liu, "Intent-based networks for 6g: Insights and challenges," *Digital Communications and Networks*, vol. 6, no. 3, pp. 270–280, 2020.

[45] G. ETSI, "004, Zero-touch network and service management (ZSM)," *Reference Architecture*, 2020.

[46] R. Yasmin, J. Petäjäjärvi, K. Mikhaylov, and A. Pouttu, "On the integration of lorawan with the 5g test network," in *2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*. IEEE, 2017, pp. 1–6.

[47] "6G Flagship project." [Online]. Available: https://www.oulu.fi/6gflagship/

[48] E. Peltonen, M. Bennis, M. Capobianco, M. Debbah, A. Ding, F. Gil-Castiñeira, M. Jurmu, T. Karvonen, M. Kelanti, A. Kliks *et al.*, "6G white paper on edge intelligence," *arXiv preprint arXiv:2004.14850*, 2020.

[49] B. Deebak and F. Al-Turjman, "Drone of IoT in 6G wireless communications: Technology, challenges, and future aspects," in *Unmanned Aerial Vehicles in Smart Cities*. Springer, 2020, pp. 153–165.

[50] H. Menouar, I. Guvenc, K. Akkaya, A. S. Uluagac, A. Kadri, and A. Tuncer, "UAV-enabled intelligent transportation systems for the smart city: Applications and challenges," *IEEE Communications Magazine*, vol. 55, no. 3, pp. 22–28, 2017.

[51] P. B. Johnston and A. K. Sarbahi, "The impact of us drone strikes on terrorism in pakistan," *International Studies Quarterly*, vol. 60, no. 2, pp. 203–219, 2016.

[52] J. O'Malley, "The no drone zone," *Engineering & Technology*, vol. 14, no. 2, pp. 34–38, 2019.

[53] M. Giordani, M. Polese, M. Mezzavilla, S. Rangan, and M. Zorzi, "Toward 6G networks: Use cases and technologies," *IEEE Communications Magazine*, vol. 58, no. 3, pp. 55–61, 2020.

[54] I. Petrov and T. Janevski, "5G mobile technologies and early 6G viewpoints," *European Journal of Engineering Research and Science*, vol. 5, no. 10, pp. 1240–1246, 2020.

[55] K. Lebeck, K. Ruth, T. Kohno, and F. Roesner, "Towards security and privacy for multi-user augmented reality: Foundations with end users," in *2018 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2018, pp. 392–408.

[56] F. Tariq, M. R. Khandaker, K.-K. Wong, M. A. Imran, M. Bennis, and M. Debbah, "A speculative study on 6G," *IEEE Wireless Communications*, vol. 27, no. 4, pp. 118–125, 2020.

[57] Y. Siriwardhana, P. Porambage, M. Liyanage, and M. Ylinattila, "A Survey on Mobile Augmented Reality with 5G Mobile Edge Computing: Architectures, Applications and Technical Aspects," *IEEE Communications Surveys Tutorials*, pp. 1–1, 2021.

[58] C. Insights, "40+ corporations working on autonomous vehicles," 2019.

[59] J. He, K. Yang, and H. H. Chen, "6G cellular networks and connected autonomous vehicles," *IEEE Network*, pp. 1–7, 2020.

[60] H. Shahinzadeh, J. Moradi, G. B. Gharehpetian, H. Nafisi, and M. Abedi, "Internet of Energy (IoE) in smart power systems," in *2019 5th Conference on Knowledge Based Engineering and Innovation (KBEI)*. IEEE, 2019, pp. 627–636.

[61] I. Andrea, C. Chrysostomou, and G. Hadjichristofi, "Internet of Things: Security Vulnerabilities and Challenges," *Proceedings - IEEE Symposium on Computers and Communications*, vol. 2016-Febru, no. August 2017, pp. 180–187, 2016.

[62] D. Pliatsios, P. Sarigiannidis, T. Lagkas, and A. G. Sarigiannidis, "A Survey on SCADA Systems: Secure Protocols, Incidents, Threats and Tactics," *IEEE Communications Surveys Tutorials*, vol. 22, no. 3, pp. 1942–1976, 2020.

[63] E. Hossain, I. Khan, F. Un-Noor, S. S. Sikander, and M. S. H. Sunny, "Application of Big Data and Machine Learning in Smart Grid, and Associated Security Concerns: A Review," *IEEE Access*, vol. 7, no. c, pp. 13 960–13 988, 2019.

[64] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, and Y. Zhang, "Consortium Blockchain for Secure Energy Trading in Industrial Internet of Things," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3690–3700, 2018.

[65] A. Miglani, N. Kumar, V. Chamola, and S. Zeadally, "Blockchain for Internet of Energy Management: Review, Solutions, and Challenges," *Computer Communications*, vol. 151, pp. 395–418, 2020.

[66] S. Nahavandi, "Industry 5.0—a human-centric solution," *Sustainability*, vol. 11, no. 16, p. 4371, 2019.

[67] X. Xu, "From cloud computing to cloud manufacturing," *Robotics and computer-integrated manufacturing*, vol. 28, no. 1, pp. 75–86, 2012.

[68] L. Mucchi, S. Jayousi, S. Caputo, E. Paoletti, P. Zoppi, S. Geli, and P. Dioniso, "How 6G technology can change the future wireless healthcare," in *2020 2nd 6G Wireless Summit (6G SUMMIT)*. IEEE, 2020, pp. 1–6.

[69] D. P. Isravel, S. Silas, and E. B. Rajsingh, "SDN-based traffic management for personalized ambient assisted living healthcare system," in *Intelligence in Big Data Technologies—Beyond the Hype*. Springer, 2020, pp. 379–388.

[70] EC The High-Level Expert Group on Artificial Intelligence (AI HLEG), "Ethics guidelines for trustworthy ai," 2019. [Online]. Available: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

[71] M. Grieves and J. Vickers, "Digital twin: Mitigating unpredictable, undesirable emergent behavior in complex systems," in *Transdisciplinary perspectives on complex systems*. Springer, 2017, pp. 85–113.

[72] M. W. Grieves, "Virtually intelligent product systems: digital and physical twins," 2019.

[73] T. Hewa, M. Ylianttila, and M. Liyanage, "Survey on blockchain based smart contracts: Applications, opportunities and challenges," *Journal of Network and Computer Applications*, p. 102857, 2020.

[74] M. Barreno, B. Nelson, R. Sears, A. D. Joseph, and J. D. Tygar, "Can machine learning be secure?" in *Proceedings of the 2006 ACM Symposium on Information, computer and communications security*, 2006, pp. 16–25.

[75] H. Kim, J. Park, M. Bennis, and S.-L. Kim, "On-device federated learning via blockchain and its latency analysis," *arXiv preprint arXiv:1808.03949*, 2018.

[76] N. Weerasinghe, T. Hewa, M. Liyanage, S. S. Kanhere, and M. Ylianttila, "A Novel Blockchain-as-a-Service (BaaS) Platform for Local 5G Operators," *IEEE Open Journal of the Communications Society*, vol. 2, pp. 575–601, 2021.

[77] Z. Liu, N. C. Luong, W. Wang, D. Niyato, P. Wang, Y.-C. Liang, and D. I. Kim, "A Survey on Blockchain: a Game Theoretical Perspective," *IEEE Access*, vol. 7, pp. 47 615–47 643, 2019.

[78] T. M. Hewa, Y. Hu, M. Liyanage, S. Kanhare, and M. Ylianttila, "Survey on Blockchain based Smart Contracts: Technical Aspects and Future Research," *IEEE Access*, pp. 1–1, 2021.

[79] S. Dey, "Securing majority-attack in blockchain using machine learning and algorithmic game theory: A proof of work," in *2018 10th computer science and electronic engineering (CEEC)*. IEEE, 2018, pp. 7–10.

[80] J. Moubarak, E. Filiol, and M. Chamoun, "On blockchain security and relevant attacks," in *2018 IEEE Middle East and North Africa Communications Conference (MENACOMM)*. IEEE, 2018, pp. 1–6.

[81] D. Efanov and P. Roschin, "The all-pervasiveness of the blockchain technology," *Procedia Computer Science*, vol. 123, pp. 116–121, 2018.

[82] U. W. Chohan, "The double spending problem and cryptocurrencies," *Available at SSRN 3090174*, 2017.

[83] S. Zhang and J.-H. Lee, "Double-spending with a sybil attack in the bitcoin decentralized network," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 10, pp. 5715–5722, 2019.

[84] M. I. Mehar, C. L. Shier, A. Giambattista, E. Gong, G. Fletcher, R. Sanayhie, H. M. Kim, and M. Laskowski, "Understanding a revolutionary and flawed grand experiment in blockchain: The dao attack," *Journal of Cases on Information Technology (JCIT)*, vol. 21, no. 1, pp. 19–32, 2019.

[85] P. Otte, M. de Vos, and J. Pouwelse, "Trustchain: A sybil-resistant scalable blockchain," *Future Generation Computer Systems*, vol. 107, pp. 770–780, 2020.

[86] Y. Cai and D. Zhu, "Fraud detections for online businesses: a perspective from blockchain technology," *Financial Innovation*, vol. 2, no. 1, p. 20, 2016.

[87] Q. Feng, D. He, S. Zeadally, M. K. Khan, and N. Kumar, "A survey on privacy protection in blockchain system," *Journal of Network and Computer Applications*, vol. 126, pp. 45–58, 2019.

[88] B. Bünz, S. Agrawal, M. Zamani, and D. Boneh, "Zether: Towards privacy in a smart contract world," in *International Conference on Financial Cryptography and Data Security*. Springer, 2020, pp. 423–443.

[89] A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak, "Blockchain: A Distributed Solution to Automotive Security and Privacy," *IEEE Communications Magazine*, vol. 55, no. 12, pp. 119–125, 2017.

[90] Z. Bao, Q. Wang, W. Shi, L. Wang, H. Lei, and B. Chen, "When blockchain meets SGX: An overview, challenges, and open issues," *IEEE Access*, 2020.

[91] A. Groce, J. Feist, G. Grieco, and M. Colburn, "What are the actual flaws in important smart contracts (and how can we find them)?" in *International Conference on Financial Cryptography and Data Security*. Springer, 2020, pp. 634–653.

[92] C. Liu, J. Gao, Y. Li, H. Wang, and Z. Chen, "Studying gas exceptions in blockchain-based cloud applications," *Journal of Cloud Computing*, vol. 9, no. 1, pp. 1–25, 2020.

[93] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," *Future Generation Computer Systems*, vol. 107, pp. 841–853, 2020.

[94] K. Chatterjee, A. K. Goharshady, and A. Pourdamghani, "Probabilistic smart contracts: Secure randomness on the blockchain," in *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. IEEE, 2019, pp. 403–412.

[95] C. G. Harris, "The risks and challenges of implementing ethereum smart contracts," in *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. IEEE, 2019, pp. 104–107.

[96] S. Kim and S. Ryu, "Analysis of blockchain smart contracts: Techniques and insights," in *2020 IEEE Secure Development (SecDev)*. IEEE, 2020, pp. 65–73.

[97] H. Poston, "Mapping the owasp top ten to blockchain," *Procedia Computer Science*, vol. 177, pp. 613–617, 2020.

[98] G. Karame and S. Capkun, "Blockchain security and privacy," *IEEE Security & Privacy*, vol. 16, no. 04, pp. 11–12, 2018.

[99] F. H. Pohrmen, R. K. Das, and G. Saha, "Blockchain-based security aspects in heterogeneous internet-of-things networks: A survey," *Transactions on Emerging Telecommunications Technologies*, vol. 30, no. 10, p. e3741, 2019.

[100] A. Singh, R. M. Parizi, Q. Zhang, K.-K. R. Choo, and A. Dehghantanha, "Blockchain smart contracts formalization: Approaches and challenges to address vulnerabilities," *Computers & Security*, vol. 88, p. 101654, 2020.

[101] Y. Zhang, S. Ma, J. Li, K. Li, S. Nepal, and D. Gu, "SMARTSHIELD: Automatic smart contract protection made easy," in *2020 IEEE 27th International Conference on Software Analysis, Evolution and Reengineering (SANER)*. IEEE, 2020, pp. 23–34.

[102] N. Atzei, M. Bartoletti, and T. Cimoli, "A Survey of Attacks on Ethereum Smart Contracts (sok)," in *International Conference on Principles of Security and Trust*. Springer, 2017, pp. 164–186.

[103] M. Wohrer and U. Zdun, "Smart contracts: security patterns in the ethereum ecosystem and solidity," in *2018 International Workshop on Blockchain Oriented Software Engineering (IWBOSE)*, March 2018, pp. 2–8.

[104] C. Liu, H. Liu, Z. Cao, Z. Chen, B. Chen, and B. Roscoe, "ReGuard: Finding reentrancy bugs in smart contracts," in *Proceedings of the 40th International Conference on Software Engineering: Companion Proceeedings*. ACM, 2018, pp. 65–68.

[105] B. Jiang, Y. Liu, and W. Chan, "Contractfuzzer: Fuzzing smart contracts for vulnerability detection," in *Proceedings of the 33rd ACM/IEEE International Conference on Automated Software Engineering*. ACM, 2018, pp. 259–269.

[106] L. Brent, A. Jurisevic, M. Kong, E. Liu, F. Gauthier, V. Gramoli, R. Holz, and B. Scholz, "Vandal: A scalable security analysis framework for smart contracts," *arXiv preprint arXiv:1809.03981*, 2018.

[107] K. Bhargavan, A. Delignat-Lavaud, C. Fournet, A. Gollamudi, G. Gonthier, N. Kobeissi, A. Rastogi, T. Sibut-Pinote, N. Swamy, and S. Zanella-Béguelin, "Short paper: Formal verification of smart contracts," in *Proceedings of the 11th ACM Workshop on Programming Languages and Analysis for Security (PLAS), in conjunction with ACM CCS*, 2016, pp. 91–96.

[108] T. Abdellatif and K.-L. Brousmiche, "Formal verification of smart contracts based on users and blockchain behavior models," in *2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*. IEEE, 2018, pp. 1–5.

[109] Z. Nehai, P.-Y. Piriou, and F. Daumas, "Model-checking of smart contracts," in *IEEE International Conference on Blockchain*, 2018, pp. 980–987.

[110] E. Albert, P. Gordillo, B. Livshits, A. Rubio, and I. Sergey, "EthIR: A framework for high-level analysis of ethereum bytecode," in *International Symposium on Automated Technology for Verification and Analysis*. Springer, 2018, pp. 513–520.

[111] P. Schaar, "Privacy by design," *Identity in the Information Society*, vol. 3, no. 2, pp. 267–274, 2010.

[112] A. Cavoukian *et al.*, "Privacy by design: The 7 foundational principles," *Information and privacy commissioner of Ontario, Canada*, vol. 5, p. 12, 2009.

[113] R. Cheng, F. Zhang, J. Kos, W. He, N. Hynes, N. Johnson, A. Juels, A. Miller, and D. Song, "Ekiden: A Platform for Confidentiality-Preserving, Trustworthy, and Performant Smart Contracts," 1804.

[114] R. Yuan, Y.-B. Xia, H.-B. Chen, B.-Y. Zang, and J. Xie, "Shadoweth: Private Smart Contract on Public Blockchain," *Journal of Computer Science and Technology*, vol. 33, no. 3, pp. 542–556, 2018.

[115] R. Gupta, S. Tanwar, F. Al-Turjman, P. Italiya, A. Nauman, and S. W. Kim, "Smart contract privacy protection using ai in cyber-physical systems: tools, techniques and challenges," *IEEE Access*, vol. 8, pp. 24 746–24 772, 2020.

[116] N. Kapsoulis, A. Psychas, G. Palaiokrassas, A. Marinakis, A. Litke, and T. Varvarigou, "Know your customer (kyc) implementation with smart contracts on a privacy-oriented decentralized architecture," *Future Internet*, vol. 12, no. 2, p. 41, 2020.

[117] M. Niranjanamurthy, B. Nithya, and S. Jagannatha, "Analysis of Blockchain technology: pros, cons and SWOT," *Cluster Computing*, vol. 22, no. 6, pp. 14 743–14 757, 2019.

[118] M. Roetteler, M. Naehrig, K. M. Svore, and K. Lauter, "Quantum resource estimates for computing elliptic curve discrete logarithms," in *International Conference on the Theory and Application of Cryptology and Information Security*. Springer, 2017, pp. 241–270.

[119] D. J. Bernstein and T. Lange, "Post-quantum cryptography," *Nature*, vol. 549, no. 7671, pp. 188–194, 2017.

[120] S. Tarantino, B. Da Lio, D. Cozzolino, and D. Bacco, "Feasibility of quantum communications in aquatic scenarios," *Optik*, p. 164639, 2020.

[121] F. Bouchard, R. Fickler, R. W. Boyd, and E. Karimi, "High-dimensional quantum cloning and applications to quantum hacking," *Science advances*, vol. 3, no. 2, p. e1601915, 2017.

[122] A. Lohachab, A. Lohachab, and A. Jangra, "A comprehensive survey of prominent cryptographic aspects for securing communication in post-quantum iot networks," *Internet of Things*, vol. 9, p. 100174, 2020.

[123] T. Saito, K. Xagawa, and T. Yamakawa, "Tightly-secure key-encapsulation mechanism in the quantum random oracle model," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 2018, pp. 520–551.

[124] S. Zhang and D. Zhu, "Towards artificial intelligence enabled 6G: State of the art, challenges, and opportunities," *Computer Networks*, vol. 183, p. 107556, 2020.

[125] ENISA, "Artificial intelligence cybersecurity challenges," ENISA, Tech. Rep., December 2020.

[126] R. Shankar Siva Kumar, D. O. Brien, K. Albert, S. Viljöen, and J. Snover, "Failure Modes in Machine Learning Systems," *arXiv e-prints*, p. arXiv:1911.11034, Nov. 2019.

[127] M. S. Jere, T. Farnan, and F. Koushanfar, "A taxonomy of attacks on federated learning," *IEEE Security & Privacy*, no. 01, pp. 0–0, jan 5555.

[128] N. Khurana, S. Mittal, A. Piplai, and A. Joshi, "Preventing poisoning attacks on ai based threat intelligence systems," in *2019 IEEE 29th International Workshop on Machine Learning for Signal Processing (MLSP)*. IEEE, 2019, pp. 1–6.

[129] M. Pawlicki, M. Choraś, and R. Kozik, "Defending network intrusion detection systems against adversarial evasion attacks," *Future Generation Computer Systems*, 2020.

[130] H. Xiao, B. Biggio, G. Brown, G. Fumera, C. Eckert, and F. Roli, "Is feature selection secure against training data poisoning?" in *Proceedings of the 32nd International Conference on International Conference on Machine Learning - Volume 37*, ser. ICML'15. JMLR.org, 2015, p. 1689–1698.

[131] A. Kurakin, D. Boneh, F. Tramèr, I. Goodfellow, N. Papernot, and P. McDaniel, "Ensemble adversarial training: Attacks and defenses," 2018. [Online]. Available: https://openreview.net/pdf?id=rkZvSe-RZ

[132] M. Soll, T. Hinz, S. Magg, and S. Wermter, "Evaluating defensive distillation for defending text processing neural networks against adversarial examples," in *Artificial Neural Networks and Machine Learning – ICANN 2019: Image Processing*, I. V. Tetko, V. Kůrková, P. Karpov, and F. Theis, Eds. Cham: Springer International Publishing, 2019, pp. 685–696.

[133] W. Li, Z. Su, R. Li, K. Zhang, and Y. Wang, "Blockchain-based data security for artificial intelligence applications in 6G networks," *IEEE Network*, vol. 34, no. 6, pp. 31–37, 2020.

[134] A. Roy, A. Chhabra, C. A. Kamhoua, and P. Mohapatra, "A moving target defense against adversarial machine learning," in *Proceedings of the 4th ACM/IEEE Symposium on Edge Computing*, ser. SEC '19. New York, NY, USA: Association for Computing Machinery, 2019, p. 383–388. [Online]. Available: https://doi.org/10.1145/3318216.3363338

[135] S. Sengupta, T. Chakraborti, and S. Kambhampati, "Mtdeep: boosting the security of deep neural nets against adversarial attacks with moving target defense," in *International Conference on Decision and Game Theory for Security*. Springer, 2019, pp. 479–491.

[136] J. Liu, L. Chen, A. Miné, and J. Wang, "Input validation for neural networks via runtime local robustness verification," *CoRR*, vol. abs/2002.03339, 2020. [Online]. Available: https://arxiv.org/abs/2002.03339

[137] B. Li, C. Chen, W. Wang, and L. Carin, "Certified Adversarial Robustness with Additive Noise," *arXiv e-prints*, p. arXiv:1809.03113, Sep. 2018.

[138] J. Ma, R. Shrestha, J. Adelberg, C.-Y. Yeh, E. K. Zahed Hossain, J. M. Jornet, and D. M. Mittleman, "Security and eavesdropping in terahertz wireless links," *Nature*, vol. 563, no. 8, pp. 89–93, 2018.

[139] V. Petrov, D. Moltchanov, J. M. Jornet, and Y. Koucheryavy, "Exploiting multipath terahertz communications for physical layer security in beyond 5g networks," in *IEEE INFOCOM 2019 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 2019, pp. 865–872.

[140] M. M. U. Rahman, Q. H. Abbasi, N. Chopra, K. Qaraqe, and A. Alomainy, "Physical layer authentication in nano networks at terahertz frequencies for biomedical applications," *IEEE Access*, vol. 5, pp. 7808–7815, 2017.

[141] M. S. Saud, H. Chowdhury, and M. Katz, "Heterogeneous software-defined networks: Implementation of a hybrid radio-optical wireless network," in *2017 IEEE Wireless Communications and Networking Conference (WCNC)*, 2017, pp. 1–6.

[142] M. A. Arfaoui, M. D. Soltani, I. Tavakkolnia, A. Ghrayeb, M. Safari, C. M. Assi, and H. Haas, "Physical layer security for visible light communication systems: A survey," *IEEE Communications Surveys Tutorials*, vol. 22, no. 3, pp. 1887–1908, 2020.

[143] M. A. Arfaoui, A. Ghrayeb, and C. M. Assi, "Secrecy performance of the mimo vlc wiretap channel with randomly located eavesdropper," *IEEE Transactions on Wireless Communications*, vol. 19, no. 1, pp. 265–278, 2020.

[144] J. Chen and T. Shu, "Statistical modeling and analysis on the confidentiality of indoor VLC systems," *IEEE Transactions on Wireless Communications*, vol. 19, no. 7, pp. 4744–4757, 2020.

[145] S. Soderi, "Enhancing security in 6g visible light communications," in *2020 2nd 6G Wireless Summit (6G SUMMIT)*, 2020, pp. 1–5.

[146] Q. Wu and R. Zhang, "Intelligent reflecting surface enhanced wireless network via joint active and passive beamforming," *IEEE Transactions on Wireless Communications*, vol. 18, no. 11, pp. 5394–5409, 2019.

[147] M. Cui, G. Zhang, and R. Zhang, "Secure wireless communication via intelligent reflecting surface," *IEEE Wireless Communications Letters*, vol. 8, no. 5, pp. 1410–1414, 2019.

[148] Z. Ji, P. L. Yeoh, D. Zhang, G. Chen, Y. Zhang, Z. He, H. Yin, and Y. li, "Secret key generation for intelligent reflecting surface assisted wireless communication networks," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 1, pp. 1030–1034, 2021.

[149] T. Nakano, Y. Okaie, S. Kobayashi, T. Hara, Y. Hiraoka, and T. Haraguchi, "Methods and applications of mobile molecular communication," *Proceedings of the IEEE*, vol. 107, no. 7, pp. 1442–1456, 2019.

[150] F. Dressler and F. Kargl, "Towards security in nano-communication: Challenges and opportunities," *Nano Communication Networks*, vol. 3, no. 3, pp. 151 – 160, 2012.

[151] L. Mucchi, A. Martinelli, S. Jayousi, S. Caputo, and M. Pierobon, "Secrecy capacity and secure distance for diffusion-based molecular communication systems," *IEEE Access*, vol. 7, pp. 110 687–110 697, 2019.

[152] Y. Qu, L. Gao, T. H. Luan, Y. Xiang, S. Yu, B. Li, and G. Zheng, "Decentralized privacy using blockchain-enabled federated learning in fog computing," *IEEE Internet of Things Journal*, vol. 7, no. 6, pp. 5171–5183, 2020.

[153] C. Dwork, A. Roth *et al.*, "The algorithmic foundations of differential privacy." *Foundations and Trends in Theoretical Computer Science*, vol. 9, no. 3-4, pp. 211–407, 2014.

[154] S. Li, S. Zhao, G. Min, L. Qi, and G. Liu, "Lightweight privacy-preserving scheme using homomorphic encryption in industrial internet of things," *IEEE Internet of Things Journal*, 2021.

[155] T. Nguyen, N. Tran, L. Loven, J. Partala, M.-T. Kechadi, and S. Pirttikangas, "Privacy-aware blockchain innovation for 6g: Challenges and opportunities," in *2020 2nd 6G Wireless Summit (6G SUMMIT)*. IEEE, 2020, pp. 1–5.

[156] A. A. Abd EL-Latif, B. Abd-El-Atty, E. M. Abou-Nassar, and S. E. Venegas-Andraca, "Controlled alternate quantum walks based privacy preserving healthcare images in internet of things," *Optics & Laser Technology*, vol. 124, p. 105942, 2020.

[157] D. Dharminder and D. Mishra, "Lcppa: Lattice-based conditional privacy preserving authentication in vehicular communication," *Transactions on Emerging Telecommunications Technologies*, vol. 31, no. 2, p. e3810, 2020.

[158] Y. Du, M.-H. Hsieh, T. Liu, D. Tao, and N. Liu, "Quantum noise protects quantum classifiers against adversaries," *arXiv preprint arXiv:2003.09416*, 2020.

[159] M. Diaz, H. Wang, F. P. Calmon, and L. Sankar, "On the robustness of information-theoretic privacy measures and mechanisms," *IEEE Transactions on Information Theory*, vol. 66, no. 4, pp. 1949–1978, 2020.

[160] M. Bloch, O. Günlü, A. Yener, F. Oggier, H. V. Poor, L. Sankar, and R. F. Schaefer, "An overview of information-theoretic security and privacy: Metrics, limits and applications," *IEEE Journal on Selected Areas in Information Theory*, vol. 2, no. 1, pp. 5–22, 2021.

[161] ITU-T Focus Group on ML for Future Networks (FG-ML5G), "ITU FG ML5G - Unified architecture for machine learning in 5G and future networks," 2019. [Online]. Available: http://handle.itu.int/11.1002/pub/8128dfee-en

[162] ITU-T Focus Group on Technologies for Network 2030, "ITU FG-NET2030 – Network 2030 Architecture Framework," 2020. [Online]. Available: https://www.itu.int/en/ITU-T/focusgroups/net2030/Documents/Network_2030_Architecture-framework.pdf

[163] 3GPP Technical Specification Group Service and System Aspects (TSG SA) WG3 (SA3), "3GPP SA3 - Security." [Online]. Available: https://www.3gpp.org/specifications-groups/sa-plenary/sa3-security

[164] NIST, "NIST Post-Quantum Cryptography Standardization." [Online]. Available: https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization

[165] A. W. Montville and B. Munyan, "Security Automation and Continuous Monitoring (SACM) Architecture," Internet Engineering Task Force, Internet-Draft draft-ietf-sacm-arch-08, Mar. 2021, work in Progress. [Online]. Available: https://datatracker.ietf.org/doc/html/draft-ietf-sacm-arch-08

[166] "5G PPP Security Work Group." [Online]. Available: https://5g-ppp.eu/5g-ppp-work-groups/

[167] NGMN, "5G end-to-end architecture framework v4.31," Nov. 2020. [Online]. Available: https://sdgs.un.org/goals

[168] IEEE, "IEEE P1915.1 security in virtualized environments." [Online]. Available: https://site.ieee.org/p1915-1-sve/

[169] ——, "IEEE P1917 software defined networking and network function virtualization reliability." [Online]. Available: https://standards.ieee.org/project/1917_1.html

[170] ——, "IEEE P1913 software-defined quantum communication." [Online]. Available: https://standards.ieee.org/project/1913.html
[171] C. Gaber, J. S. Vilchez, G. Gür, M. Chopin, N. Perrot, J. L. Grimault, and J. P. Wary, "Liability-aware security management for 5g," in *2020 IEEE 3rd 5G World Forum (5GWF)*, 2020, pp. 133–138.
[172] 5GZORRO Project, "5GZORRO (Zero-touch security and trust for ubiquitous computing and connectivity in 5G networks) Project." [Online]. Available: https://www.5gzorro.eu/
[173] Hexa-X Project, "Hexa-X Project." [Online]. Available: https://hexa-x.eu/
[174] AI@EDGE Project, "AI@EDGE (A secure and reusable Artificial Intelligence platform for Edge computing in beyond 5G Networks) Project." [Online]. Available: https://cordis.europa.eu/project/id/101015922
[175] "Next G Alliance." [Online]. Available: https://www.nextgalliance.org/
[176] C. Castro, "Korea lays out plan to become the first country to launch 6G." [Online]. Available: https://www.6gworld.com/exclusives/korea-lays-out-plan-to-become-the-first-country-to-launch-6g/
[177] "6G/B5G Promotion Strategy." [Online]. Available: https://b5g.jp/en/

Pawani Porambage is a researcher at the Centre for Wireless Communications, University of Oulu, Finland. She obtained her B.Sc. Degree in Electronics and Telecommunication Engineering from University of Moratuwa, Sri Lanka in 2010, MSc. Degree in Ubiquitous Networking and Computer Networking from University of Nice Sophia-Anipolis, France in 2012, and Doctor of Technology in communication engineering from University of Oulu, Finland in 2018. She has over nine years of experience in network security domain and co-authored more than 50 publications. Her main research interests are network slicing, blockchain, lightweight security protocols, security and privacy on IoT, and AI/ML for security and privacy.

Gürkan Gür (Senior Member, IEEE) is a senior lecturer at Zurich University of Applied Sciences (ZHAW) – Institute of Applied Information Technology (InIT) in Winterthur, Switzerland. He received his B.S. degree in electrical engineering in 2001 and Ph.D. degree in computer engineering in 2013 from Bogazici University in Istanbul, Turkey. His research interests include Future Internet, 5G and Beyond networks, information security, and information-centric networking. He has two patents (one in US, one in TR) and published more than 80 academic works. He is a senior member of IEEE and a member of ACM.

Diana Pamela Moya Osorio (M'16) received the B.Sc. degree in electronics and telecommunications engineering from the Armed Forces University (ESPE), Sangolquí, Ecuador, in 2008, and the M.Sc. and D.Sc. degrees in electrical engineering with emphasis on telecommunications and telematics from the University of Campinas (UNICAMP), Campinas, Brazil, in 2011 and 2015, respectively. Since 2015, she has been acting as an Adjunct Professor with the Department of Electrical Engineering, Federal University of São Carlos (UFSCar), São Carlos, Brazil. In 2020, she joined the 6GFlagship Program at CWC, University of Oulu, as Senior Research Fellow. She also holds a research post as Postdoctoral Researcher for the Academy of Finland since 2020. She has served as TPC and reviewer for several journals and conferences. Her research interests include wireless communications in general, 5G and 6G networks, PHY security, UAV-based communications.

Madhusanka Liyanage (Senior Member, IEEE) received his B.Sc. degree (First Class Honours) in electronics and telecommunication engineering from the University of Moratuwa, Moratuwa, Sri Lanka, in 2009, the M.Eng. degree from the Asian Institute of Technology, Bangkok, Thailand, in 2011, the M.Sc. degree from the University of Nice Sophia Antipolis, Nice, France, in 2011, and the Doctor of Technology degree in communication engineering from the University of Oulu, Oulu, Finland, in 2016. From 2011 to 2012, he worked a Research Scientist at the I3S Laboratory and Inria, Shopia Antipolis, France. He is currently an assistant professor/Ad Astra Fellow at School of Computer Science, University College Dublin, Ireland. He is also acting as an adjunct Processor at the Center for Wireless Communications, University of Oulu, Finland. He was also a recipient of prestigious Marie Skłodowska-Curie Actions Individual Fellowship during 2018-2020. During 2015-2018, he has been a Visiting Research Fellow at the CSIRO, Australia, the Infolabs21, Lancaster University, U.K., Computer Science and Engineering, The University of New South Wales, Australia, School of IT, University of Sydney, Australia, LIP6, Sorbonne University, France and Computer Science and Engineering, The University of Oxford, U.K. He is also a senior member of IEEE. In 2020, he has received "2020 IEEE ComSoc Outstanding Young Researcher" award by IEEE ComSoc EMEA. Dr. Liyanage's research interests are 5G/6G, SDN, IoT, Blockchain, MEC, mobile and virtual network security. More info: www.madhusanka.com

Andrei Gurtov is a Professor of Computer Science at Linköping University, Sweden. Previously he was at University of Oulu (3 years) and Aalto University (6 years) and visiting the International Computer Science Institute at Berkeley multiple times. He received his M.Sc (2000) and Ph.D. (2004) degrees in Computer Science from the University of Helsinki, Finland. Prof. Gurtov co-authored over 200 publications, including 4 books, 5 IETF RFCs, 6 patents, over 60 journal and 110 conference articles. He supervised 15 PhD theses.

Professor Gurtov's research interests are in network protocols, security of vehicular, airborne, industrial systems, mobile, wireless and IoT networks, SmartGrids. He is an ACM Distinguished Scientist, IEEE ComSoc Distinguished Lecturer (2016-19) and Vice-chair of IEEE Sweden section. He received best paper awards at IEEE CSCN'17 and IEEE Globecom'11, was co-adviser of the best Doctoral Thesis in CS in Finland in 2017. He had served on numerous journal editorial boards and conference program committees, including IEEE Internet of Things journal, MDPI Sensors, IEEE ICNP, ACM MSWiM, and IFIP Networking. URL: http://gurtov.com

Mika Ylianttila (M. Sc, Dr.Sc, eMBA) is a full-time associate professor (tenure track) at the Centre for Wireless Communications - Networks and Systems research unit, at the Faculty of Information Technology and Electrical Engineering (ITEE), University of Oulu, Finland. He is the director of Communications Engineering Doctoral Degree Program and he leads NSOFT (Network security and softwarization) research group which studies and develops secure, scalable and resource-efficient techniques for 5G and beyond 5G and IoT systems. He has co-authored more than 200 international peer-reviewed articles. He is a Senior Member of IEEE and associate editor in IEEE Transactions on Information Forensics and Security.