Beyond Fragmented Standards: A Comprehensive Survey of Security and Privacy in 6G and Future Communication Networks

Bidushi Barua, Ahsan Khan, Kangfeng Ye, Panagiotis Papanastasiou, Yifan Liu, Mohit Bidikar, Anthony Moulds, Julie McCann and Poonam Yadav

***Abstract*—This paper presents a comprehensive survey of security and privacy challenges in Sixth-Generation (6G) and future communication networks; moving beyond fragmented standards and technology-specific studies to deliver a cross-layer analysis of evolving threats and countermeasures. Unlike previous generations, 6G will integrate diverse enabling technologies such as Reconfigurable Intelligent Surfaces (RIS), Joint Sensing and Communication (JSAC), Non-Terrestrial Networks (NTN), and AI-native architectures, significantly expanding the attack surface of communication networks. We examine vulnerabilities due to new enabling technologies, new architectural features, and new applications which are expected in 6G networks, and highlight risks including adversarial machine learning, software supply-chain attacks, privacy breaches, and quantum-era threats. By synthesizing insights from cutting-edge research literature and standardization/pre-standardization bodies such as 3GPP, ETSI, ITU, IETF, O-RAN Alliance, AI-RAN Alliance, we develop a unified threat taxonomy and map emerging solutions, including zero-trust frameworks, blockchain-based authentication, quantum-safe cryptography, and privacy-preserving edge intelligence. This survey offers researchers and practitioners a holistic foundation for designing secure-by-design, resilient 6G architectures that address interdependent, multi-layer risks in future hyper-connected ecosystems.**

***Index Terms*—6G Networks, Security, Privacy, Future Communication Networks, Standards**

I. Introduction

SINCE the inception of wireless communications, each generational shift from 1st Generation (1G) to 5th Generation (5G) has led to major transformations in the interaction paradigm between people, devices, and systems. 1G networks enabled analogue voice transmission; 2nd Generation (2G) networks introduced digital voice and short message service (SMS); 3rd Generation (3G) networks brought mobile internet; and 4th Generation (4G) networks delivered broadband-grade connectivity for streaming and cloud applications [1]. The advent of 5G networks around 2020, with its Enhanced Mobile Broadband (eMBB), Ultra-Reliable and Low Latency Communication (URLLC), and Massive Machine-Type Communications (mMTC) capabilities, marked the onset of hyper-connectivity [2]. As 5G matures globally, the focus shifts from connecting people to connecting everything, setting the stage for 6th Generation (6G) networks which are expected to represent a transition from connected things to connected intelligence [3].

This work is supported by EPSRC and DSIT funded project - CHEDDAR: Communications Hub For Empowering Distributed Cloud Computing Applications And Research (EP/X040518/1), (EP/Y037421/1) and EPSRC funded project REMOTE (EP/Y019229/1). This manuscript benefited from the use of generative AI tools (e.g., ChatGPT by OpenAI) for language refinement. All content was critically reviewed and verified by the authors.

However, as digital ecosystems expand, 5G falls short of supporting applications with demanding Key Performance Indicators (KPIs) such as sub-millisecond latency, ultra-reliability, and pervasive intelligence. Emerging paradigms such as extended reality (XR), digital twins, tactile internet, autonomous vehicles, real-time Brain Computer Interfaces (BCI), and Internet of Everything (IoE) require not only higher data rates and lower latency but also stronger synchronization, reliability, and contextual awareness [2, 1, 3]. The convergence of communication, sensing, and computation at the network edge further demands adaptive, self-governing systems with minimal human intervention.

To meet these requirements, 6G is envisioned as an Artificial Intelligence (AI)-native, integrated communication and sensing infrastructure, which is expected to deliver a tenfold improvement in KPIs over 5G. According to International Telecommunication Union (ITU) and initiatives such as Hexa-X, KPI targets include up to 1 Tbps peak data rates, sub-100 ţs latency, 99.99999% reliability, over 10^7 devices/km^2 density, and 10100Œ energy efficiency gains [4, 5]. Therefore, the realization of these goals demand not just an architectural redesign but a fundamental rethink of how security and privacy features are embedded into the new network fabric [2].

Distinct from prior generations, 6G will integrate technologies such as Reconfigurable Intelligent Surface (RIS), Joint Communications and Sensing (JCAS), Massive Multiple-Input Multiple-Output (mMIMO), and Non-Terrestrial Networks (NTN) [3, 6], which collectively are expected to expand the attack surface of communication networks. RIS will introduce programmable-surface spoofing and eavesdropping risks; JCAS will enable side-channel attacks through environmental inference [7]; and ultra-high-frequency (Terahertz Communication (THz), sub-THz) bands will expose beamforming to hijacking and Denial-of-Service (DoS) attacks. High-mobility NTN, including Unmanned Aerial Vehicles (UAVs) and LEO satellites, will complicate trust establishment and secure handovers [8, 9].

Architecturally, 6G will rely on decentralized and softwarized frameworks such as Open Radio Access Network (O-RAN) and Zero Trust Architecture (ZTA) [10, 11], that will enhance flexibility, but at the expense of amplifying of exposure to supply-chain compromises, insider threats, and policy misalignment. The pervasive use of AI/Machine Learning (ML) for orchestration and threat detection will introduce new risks such as Adversarial Machine Learning (AML), poisoning, and inversion attacks. The absence of standardized security-by-design principles further will increase susceptibility to coordinated, multi-layer intrusions that could

erode trust and resilience in mission-critical sectors.

While extensive research exists on individual aspects of 6G security, ranging from physical-layer defenses and blockchain access control to post-quantum cryptography, most efforts remain fragmented or narrowly scoped. Few studies offer a unified view across the 6G protocol stack, spanning enabling technologies, architectures, and application-layer vulnerabilities. Given the inter-dependencies introduced by AI-native control, integrated sensing, and decentralized trust, there is an urgent need for a cross-layer, system-level understanding of the 6G security-privacy continuum. This paper, presents a holistic survey that synthesizes these perspectives, developing a comprehensive threat taxonomy, mapping emerging countermeasures, and clearly identifying future research challenges for secure and resilient 6G ecosystems.

A. Paper Structure

The rest of the paper is organized as follows. Section II presents other related works in the area of security and privacy in 6G networks, and Section III explores the transition of security architectures in 5G toward integrated security and privacy frameworks in 6G networks. Within Section III, the security and privacy-related framework of current 5G networks, the vulnerabilities existing in current and evolving 5G networks, are elaborately discussed, followed by the vision of 6G networks, the potential 6G security architecture and the unique security and privacy challenges that are expected to arise in them. This is followed by Section IV, where the ongoing standardization activities in the area of 6G security and privacy, are presented. In Section V, the threat landscape, considering the security attacks and requirements of each enabling technology that will be prevalent in 6G, is elaborated. Then, a description of a few recent, key technical solutions to counteract or prevent the security and privacy attacks discussed in the previous section, are presented in Section VI. Finally, we have the conclusion in Section VII.

II. Related Work

As 6G systems promise hyper-connectivity, ultra-low latency, and context-aware intelligence, ensuring robust security in these networks has become a core research priority. A growing body of survey literature has attempted to anticipate emerging threats and propose early-stage defenses. These studies range from broad overviews of 6G architecture to detailed analysis of specific technologies, but they often lack a unified view that captures the complex and multi-faceted nature of 6G. In this section, we structure the existing works into thematic clusters, analyze their contributions, and identify key gaps that motivate our work on unified, cross-layer security and privacy taxonomy, and their potential counter solutions for 6G networks. As summarized in Table I, existing survey articles either focus on individual technologies or specific threat domains but fail to provide an integrated taxonomy for 6G security and privacy challenges.

A. 6G Security Landscape and Standardization

Several recent surveys aim to lay the foundation for securing future 6G systems by offering high-level taxonomies and standardization blueprints. Yang et al. [2] propose a roadmap that incorporates architectural enablers such as ZTA, Software-Defined Networking (SDN), and Network Function Virtualization (NFV), promoting security-by-design and privacy-by-design principles. Similarly, Nguyen et al. [1] discuss the intersection of 6G enablers with emerging risks such as eavesdropping, poisoning, and spoofing, offering a layered view but without granular threat mapping or system-level taxonomy. The authors of [12] present a survey on threats faced by AI agents. In [13], NVIDIA presents confidential computing solutions that protect data in transit, at rest and in use, throughout their life cycle from unauthorized entities. Ahmad et al. [14] and Abdel-Hamid et al. [15] extend the scope to Beyond 5G (B5G) technologies but primarily focus on 5G-era risks, offering limited insights into evolving 6G paradigms such as semantic intelligence, RIS, and cross-layer orchestration.

B. Enabler-Specific Security Reviews

RIS-focused studies, such as Naeem et al. [16], discuss how programmable metasurfaces introduce new attack vectors, including reflection manipulation and signal spoofing. However, the analysis remains confined to hardware-level threats. Similarly, Kim et al. [17] analyze the role of Federated Learning (FL) and blockchain in Vehicle-to-Everything Communication (V2X) systems, yet the findings are domain-specific and not generalized across other 6G enablers. In the context of O-RAN, Porambage et al. [18] highlight threats such as rogue xApps and RAN Intelligent Controller (RIC) vulnerabilities, proposing ZTA and AI-based defenses. Meanwhile, Dardari et al. [19] survey NTN with a focus on architectural and mobility challenges, though lacking depth in security mechanisms such as secure handover, privacy preservation, or zero-trust enforcement.

C. Edge Intelligence and Federated Learning

Federated and decentralized learning have emerged as key paradigms for privacy-aware intelligence in 6G. Ferrag et al. [20] and Mao et al. [21] delve into security threats at the edge, including data poisoning, backdoor attacks, and identity spoofing. While they provide technical depth for edge learning, they omit broader enabler interactions or system-level orchestration. Nguyen et al. [22] offer a detailed survey of FL in Internet of Things (IoT), outlining defense mechanisms like differential privacy and blockchain, yet overlook how FL integrates with RIS or semantic layers. Tassi et al. [23] focus on Decentralized Federated Learning (DFL), emphasizing its scalability and resilience but without contextualizing its role in multi-domain 6G settings.

D. Application-Domain Surveys

Security concerns in vertical domains such as vehicular networks are captured in domain-specific surveys. Sumra et

TABLE I: Comparative Analysis of Existing Literature on 6G Security: Focus Areas, Technological Enablers, Threat Domains, and Key Limitations

Ref	Focus Area	Enablers Covered	Threat Domains	Limitations
[2]	Standardization and 6G security threats	RIS, THz, ML, AI-native infra	General threat types, trust models, DoS, spoofing	Lacks taxonomy, no detailed treatment of application-layer security
[1]	Prospective 6G technologies and associated risks	RIS, THz, AI/ML, Blockchain	Spoofing, poisoning, eavesdropping, trust models	No application-layer security, lacks taxonomy and integrated defense framework
[14]	Security overview for 5G and beyond	Network slicing, SDN, NFV, blockchain	Eavesdropping, jamming, rogue slicing, side-channel attacks	5G-centric; lacks detailed 6G enabler analysis and forward-looking security models
[15]	Security in B5G and 6G communication networks	UAVs, THz, RIS, blockchain	Privacy leakage, spoofing, data integrity, authentication threats	Lacks structured taxonomy and defense mapping; generalist perspective
[16]	Security and privacy for RIS in 6G	RIS (reflection control, deployment)	Eavesdropping, spoofing, signal manipulation	Narrow focus on RIS; lacks integration with broader 6G architecture or enabler inter-dependencies
[17]	FL and blockchain-based security in 6G V2X	FL, blockchain, V2X, edge AI	Model poisoning, Sybil attacks, data tampering	Focused on V2X; lacks generalizability across other 6G use cases or layers
[18]	Security, privacy, and trust in O-RAN for 6G	RIC, ZTA, AI anomaly detection, blockchain	Rogue xApps, data leakage, interface tampering	Focused on O-RAN; lacks integration with other 6G domains and cross-layer threats
[19]	Enabling technologies and challenges in 6G NTNs	Satellites, UAVs, HAPS, RIS	Handover failures, dynamic spectrum risks, latency threats	Lacks focus on E2E security, privacy-preserving methods, and zero-trust integration
[20]	Edge learning security for 6G-enabled IoT	Federated Learning, Edge AI	Data poisoning, backdoors, adversarial examples, privacy leakage	Focuses only on IoT edge learning; lacks broader enabler and architectural security coverage
[21]	Security and privacy at 6G network edge	Edge computing, zero-trust, immersive services	Identity spoofing, inference leakage, access control, trust models	Lacks system-wide threat taxonomy and enabler diversity (e.g., RIS, JCAS)
[22]	FL integration in IoT with privacy/security focus	FL, blockchain, differential privacy	Poisoning, inference, model manipulation	Focused on IoT-FL; lacks integration with broader 6G enablers and cross-layer security view
[23]	Decentralized federated learning	DFL, peer collaboration, FL over edge	Poisoning, Sybil attacks, unstable convergence	Strong DFL focus; lacks broader 6G enabler context and system-level integration
[24]	Security review for V2X in VANETs	VANETs, V2V, V2I, encryption, trust models	Sybil attacks, message falsification, DoS, privacy leakage	Limited to VANETs; lacks alignment with 6G enablers and future-proof models
[25]	RL-based physical and cross-layer security in 6G	RIS, THz, RL, edge AI	Jamming, spoofing, eavesdropping	Focused on RL methods; lacks broad threat taxonomy and architectural-level security analysis
[26]	Role of physical layer security in 6G	PLS, AN injection, beamforming, secure CSI	Eavesdropping, jamming, spoofing	Strong PHY focus; lacks cross-layer integration and AI-driven adaptability
[27]	Security of network slicing in 5G/6G	AI-based slice monitoring, blockchain, secure orchestration	Slice hijacking, isolation failure, rogue slice	Focused on slicing; lacks integration with other 6G enablers and holistic architecture
[28]	AI convergence with 6G communication networks	Semantic comm., beamforming, threat detection	AI-based attacks, lack of transparency, adversarial examples	Focused on AI integration; lacks detailed privacy models and threat taxonomy
This work	Comprehensive threat taxonomy across 6G enabling technologies and countermeasures	6G enabling technologies (RIS, THz, NTN, JCAS etc.) and applications (e.g., V2X)	Potential threats in all layers of the 6G network	

al. [24] review security issues in Vehicular Adhoc Network (VANET)-based V2X systems, detailing attack taxonomies and countermeasures. However, their scope is confined to VANETs, lacking alignment with 6G-specific enablers such as edge AI or RIS. Kim et al. [17] offer another V2X-focused survey with FL and blockchain integration but similarly miss broader architectural mapping.

E. Cross-Layer and AI-Converged Security

Advanced 6G paradigms demand AI-native, cross-layer security frameworks. Alazab et al. [25] explore how Reinforcement Learning (RL) enhances security across physical and network layers but focus on algorithmic efficacy rather than architectural breadth. Bassem et al. [26] advocate for Physical Layer Security (PLS) using techniques like artificial noise injection and secure beamforming. However, they do not address integration with higher-layer enablers. Rimal et al. [27] tackle network slicing security but miss interdependencies with semantic or RIS-based systems. Similarly, the work by Akhtar et al. [28] emphasizes the AI-6G convergence for threat detection and intelligent beamforming but lacks depth in privacy-aware intelligence or federated optimization.

F. Identified Gap and Our Contribution

Across these diverse contributions, a common limitation is the absence of a unified, enabler-integrated, and cross-layer taxonomy that reflects the full complexity of 6G networks. While individual threats and defenses are explored in silos, few works holistically map vulnerabilities from the physical layer to semantic and application layers, while also addressing the interplay among federated learning, blockchain, RIS, ZTA, and NTN. Our work fills this gap by synthesizing a comprehensive threat taxonomy, classifying layered and cross-enabler vulnerabilities, and aligning them with emerging countermeasures, thereby laying the groundwork for secure-by-design 6G architectures. The large collection of resources, based on which this threat landscape is presented in this survey, is not limited to containing only research-motivated papers on this topic but also publications and reports submitted by several standardization bodies on security and privacy in 6G networks. This aims to offer a more realistic outlook for researchers and industry to potentially inspire major advancements in 6G security and privacy solutions.

III. Evolution from 5G to 6G Security Architectures

To support the future 6G vision, it is necessary to consider the existing 5G security frameworks, recognize the security and privacy vulnerabilities in 5G networks and therefore, identify the significant novel features that are necessary to be incorporated to make 6G networks resilient and secure. In this section, we discuss the current 5G security framework (Subsection III-A), the existing vulnerabilities in them (Subsection III-B), the vision of 6G networks (Subsection III-C), followed by the potential 6G security architecture design and the unique security challenges that will accompany 6G networks (Subsection III-D).

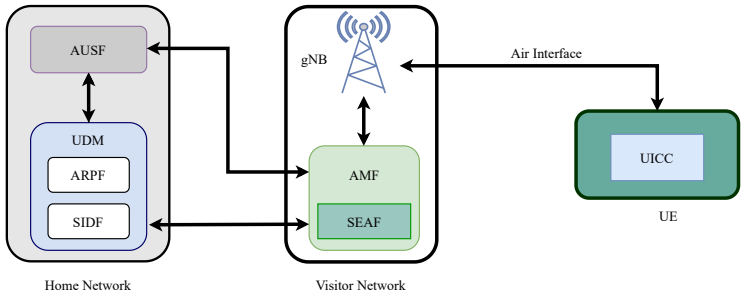

Figure 1: 5G security architecture: network entities and their interactions across user, access, and core domains.

A. Current 5G Security Framework

In this section, the 5G security architecture and 5G security access and authentication procedures are reviewed.

1) The Network Architecture for Security: Here, we look at the components involved in security provision within the 5G network and their roles in achieving authentication and access for security provisions. The User Equipments (UEs), the core of the Home Network (HN) and the core of visiting networks are mainly the nodes interacting for security in 5G networks. The radio access network comprises of base stations which are called Next Generation Node Bs (gNBs) that communicates with the UEs. The following elaborates on the functions within the UE or Core Network that facilitate the authentication and access procedures (as illustrated by Figure 1).

(a) User Equipment (UE): The UE contains the physical smart card that is represented by a platform called Universal Integrated Circuit Card (UICC) that is capable of running multiple applications. One of the main applications is the Universal Subscriber Identity Module (USIM), which contains all the information related to the user's identity, authentication keys, and subscriber network.

(b) Visitor Network Core Network Within the Core of the visiting network of the subscriber, are two important functional components:

(i) Access and Mobility Management Function (AMF) which contains all the access management information of the subscriber in the Visiting network. Some of the access management information are management information regarding cryptographic keys and mobility. The UE connects to the AMF through the Radio Access Network (RAN) via the air interface.

(ii) Security Anchor Function (SEAF) which manages the authentication procedures of the Visiting Network

(c) Home Network Core Network: The HN has four main nodes for carrying out security-related functions.

(i) Unified Data Management (UDM): UDM contains the subscriber database. The AMF and UDM work closely together.

(ii) Authentication Credential Repository and Processing Function (ARPF): ARPF stores important security keys and performs calculations involving security.

(iii) Subscription Identifier De-concealing Function (SIDF): SIDF is responsible de-concealing the identity of the UE.

(iv) Authentication Server Function (AUSF): AUSF manages authentication.

2) 5G Security Model: 5G networks presented architecture and authentication protocols that satisfied a service-oriented network model. As per 3rd Generation Partnership Project (3GPP) standards [29], the security architecture of 5G networks is based on (a) two-party trust model, (b) independent security domains, (c) the three strata in which these domains operate and (d) transmission security mechanisms across these domains and strata (as shown in Figure 2), which are elaborated in the next subsections.

(a) Two-party Trust: The 5G security architecture relies on a two-party trust model between stakeholders. In this model, the UE and its home operator mutually authenticate using a pre-provisioned longterm secret key, establishing the root of trust. Upon successful authentication, a hierarchy of intermediate keys are derived from that root key to secure signaling and data transports for confidentiality and integrity.

Similar two-party trust principles apply to other relationships in 5G networks: between UE and service providers, between multiple service providers, and between devices and the network. Each pairing essentially forms its two-party trusted link, underpinning all 5G service interactions. Each partner derives and uses keys rooted in the shared credential, forming the basis for secure authentication and data protection across the ecosystem [30].

(b) 5G Security Domains: The 5G Security architecture comprises of six independent domains [30, 31] and they are described below.

(i) 5G Network Access Security: These are a set of security features based on 3GPP Release 15 and 16 standards that enables the UE to authenticate and access the services via the network securely in addition to providing protection from attacks on the radio interfaces. The access includes both 3GPP and trusted non-3GPP access. These features also includes security context delivery from Serving Network (SN) to UE for access security.

(ii) 5G Network Domain Security: A set of security features between network functions within the same operator that enables nodes to securely exchange signaling data and user plane data.

(iii) 5G User Domain Security: Security features that secure the user access to UE.

(iv) 5G Application Domain Security: These security features enable applications in provider and user domains to securely exchange messages.

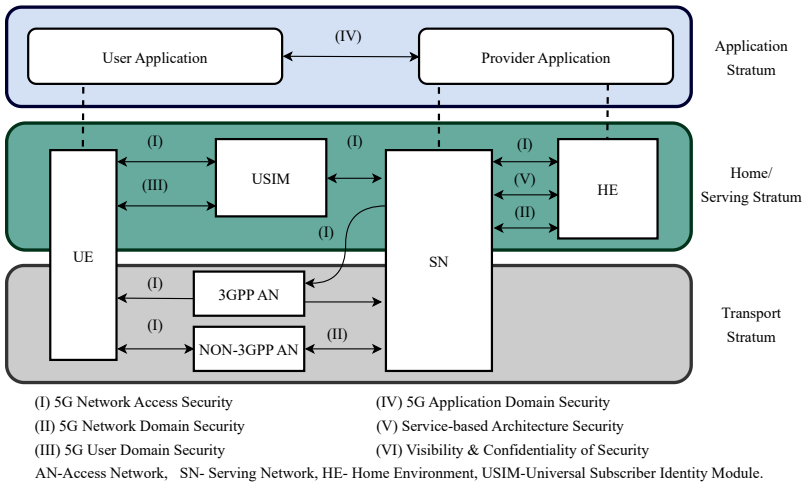

Figure 2: Layered structure of 5G security architecture across transport, serving, home, and application strata.

(v) Service-based Domain Security: This domain was added in 5G and is related Service-based Architecture (SBA) [32]. This set of security features enable network element registration, aspects of discovery and authorization security and responsible for the protection of service-based interfaces.

(vi) Visibility and confidentiality of security: This set of security features enables the user to be informed of the security feature in operation. [19]

(c) 5G Security Strata: The 5G Security architecture comprises three strata [30] which are described below.

Transport stratum: This stratum, with low security sensitivity, is located at the bottom of the architecture. It includes some UE functions, all gNodeB functions, and some core network functions, such as the User Plane Function (UPF). These functions, excluding the UE functions, do not involve sensitive data, such as Subscription Permanent Identifiers (SUPIs) and user root keys. They manage only low-level keys in the key hierarchy, for example, user access keys. Low-level keys can be derived, replaced, or updated by a high-level key at the home/serving stratum. However, a low-level key cannot induce a high-level key.

Serving stratum: This stratum includes the core network functions of the operator's HN such as the AMF, Network Repository Function (NRF), Security Edge Protection Proxy (SEPP), and Network Exposure Function (NEF). It has higher security sensitivity as compared to the transport stratum. The core network functions of this stratum manage only mid-level derived keys in the key hierarchy. A mid-level key can be derived, replaced, or updated by a high-level key at the home stratum. However, a mid-level key cannot induce a high-level key.

Home stratum: This stratum with high security sensitivity includes the AUSF and UDM of the operator's HN, as well as the USIM in the UE. It contains sensitive data such as the SUPIs, user root keys, and high-level keys.

Application stratum: This stratum is closely related to service providers, but hardly related to operator networks. The application stratum involves 5G applications that need end-to-end security assurance for high security and transport security requirements.

(d) Authentication Framework Robust authentication protocols are necessary in a network for legitimate users to have seamless access to the network and for unauthorized users to be denied any access. 3GPP defined two 5G authentication mechanisms -primary and secondary. Primary authentication is specified for mutual authentication of the UE and the network. 5G Authentication and Key Agreement (5G AKA) protocol is used for this authentication and is used to verify the device's authenticity when it connects to a network. Secondary authentication in the form of Extensible Authentication Protocols (EAPs) are applicable when a device connects to a service on the Internet via a 5G network. 5G introduced a common authentication platform for both 3GPP and non-3GPP access networks. With a unified platform, 5G enables one authentication execution, in which a UE can be authenticated in a 3GPP access network, and then move to other non-3GPP networks without the need for re-authentication. To provide better protection of identities of UEs, 5G used an encrypted version of SUPI called Subscription Concealed Identifier (SUCI) to conceal the subscriber's real information during the authentication process. This prevented sending of IMSI in plain text over 5G networks. 5G also enabled authentication protocols EAP-AKA, EAP-TLS for non-USIM devices to access 5G network services [1].

(e) 5G Transmission Security Mechanism Within the Network Access domain, the UEs access the 5G network through the Access network via Access Stratum (AS) and Non-Access Stratum (NAS) signaling. The protection of the AS signaling, which is used for radio interface and communication between the UE and the RAN, is achieved by using keys in the lowest layer of 5G key hierarchy and one of three cryptographic algorithms -AES, Snow 3G or ZUC. The security of NAS, which is signaling between the UE and Core Network, is ensured by using NAS keys and one of the same cryptographic algorithms as mentioned above [30].

(f) 5G Key Exchanges In both the authentication protocols 5G AKA and EAP AKA, key exchanges take place. For a UE initializing its access to the network, it shares its secret key

stored in its USIM, which needs to match with the shared secret key stored in the UDM of the core network during the initial duration of the connection. The UE then sends its SUPI concealed as SUCI to the network. Once the device is verified and admitted to the network, keys are derived to secure it within the network, and finally, a master session root key Key [from] Authentication Server Function (KAUSF) is generated. The duration and updating of these exchanged keys are crucial for maintaining confidentiality. For instance, 3GPP TS33.501 specifies that if a UE connects to the base station for a prolonged period of time, then the keys are exchanged every 24 hours or less based on the operator's preference.

B. Gaps and Limitations of 5G Security

In this subsection, the vulnerabilities concerning security and privacy in 5G networks are discussed. By considering and analyzing of these threats and risks in current networks, secured and robust 6G networks can be designed for the future. Some of these threats are,

(a) SDN/NFV threats: SDN related software attacks can include critical APIs getting exposed to unintended software, and centralized network control and inception of OpenFlow can make the network susceptible to Distributed Denial-of-Service (DDoS) attacks [33, 34]. Moreover, overloading of this software-controlled system can cause the entire network to break down. The integration of NFV to 5G networks increases the vulnerability of host systems of Virtualized network functions by exposing the related hypervisors to attackers. Such exposure through misconfiguration can result in risking the security of the entire core network. This could possibly lead to malware having access to information from other network users and unauthorized API calls. Cross-contamination of shared resources is another possible threat [31].

(b) User Privacy threats: In 5G AKA protocol, the agreement between the subscribers and network suffers from integrity vulnerabilities due to the lack of a binding assumption of channel between the SN and HN, which in turn can lead to an attacker's ability to access the network at the cost of transferring the bill to another subscriber. Moreover, user tracking by observation of synchronization failure messages over time can act as a major user privacy threat [1, 31]. A harmless service like paging can be exploited to locate a user with fewer than 10 calls [35]. A rogue base station can fool a UE into disclosing its SUPI by spoofing a pre-authentication message [36]. Moreover, although 5G-AKA offers privacy preservation against passive attackers, it is vulnerable to linkability attacks due to active attackers [37], and a potential fix would require designing a countermeasure in a standard compatible manner, which makes it more challenging.

(c) Security risks due to 5G deployments: 5G operations needed either a Stand-alone (SA) or a Non-Standalone (NSA) deployment of base stations. SA deployed networks although have the benefit of native security , supporting a transition procedure would create potential security risks. On the other hand, to support NSA, dual connectivity with 4G-LTE and 5G-NR would require dual authentication but the optional use of confidentiality protection might make the system potentially vulnerable to attacks [1].

(d) 5G O-RAN threats: RAN and core are both critical components of 5G networks because gNBs (5G base stations) terminate the encryption of user data, except when it is encrypted externally and is beyond the control of an operators 5G network. As a result of this, gNBs have full access to all data to and from devices in clear text. Moreover, technical developments and initiatives, such as distributed RAN, split RAN, O-RAN and Common Public Radio Interface (CPRI)/eCPRI consortiums, further fragment and distribute the deployment of RAN functions, with serious security implications. For instance, all the options make it unclear how functions will be distributed and co-located in the long run. There is a risk that market demands will drive the most cost-effective function distribution, not necessarily the most secure one [38].

(e) Threats due to 5G Network slicing: Network slicing has transformed the way the telecom industry views the network from network-as-an-infrastructure to network-as-a-service. However, slicing brings in weaknesses in terms of security. Integration of AI and ML into network slicing leads to adversarial machine attacks where the adversaries add data samples with disrupting factors to misguide the ML model, leading to the appearance of vulnerabilities that were not originally present. Therefore, it becomes necessary to train these ML models keeping adversarial methods in mind to create a more secure environment [31].

(f) Threats due to 5G MIMO: 5G MIMO security research findings have shown that the probability of detection of an eavesdropper in a network is higher with a higher number of base station antennas [39]. However, some of the threats in 5G Multiple-Input Multiple-Output (MIMO) are that (1) the security algorithms defined for 5G MIMO produce a large amount of noise in the absence of sufficient spatial redundancy, (2) eavesdroppers can invade the privacy of users with poor connections, and (3) the currently measurable indicators for MIMO security algorithms do not match up to the theoretical values [31].

(g) Cloud computing related threats: Cloud computing has appeared as an intellectual paradigm that allows computing resources on a pay-per-use way, while these resources are dynamically configured to manage different workload needs. This is due to the virtualization technology, which provides the creation of multiple VMs that share the same physical resources. Although could computing provides several benefits for 5G networks, the cloud possess several challenges in security and privacy aspects of the network. Some of the key security vulnerabilities related to cloud computing are (a) Network-related attacks such as XML signature (wrapping attack), flooding attacks etc., (b) Virtualization and hypervisor vulnerabilities, (c) identity and access management related threats, (d) data and storage security attacks [40].

(h) Critical infrastructure threats: The security of critical mobile infrastructures is increasingly challenging in 5G networks due to the presence of Advanced Persistent Threats (APTs) [41] that aim to achieve data exfiltration, unauthorized access and control in the network. The well-funded, sophisticated attackers in APT moves laterally after establishing a beachhead in the network through misconfigurations,

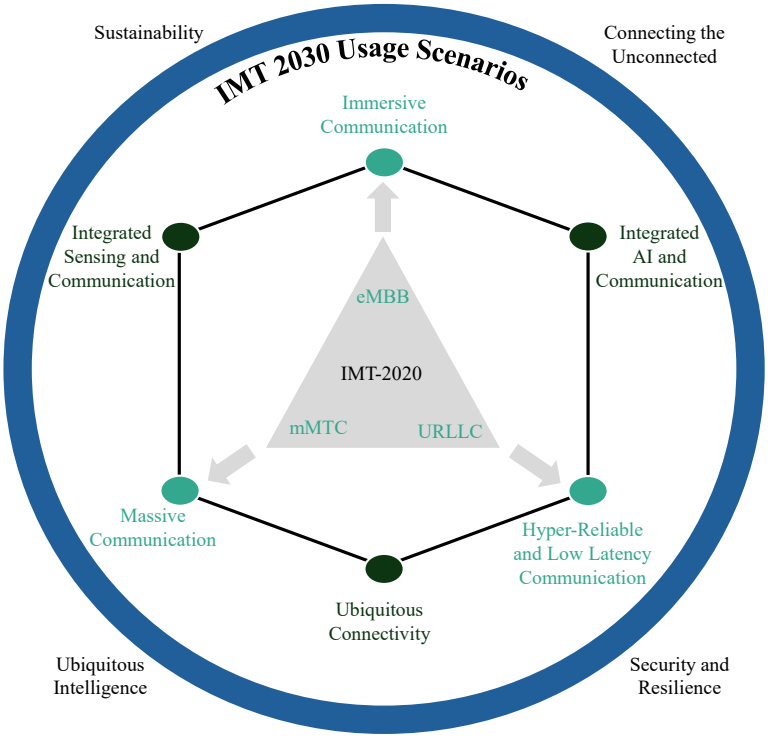

Figure 3: IMT-2030 framework outlining six representative 6G usage scenarios and four overarching design aspects, as proposed by ITU-R to guide global 6G development [5].

vulnerabilities and compromised credentials. The main security challenge in dealing with APTs lie in preventing an external threat from penetrating into a secure perimeter and becoming an internal threat that can move laterally through the network. This challenge gets worse due to the presence of multi-stakeholder deployments, which create unassigned and variable postures and responsibilities in the network [42]. In the next subsection, we explore how the future 6G networks are envisioned and the general features these networks will potentially encapsulate.

C. Definition and Vision of 6G

The 6G technology is driven by the convergence of several advanced enabling technologies that will potentially push the boundaries of speed, intelligence, sensing and connectivity in networks. Among several popular research initiatives that have been undertaken for shaping and developing this technology, the key standard development organizations and research projects are International Mobile Telecommunications 2030 (IMT-2030) by the International Telecommunication Union Radiocommunication Sector (ITU-R) [5], 6G Smart Networks and Services Industry Association (6G-IA) [43] by European Industry and Research, North America's Next G Alliance (NGA) [44], European Union's flagship Hexa-X project [45]. Driven by key stakeholders worldwide, a unified vision and global consensus on 6G are expected to emerge, leading to its commercial launch around 2030. Some of the main objectives and requirements of 6G technologies as defined by these standards are to deliver systems with ultra-high data rates, ultra-low latencies, ultra-reliability, large-scale and ultra-dense connectivity, highly improved energy efficiency [5], immersive communication, sustainability [1], seamless integration of non-terrestrial networks [46] and sensing [47] into the communication network, and fusion of the digital, physical and human world through combination of intelligent and innovative technologies [48]. Figure 3 illustrates some of the IMT-2030 6G use case scenarios and overarching aspects by ITU-R.

In 5G, the three main usage scenarios which were identified based on user demands were eMBB, URLLC and mMTC with goals of increased capacity, reduced latency, enhanced reliability, higher throughput, reduced cost and enhanced connectivity and diversified services to verticals such as manufacturing, healthcare and transportation. To support these trends, new enabling technologies such as network slicing, O-RAN and mMIMO emerged along with remarkable innovations in the areas of virtual and augmented reality (VR/AR), the IoT, and AI. However, deploying communication-centric 5G technology in some verticals that support complex operations and legacy systems has been challenging from an economic and environmental perspective. 5G technologies supported individual services like digital healthcare and wearable technology, but 6G will enable and benefit a wider range of vertical industries such as Intelligent Transport System, Zero-Power Communications [30]. Due to the wide variety of applications, 5G networks face the challenge of satisfying dramatically increased service heterogeneity and diversity under stringent resource constraints [49]. Therefore, 6G networks are expected

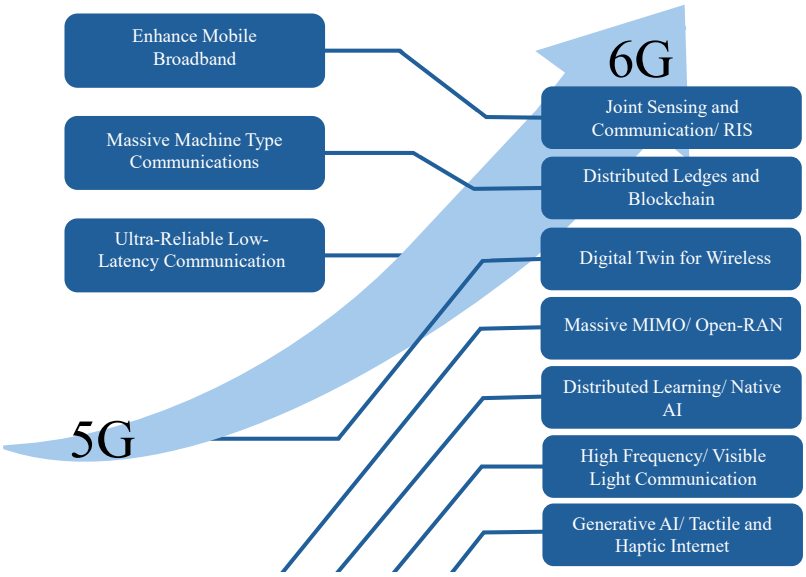

Figure 4: Paradigm shift from communication-centric 5G systems to AI-native, context-aware, and sensing-integrated 6G networks.

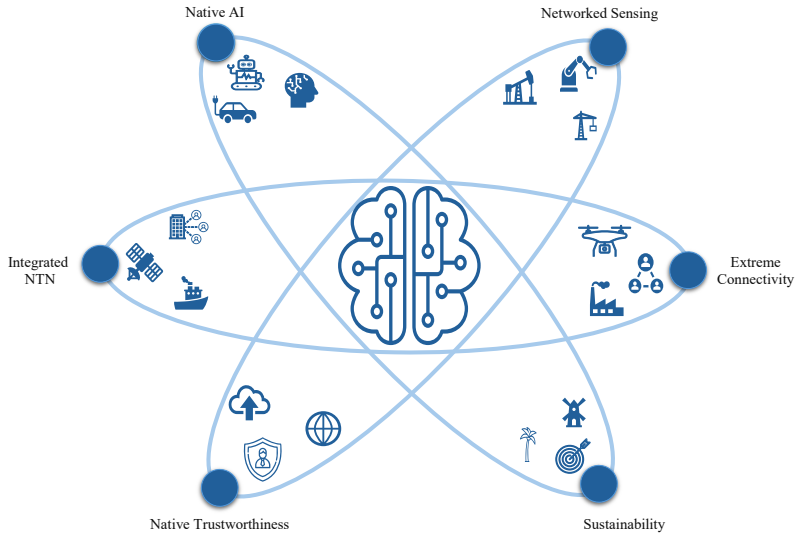

Figure 5: Illustration of core capabilities envisioned for 6G, aligned with emerging performance, architectural, and trust requirements defined by global standardization bodies.

to provide integrated and inherent features with advanced adaptability to support the wider range of diverse verticals and counter the drawbacks of the previous generation of networks. In 6G technologies, apart from further enhancements in technologies that were used in 5G network applications such as O-RAN, mMIMO, network slicing, and AI, some of the new advanced technologies that are expected to facilitate huge network performance improvements include the use of RIS to control the wireless environment, JCAS for enhanced sensing and communication performance, Native AI [50] for making the network more autonomous, adaptable, and efficient, higher frequency bands such as Millimeter Wave Communication (mmWave), THz for communication the will potentially support ultra-high data rates, digital twin technology which will enable real-time virtual replicas of physical systems for predictive network optimization, and distributed learning technologies, such as FL, that will support privacy-preserving and intelligent decision-making at the network edges. In addition to these enabling technologies, 6G will also include satellites and marine communications in the form of NTN, advanced V2X, which will also be connected to satellites etc. Therefore, it is necessary to explore all these technologies (Figure 4) that will support and enable the achievement of the target KPIs and operational goals of future 6G communications, which will in turn drive the people, industry and society towards a future with intelligent, sustainable, secure, resilient, energy-

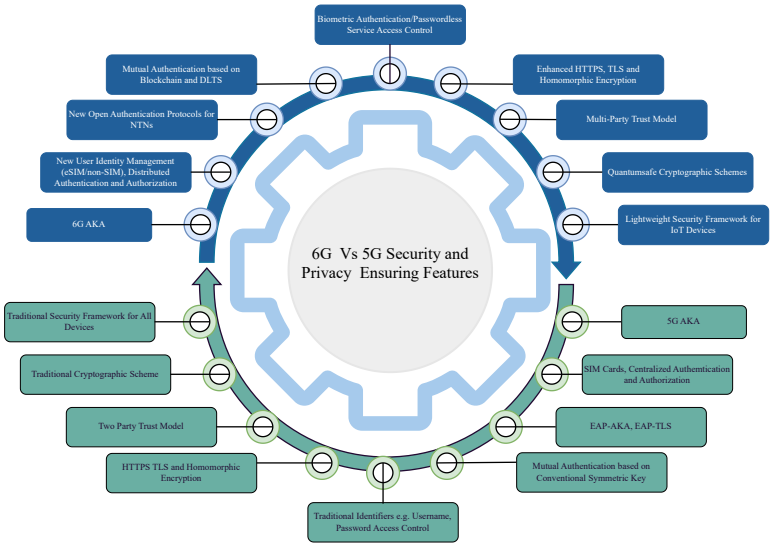

Figure 6: Comparison of 5G and 6G Security and Privacy Requirements.

efficient and ubiquitous connected systems [49] (as illustrated by Figure 5).

D. Unique Security Challenges in 6G and Potential 6G Security Architecture

In this subsection, we describe the unique challenges in security and privacy that 6G networks will have to tackle. In Figure 6, we have shown a comparison of challenges between 5G and 6G networks, to emphasize on the novel challenges in security and privacy, which 6G networks will bring in.

To establish seamless connectivity among a massive number of humans and diverse devices is one of the key goals of 6G networks. However, these devices are vulnerable to security risks and face the challenge of being compromised and exploited by malicious entities Additionally, due to the widespread adoption of diverse open-source technologies, network virtualization, containerization, adversarial ML, and unauthorized exploitation of user information, there will be far more security threats in the network than in 5G [1]. Cross-domain authentication due to the open nature of networks will be a challenging aspect to deal with in these networks. Furthermore, the integration of networks spanning space, air, and marine domains into the terrestrial domains will further increase the attack surfaces. Therefore, to handle these new and unique requirements of 6G networks, it becomes essential to explore more elastic and uniform network-wide security architectures [51], rather than apply perimeter-based defense frameworks of 5G networks. 6G networks are expected to generate high amounts of data, which can prove to be useful digital resource for training AI systems within the network. Therefore, it is necessary to ensure the security and efficiency of these high-value data assets. Unlike in previous generations, when the data transmission was prioritized, in 6G networks due to the presence of different stakeholders, the protection and privacy of these high-value data assets and prevention of their abuse, needs to be prioritized [30]. Moreover, automating intelligence and security in 6G networks will be necessary for handling security and privacy in massive, ubiquitously connected, hyper-reliable and low-latency 6G networks. On integrating intelligence in 6G use case scenarios by incorporating AI will enable learning-based security for predicting, identifying and mitigating threats. Automating security frameworks will benefit the network by automatically responding to incidents and adapting the security policies accordingly in real-time [52]. In future networks, the exclusive use of a vast number of zero-cost, low-power devices would require designing lightweight security and privacy-related frameworks involving these devices with limited capabilities, which is at par with the security of other devices in the system. In JCAS, lower-layer signals are used in sensing to explore the physical attributes, and therefore, it is necessary to protect the sensitive data contained in these signals from any potential security or privacy breach. As described by the authors in [15], the 6G architecture is expected to upgrade from the 5G security architecture (in Figure 2), as shown below in Figure 7. The new upgraded features of 6G security architecture are highlighted in red. According to this architecture, the following key features in each domain will be potentially included to counter the security and privacy challenges that 6G networks are expected to encounter.

(a) 6G Network Access Security: New authentication protocols, along with security and cryptography mechanisms, are necessary for 6G networks, which can be provided by 6G-AKA, PLS and quantum-safe cryptography, respectively.

(i) 6G AKA: The design of 6G-AKA needs to ensure a robust, fast, reliable, and trustworthy authentication protocol between the end users and the core network, between HN and SN, enable device-to-device direct authentication, bridge gaps between devices with diverse and incompatible security capabilities, and revise its new subscriber identifier privacy model [1]. Succeeding from 5G network authentication, 6G-AKA should enable countering attacks to which 5G-AKA

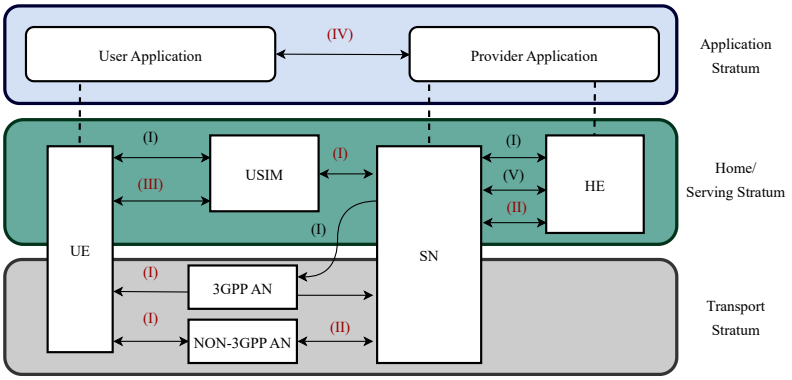

Figure 7: Potential 6G Security Architecture.

is vulnerable to such as linkability attacks, DDoS attacks, single-point-of-failure problem, and forward/post-compromise secrecy etc.. Moreover, 6G-AKA design will determine the authentication in cross-slice communications and the verification of the claimed identity of an endpoint in a deep-sliced and open programmable networking platform. PLS will be highly useful in dealing with conventional threats such as impersonation attacks, and quantum-safe cryptography for ensuring security in highly sensitive and strategic sectors such as banking and defense. These two technologies are discussed in more detail in Section VI.

(ii) New SIM and decentralized subscription model: A shift in identity management by making changes in identity storage or release, can remove many limitations of 5G applications such as IoT. Using an eSIM or a non-SIM model will enable removal of barriers to implant devices in 6G networks. Moreover, an upgrade from centralized authentication and authorization in 5G networks to a decentralized model which will help a visitor network authenticate a UE and sell services such as AR/VR to subscribers it serves.

(iii) New open non-3GPP authentication protocols: New authentication protocols apart from EAP-TLS, and EAP-AKA, are necessary for supporting new communication networks such as space and maritime networks. However, these new networks to be integrated in 6G will face constraints due to limited and unbalanced network resources. Open authentication protocols are thus recommended for these integrated networks in 6G.

(iv) Security-enhanced EAP TLS: EAP-TLS is considered a promising certificate-based mutual authentication protocol in 5G private networks and is included in 5G security standard TS 33.501. However, the transmission of these certificates creates substantial overhead in networks. Therefore, advanced 6G EAP-TLS is will support certificate-less authentication method and other advanced security features for device-to-device authentication without certificates, which will benefit applications like V2X and Digital-to-Digital (D2D) communications in 6G networks.

(b) 6G Network Domain Security: The design of enhanced mutual authentication protocols that protect confidentiality and integrity is necessary in 6G networks. In 5G networks, mutual authentication is based on a conventional symmetric model. However, incorporating Blockchain and Distributed Ledgers can guarantee mutual trust, preservation of high privacy, and prevention of single-failure disruption. They can also authenticate and improve reliability among 6G entities, such as between nodes or servers involved in authentication or between the HN and SN.

(c) 6G User Domain Security: Password-based protection can be easily compromised, involve a cost for storage and could be hard to remember. Future user-based identification and authorization can be based on the bio-identity of users and avoid the use of passwords. For e.g., future technologies such as brainwave or heartbeat-based authentication can be an efficient and theft-resistant password-less service access control mechanism which will enhance user experiences.

(d) Enhanced HTTPS TLS and Homomorphic Encryption: These service and data security mechanisms will be enhanced by equipping them with quantum-resistant algorithms. Homomorphic encryption enables operations on encrypted data without decryption, allowing it to be sent by subscribers to untrustworthy third parties for storage and processing.

(e) End-to-end Service-based and Policy-based Architecture: The deployment of SBA in RAN and core networks will enable flexibility, scalability and efficiency as compared to traditional monolithic architectures. In terms of security, due to the network virtualization and cloud-based frameworks, SBA can enable dynamic scheduling of different modules of authentication, encryption and Intrusion Detection System (IDS) and thereby make the network resilient to various attacks [52]. However, in 6G networks, this service-based architecture is designed for end-to-end security where protection is managed across different layers, domains and networks, and reducing the chances of expansion of attack surfaces. Thus, unlike 5G networks where E2E communication link's security is emphasized, in 6G networks, the security architecture aims to ensure the security and privacy of each component, communication link and data flow within the network. This will ensure the

hierarchy, flexibility, scalability, resilience, trust and privacy of the network.

IV. Progress in Standardization Activities

6G will potentially inherit and build on the security defined and implemented for 5G [11]. This includes security specified in standardization related organizations like 3GPP (Third Generation Partnership Project), ITU, Internet Engineering Task Force (IETF), the European Telecommunications Standards Institute (ETSI), National Institute of Standards and Technology (NIST), O-RAN Alliance, as well as technology, processes, and tools used for security in 5G, such as defined in the security assurance scheme National Electronic Security Authority (NESA) by GSMA. For 6G, standardization of security remains crucial, partly to keep the cost at a reasonable level, but also to provide a desired degree of vendor interoperability in 6G products. The 6G security standards are being developed with contributions from several key standardization bodies, including 3GPP, ETSI, IETF, ITU, NIST and NESAS, and popular projects like Hexa-X, COST and ROBUST-6G where standards are developed by addressing the challenges associated with adoption of new technologies such as AI, and Machine learning while considering the implications of novel enabling technologies towards the network's security, privacy and sustainability. 3GPP and ETSI are standardizations focused on technical aspects of 6G security while NESA compliance is defined for organizational security posture and will influence the security practices implemented in 6G networks. These organizations are working to ensure 6G networks are secure and resilient, building upon existing 5G security frameworks and addressing new challenges presented by 6G technologies like RIS, quantum computing and JCAS.

(a) ETSI: ETSI focuses on developing globally applicable 6G standards for Information and Communication Technologies (ICT). The security and privacy aspects ETSI addresses include virtualization security, automated management systems, data security using AI, users' privacy, and post-quantum cryptography. Among the multiple Industry Specification Groups (ISGs) launched by ETSI, ETSI NFV ISG has developed a White paper [53] in April 2025, that analyze use cases and trends in the evolution of NFV for 6G such as AI-driven threat detection mechanisms to ensure robust protection against cyber security threats. ETSI ISG Zero Touch Network and Service Management (ZSM) released an activity report in 2023 [54] on ZSM, where a group specification GS ZSM 014 that specifies security capabilities for the ZSM framework architecture and a Group Report (GR) GR ZSM 017 on closed-loop automation security aspects. In another white paper on Multi-access Edge Computing (MEC) [55], the authors describe the new security challenges due to its distributed, multi-stakeholder environment, and outlines the risks, threats, and required protections to ensure end-to-end, secure deployment of edge computing systems across networks and applications. ETSI's Industry Specification Group on Securing Artificial Intelligence (ISG SAI) focuses on developing technical reports and specifications that mitigate against threats arising from the deployment of AI, threats to AI systems from other AIs and from conventional sources. In 2023 ISG SAI published four deliverables as GRs [56]. Three of these reports collectively addressed the explicability and transparency of AI processing and provided an AI computing platform security framework. The fourth report explored the threats posed by so-called deepfakes and strategies to minimize them. The ETSI ISG Experiential Networked Intelligence (ENI) published a GR [57] on AI Agents based Next-generation Network Slicing in 2025. ETSI released reports in 2025 and 2026, that strongly emphasized the security, privacy, trustworthiness and sustainability considerations of JCAS in 6G networks. The report released in 2025 outlines 18 advanced use cases where the fusion of communication and sensing technologies will create a more context-aware, efficient and responsive digital environment [58]. For instance, nine out of 18 use cases highlighted, focus on sensing humans, which will prioritize ethical handling of personal data, measures like user consent, anonymization, and protection against unauthorized access. ETSI's recommendations for end-to-end encryption, authentication, and access control for sensing data on JCAS security are crucial for maintaining trustworthiness in 6G. This highlights the need for physical layer mechanisms that can contribute to data integrity and source authentication in JCAS scenarios, which rely heavily on radio signals for both communication and environmental awareness. The report [59] submitted in February 2026, provides potential technical and non-technical requirements of 6G networks to facilitate JSAC services that can overcome challenges specifically around unauthorized sensing, data confidentiality, human privacy, AI-based data processing, and secure handling of sensing data. The ETSI GR ISC 001 report [58] emphasizes that physical layer techniques, such as robust signal processing and interference management, will be essential to ensure the integrity and confidentiality of both communication and sensing data, thereby safeguarding the foundational awareness layer of 6G. ETSI Smart Body Area Networks (SmartBAN) group [60, 61] is working on the standardization of security and privacy for BAN in TR 103.638 and considers physical layer security as one potential approach to ensure confidentiality of in- and on-body devices. ETSI ISG Quantum Key Distribution (QKD) released an activity report [62] to develop specifications that will enhance the security and interoperability of quantum computers deployed across the world.

(b) 3GPP: The 3GPP is actively working on security and privacy aspects of 6G through its Technical Specification Group Service and System Aspects Working Group for Security and Privacy (TSG SA WG3). SA WG3 is involved in defining the requirements and specifying the architectures and protocols for security and privacy in 3GPP systems. 3GPP is working towards creating a 6G security framework that is flexible, scalable, and automated, supporting decentralized key management and trusted communication establishment. 3GPP's Release 18 is the first release of 5G Advanced Systems with the 3GPP WG3 making great progress in specifications related to security and privacy aspects in key areas of security enablers in verticals, security enhancements in 5G Core, security enhancements in RAN, security function evolution, and security assurance [63]. Release 19 will primarily focus

on improving performance and addressing critical needs in 5G commercial deployments, paving the way for 6G standardization with emphasis on work items such as Post Quantum Cryptography (PQC) and public safety enhancements [64]. 3GPP recently completed a study [65] in identifying potential use cases, traffic scenarios and performance requirements for ambient power (zero-energy) IoT. 3GPP's Release 20 (2025-2027) will focus on 6G studies and improvements to security aspects such as L2 control signaling, while Release 21 will deliver the first normative 6G specifications, aligning with the IMT-2030 submission requirements.

(c) ITU: ITU-R is working towards recommending technical performance requirements and common evaluation criteria for 6G, known as IMT-2030. The ITU-R Working Party 5D (WP5D) is responsible for developing and evaluating terrestrial IMT systems, with a focus on 6G networks. The International Telecommunication Union Telecommunication Standardization Sector (ITU-T) is involved in advancing PQC standardization efforts [66] along with ETSi and ISO/IEC JTC 1 [67] to establish interoperable and certifiable frameworks for quantum-safe networks. Moreover, the ITU Recommendation [5] covers the usage scenario of mMTC such as involving the connection of a massive number of devices or sensors (use cases including applications in smart cities, transportation, logistics, health, energy, environmental monitoring, agriculture, etc, considering IoT devices without battery or with long-life batteries). The Recommendation states that the IMT-2030 system is expected to be secure by design. Additionally, to provide a comprehensive framework for the responsible handling of personal data, including collection, processing, storage, and sharing, ITU has transposed the Personal Data Protection and Privacy Principles by the UN High-Level Committee on Management (HLCM) into its regulatory framework in 2023 [68].

(d) NIST: NIST has been involved in processes to solicit candidates, define, evaluate, and standardize quantum-resistant algorithms for digital signatures, public-key encryption, and cryptographic key establishment. In August 2024, NIST released a final set of encryption tools designed to withstand cyber attacks from a quantum computer [69]. The standards have resulted from an eight-year effort by NIST, and contain the computer code for the encryption algorithms, instructions on implementing them, and use cases. These are the first completed standards of the NIST's PQC standardization project and they ensure the security of various electronic information, whether they are confidential email messages or transactions through e-commerce. NIST is taking initiatives to transition the current systems to new standards as they are ready for immediate use. In the area of JCAS, the standardizations proposed by 3GPP are [70] focussed on prioritized use cases, sensing types and their deployment scenarios in JCAS.

(e) IETF: The technical standards and Best Current Practice documents developed in the IETF provide important foundational elements for security and privacy on the Internet. IETF standards strive to be resilient against a host of known and emerging threats. Internet security has long been an integral part of the process of developing Internet standards. Some of the latest efforts by IETF are the latest version of Transport Layer Security protocol, TLS 1.3, Automated Certificate Management Environment (ACME) protocol and the emerging Messaging Layering Security (MLS) protocol [71]. TLS 1.3 updates the most important security protocol on the Internet and delivers superior privacy, security, and performance over previous versions. Privacy Pass protocol is another initiative which aims to improve user privacy in web-based interactions.

(f) AI-RAN Alliance: The AI-RAN Alliance has currently three working groups, namely 'AI for RAN', 'AI and RAN', and 'AI on RAN'. The AI for RAN WG focuses on developing practical solutions on enhancing RAN performance using AI, while the WG AI and RAN discusses convergence, resource sharing and working optimization between the AI and the RAN infrastructures. WG 3, AI on RAN, works on edge AI deployments on RAN infrastructure. A white paper [72] was released by this Working Group (WG) in March 2026, which argues that AI is not only a technical necessity but also a powerful driver of commercial opportunity for for differentiated connectivity, particularly in the uplink and mobile scenarios.

(g) O-RAN Alliance: To provide a robust and consistent 6G security framework, O-RAN Alliance defined specifications will be about the management of cloud resources and network functions in O-RAN environments [73]. O-RAN ALLIANCEs Security Working Group, also referred to as WG11, describes the current state and plans for O-RAN security. O-RAN security specifications were enhanced with new requirements and controls that bring O-RAN closer to a ZTA. Updates to the security specifications enable mobile network operators to operate an Open RAN that meets and exceeds industry expectations for an open, interoperable, and secure system. The O-RAN ALLIANCE Security Working Group is defining a secure O-RAN architecture that includes architectural elements, network functions, interfaces, and data, in collaboration with the other O-RAN ALLIANCE working groups. The O-RAN Security work items include Service Management and Orchestration (SMO), Near-RT RIC Security, O-Cloud Security, AI/ML Security, Open Fronthaul Security, Shared O-RU Security, OAuth 2.0 etc. [74].

(h) Hexa-X, COST, ROBUST-6G: The Hexa-X European 6G research project focused on exploratory research for the next-generation mobile networks with the intention to connect human, physical, and digital worlds with a fabric of technology enablers [75]. To deliver the necessary level of security in 6G networks, privacy, and trust, Hexa-X has identified a set of 6G security technology enablers which are trust foundations, AI/ML assurance and defense, privacy-enhancing technologies, distributed ledger technologies, physical layer security and quantum security. Security and privacy-related objectives that were addressed in recent deliverables include the risk assessment covering security and privacy threat analysis as well as threat impact, and mitigation technologies to address the threats. The Hexa-II initiative considers the social aspects of security, especially in terms of privacy risks, since the 6G will provide connectivity and services anywhere for everyone. Privacy and security are important requirements to be considered both for Terrestrial Networks (TNs) and NTN. Hexa-II also identifies the privacy/security, reliability/availability,

and service continuity concepts as the main constraints and challenges for the next generation networks [76]. The COST Action 6G-PHYSEC focus on creating a European network of academia and industry experts that helps the development of trustworthy and resilient 6G that can instill trust, secure communications and privacy by proposing novel PLS solutions [77]. Five working groups are defined under COST, which are focused on trustworthy 6G, intelligent and resilient systems, quantum-resistant security, scalable and sustainable security, and experiments and demonstrations [78]. ROBUST-6G [79] is a 6G Smart Networks and Services (SNS)-funded project with the primary aim of contributing to the development of data-driven, AI/ML-based security solutions for 6G. ROBUST-6G explicitly encompasses physical layer security within its scope. It includes a dedicated "Physical Layer Security Module" designed to detect and mitigate physical layer threats autonomously using local AI capabilities.

V. Threat Landscape Specific to 6G Enabling Technologies

To design a novel 6G security and privacy architecture, it would be essential to consider the vulnerabilities inherited from the 5G networks and the new threat vectors in the future 6G networks, so that the necessary combat mechanisms are identified and incorporated. In this section, we consider the enabling technologies of 6G and some advanced applications of 5G technology that will potentially contribute as enablers to 6G networks. We describe the potential threats each of these technologies will impose on the network and the necessary security and/or privacy-related measures which will be required to counteract these attacks (Figure 8). For a clear understanding of these threat surfaces, we classify the threats into four categories: physical layer threats, architectural threats, application layer threats, and quantum threats. Each of these threats is explained in detail in the following subsections.

A. Physical Layer Threats

In this section, the security and privacy threats that will be experienced in some of the physical layer technologies of 6G networks are described. The key technologies discussed in this section are RIS, JCAS, NTN, newer frequency spectrum bands (Visible Light Communication (VLC), mmWave, THz), and mMIMO. The physical layer's security is dependent on the physical characteristics of and noise surrounding wireless channels, which is mainly explored in this section for each enabler of 6G technology. For each of these technologies, we describe the definition, functionalities, potential threats in 6G networks they would bring in, and the security and privacy requirements that would be necessary to prevent/counteract these attacks.

1) Reconfigurable Intelligent Surfaces (RIS): RIS are anticipated to be a key component of 6G networks, enabling programmable control over the way wireless signals reflect and propagate. This capability significantly improves coverage and reliability, especially at high frequencies such as mmWave and THz, where maintaining line-of-sight is often a challenge [80]. Compared to 5G, where RIS deployments are more limited and experimental, 6G envisions widespread, AI-orchestrated RIS integration across ultra-dense networks environments. While this evolution improves adaptability, it also expands the attack surface through increased programmability and potential for malicious reconfiguration at scale.

These developments aggravates privacy concerns, as the dynamic manipulation of signal paths in 6G enables more sophisticated inference attacks on user behaviors and locations in heterogeneous IoT environments. Moreover, the RIS deployment introduces a unique set of security and privacy risks that must be proactively addressed. One fundamental threat is passive eavesdropping, as the reflective properties of RIS can unintentionally expose signals to unintended receivers [81]. More seriously, unauthorized or rogue RIS devices, also known as "illegal RIS" (IRIS), may be deployed to redirect traffic, disrupt service, or leak sensitive data [82]. Additionally, attackers could exploit side channels through RIS control signals to infer network behavior or injecting malicious configurations [80]. In IoT-intensive scenarios, poorly secured RIS could even expose sensitive information about user location and behavioral patterns [16].

To ensure secure and trustworthy RIS deployments in 6G, several countermeasures are essential. At the hardware level, RIS should incorporate secure identity mechanisms and attestation protocols to verify authenticity. All control-plane communication must be encrypted and integrity-checked to prevent unauthorized reconfiguration. At the physical layer, defensive techniques such as artificial noise injection, cooperative jamming, and secure precoding can mitigate the risks of interception and eavesdropping [81].

While RIS offers exciting opportunities to reconfigure wireless channels on demand, its programmable nature makes it both a strategic asset and a potential liability. As such, future research must prioritize standardizing RIS trust models, developing secure RIS orchestration frameworks, and enabling privacy-preserving beamforming techniques suitable for ultra-dense, large-scale, AI-driven 6G deployments [80].

2) Joint Communications and Sensing (JCAS): JCAS in 6G networks is the incorporation of radar sensing capabilities with the wireless communications network through alterations at the core functionalities of the network [83]. This will potentially enable sensing nodes to have dynamic access to contextual information from wireless channels [30], which is expected to support and facilitate a wide array of novel use cases across various domains as proposed by 3GPP and other organizations [70, 58, 84]. This will potentially lead to enhancing of sensing performance in terms of better sensing precision, reduced latency and ubiquitous sensing services. On the other hand, by using the sensing capabilities such as perception, and recognition, will enable the wireless communication system in JCAS to improve its performance [30]. This integration will lead to an advanced multi-functional wireless system with potentially increased energy and spectrum efficiency, hardware reuse and computational efficiency [85, 86]. Despite their numerous benefits and emerging use cases however, JCAS is expected to encounter various security and privacy-related challenges, which may impact the network and its users adversarially [87]. We discuss here, some of these

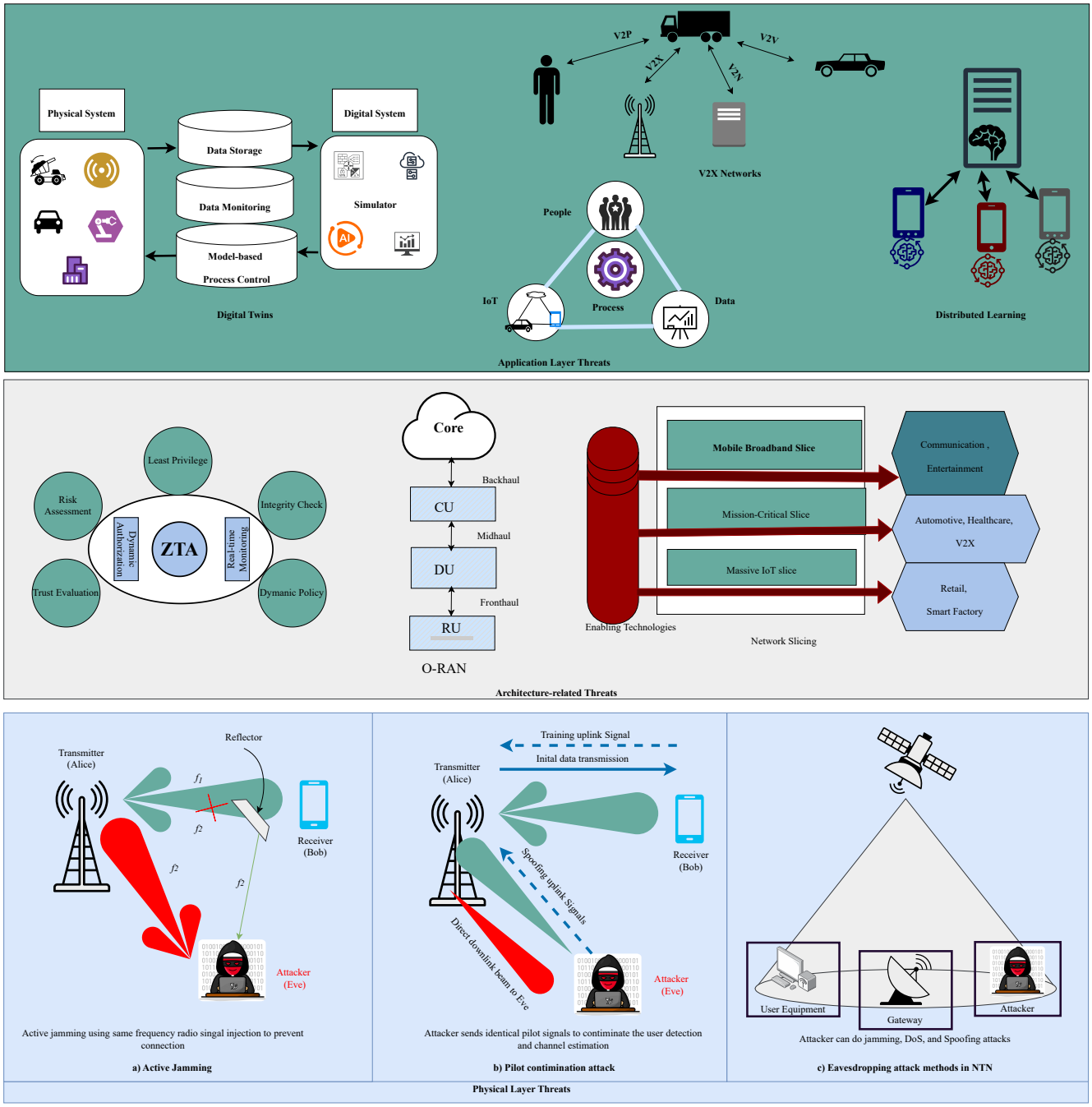

Figure 8: Threat Landscape (Classification of threats and their sources) in 6G Networks.

threats and the potential security and privacy requirements necessary to overcome these threats.

(a) Information Leakage and Eavesdropping/ Exploratory Attacks: Due to the inherent broadcast nature of wireless channels, and the operations of communication and sensing being performed jointly and concurrently, there is a possibility of leakage of sensing information to wireless communication networks [88, 89] or sensing nodes overhearing wireless channel information [90]. The JCAS waveform is designed to offer functionalities for both sensing and communication, which is why malicious users can extract information intended for communication/sensing users only [91] threatening the security and privacy of these networks. Malicious entities may overhear the channel state information of targets that are confidential and specific to the target [92]. Malicious eavesdroppers, in the form of communication users, can also gain access to localization information [92]. Such vulnerabilities in JCAS networks can lead to malicious users breaching the privacy of users or contaminating legitimate reception of signals.

(b) Data Manipulation/Degradation and Exploitation Threats: The trustworthiness of sensing systems in JCAS would be a key performance indicator in 6G systems, there-

fore, the integrity of sensing data is crucial [93]. Sensing information extracted by eavesdroppers such as location or system behavior characteristics can cause a major risk in the security and privacy of JCAS users. Replay, spoofing, jamming and data tampering are some of the potential security threats that the network users will be vulnerable to that can cause inaccurate sensing [86]. Data processing of the sensing information at the edge nodes might cause extraction of sensitive information of the targets and exploitation this data to obtain unauthorized insights into the behavior of users. Moreover, the sensitive data exchanged between UEs or core functions during data processing in the network can risk the exposure of sensitive Personally Identifiable Information (PII) information contained within them [27]. The degree of freedom due to JCAS in Distributed MIMO (D-MIMO) can create new gaps for security attacks [88]. Data poisoning [94] is another issue where attackers can inject malicious data to manipulate the sensing results.

(c) User Privacy Challenges: Enhanced sensing is capable of determining the precise locations of targets/objects and sometimes even provides continuous monitoring, which can reveal contextual information like the target movement pattern etc.. The sensing data captured by the sensing units encompasses both non-human and human targets within the sensing area. The inclusion of PII from humans amplifies the security and privacy issues. High-resolution data could reveal more private, biometric information, such a heart rate, etc. of individuals [30]. JCAS networks, facilitated by electromagnetic waves, can penetrate walls and operate without user consent to cause privacy breaches, which will potentially create an uncontrollable, complex and unpredictable environment that prevents any user from identifying or executing a privacy measure to protect themselves [95, 27]. Moreover, privacy management systems such as Privacy Impact Assessment (PIA) [96] in emerging 6G JCAS networks architectures lack a unified, systematic evaluation of privacy risks and is impacted by the absence of any precise numeric criteria that can assess these risks and evaluate the system's performance [27].

(d) Authorization and Authentication Threats: Data disclosure in JCAS systems can lead to security threats [86]. Having unauthorized access to the sensing data due to a lack of proper authentication in disclosure agreements can hand this data to adversaries. Interception of sensed data during transmission to third parties or adversaries can expose their non-encrypted private information. Data tampering during disclosure could lead to unreliable outcomes. Sensing information in JCAS can be exploited at different levels, whether it is through data capturing, data processing or during disclosure of data. Therefore, sensing data acquisition must comply with different granularity in authorization and privacy protection along with different regional regulations [30]. The data gathered from these networks are subject to privacy breaches such as identity disclosure, location tracking, profiling, misusing information gathered by sensor nodes which implies that it is necessary to include these data as personal data that is subjected to data regulations such as the European Unions General Data Protection Regulation (GDPR) and/or other standards [97]. Moreover, it is necessary to define sensing consent and transparency function at the core, RAN and the UE in a JCAS network [27].

Based on the threats identified in 6G JCAS networks, some of the security and privacy requirements that will be necessary are discussed below.

(a) Leakage and Eavesdropping Mitigation Techniques: As we discussed before, due to the single modality for communication and sensing function in JCAS, there are possibilities of leakage of sensitive information carried by these sensing signals. Therefore, techniques to minimize these leakages are essential for maintaining security and privacy of these networks. In [89], the authors proposed an approach of mitigating leakage of information between the two systems by balancing sensing with providing secrecy of information. The transmitter where the transmitter simultaneously conveys information and estimates channel state information but the receiver acting as an eavesdropper, receives this information only partially, reducing the chances of divulging sensitive information. Another approach discussed in [30] is the proper design of sensing reference signals based on shared information exchanged between the sensing and sensed nodes which could be used to protect sensing result from eavesdroppers.

(b) FL to train Distributed Models Without Sharing Data: FL can be a useful tool to train models in JCAS networks where the sensing data Data augmentation and lightweight versions would help to counter challenges when the there is a possibility of high communication overhead [98].

(c) Defining of Sensing Consent and Transparency at the Nodes: In 6G JCAS networks, it would be crucial to define new network functions at different levels of the architecture so that sensing consent and transparency is maintained during monitoring sensing sessions. In [27], the authors proposed a new network function called Sensing Policy, Consent, and Transparency Management Module (SPCTM) which is defined at the core of the network for the same purpose. Considering the roles of gNB and UEs in distributed JCAS systems, functionalities similar to SPCTM should also be designed for UEs and gNBs [86].

(d) Privacy-enhanced Data Management and Information Processing: The inherent complex architecture of JCAS architectures makes is challenging to assess and mitigate privacy risks. In Cyber-Physical Systems (CPS) designed for JCAS networks, the challenge lies in making informed decisions on risk mitigation while ensuring a balance between privacy protection and functional efficiency of the system. These decisions can be effectively taken based on a quantifying approach towards aggregation, normalization and prioritization of privacy risks. Thus, new structured, quantifiable and dynamic frameworks of privacy management and data processing are necessary that will have the ability to aggregate privacy risks across components and and update dynamic evaluation with incorporation of new controls [86, 27].

(e) Counter-measures and Preventive Design at Physical Layer: To counteract the unique security and privacy threats in JCAS networks, it is essential to design a layered security system [47] that combines secure physical-layer design with robust operational and system policies. Some of the counter measures to prevent jamming, spoofing in communication and interference and malicious sensing in sensing include secure

waveform design [99], physical-layer authentication [100], and robust signal processing techniques [101]. On the other hand, these attacks can be prevented by implementing physical layer designs such as Hybrid Cyber-Physical TestBeds (CPTs) [102], implementing security policies such as authentication and incident handling in parallel to the technical counter measures and continuous monitoring, assessment and adaptation to new threats.

3) Non-Terrestrial Networks (NTNs): 6G networks are envisioned to provide ubiquitous, high-capacity, low-latency connectivity across land, oceans, and airspace. Especially, the extension of the ground-based infrastructures to space will potentially bring about a new wave of connectivity and would require progress and innovation in other related sectors like communications, navigation, monitoring of the environment, surveillance and research. The NTN mainly comprises of aerial and space borne elements like satellite systems, High-Altitude Platforms (HAPS), and UAVs. The dynamic ecosystem formed by combination of heterogeneous and complex architectures of terrestrial networks and NTN is also described as Space Information Networks (SINs) [103]. Through complementing terrestrial network services, NTN aims to deliver highly reliable and ubiquitous connectivity, global coverage and a wide array of novel services, such as global IoT, disaster response, and real-time surveillance in infrastructure-sparse regions. NTN can be logically divided into three interdependent segments: the space borne Segment, the air borne Segment, and the ground Segment. These segments form a hierarchical, multi-layered architecture requiring dynamic coordination to support evolving mobility patterns, user demands, and mission-critical applications.

However, due to rapid progress in digitization and the reliance of NTN on Commercial Off-the-Shelf (COTS) components, open networks, SDNs, and Internet of Space Things (IoST), the threat surface in these networks are expected to expand manifold. Due to the complex integration and interconnectedness of diverse communication technologies involved, and evolving cyber threats, NTN can pose a significant risk to critical infrastructures, such as national security. Moreover, these networks are more vulnerable to threats than terrestrial networks, because unlike the latter, the performance of NTN are limited by constraints like their longer development life cycles, limited computational resources, and physical inaccessibility once deployed. A few of the critical security vulnerabilities in NTN are,

1) **Security and Privacy Threats due to Nature of links:** It is essential that NTN play the crucial role of safeguarding confidentiality, integrity of transmitted data. But due to the broadcast nature of channels, mobility, extended coverage and vast distances of transmission, NTN links are susceptible to unauthorized data interception, eavesdropping, and signal jamming [19]. When transmission of sensitive data is concerned, the vulnerabilities due to the long distance of propagation raises privacy-related threats too. Infrastructure-based security practices and conventional security approaches are less effective in practically dealing with such vulnerabilities especially in dynamic environments. Therefore, there is the need for lightweight, adaptive, scalable, advanced encryption security solutions that can enhance the reliability of NTN transmission links. One of these solutions is PLS which leverages the randomness of wireless channels to ensure their security and integrity [104].
2) **System Complexity, Heterogeneity and Interconnectedness:** The NTN are formed by the complex and deeply interconnected integration of highly diverse set of communication networks and platforms, ranging from satellites to HAPS and terrestrial infrastructures. Each of these networks are defined by their unique latency, mobility, and link characteristics and a weakness in any physical or logical connectivity can quickly affect the entire network. This heterogeneity and complexity of networks also increase the complexity of routing, resource management, and inter-system orchestration [19, 105]. The rise of mega constellations which are large groups of interconnected satellites, are creating new cybersecurity challenges. With the extensive use of COTS components and cost-effective satellite mega-constellations that rely on open source software and hardware, the dangers of cyberthreats are expected to increase further. Therefore, it is necessary to find novel frameworks to ensure security across interoperable, diverse networks and platforms.
3) **Security in Virtualized Multi-Orbit Architectures:** The integration of multi-orbit architectures and multiple terrestrial networks by using satellites as routers is necessary in 6G networks. However, this will lead to new security risks in the future. In these scenarios, it will be critical to track traffic across different networks and constellations and ensure end-to-end security. Further, the adoption of O-RAN and SDN/NFV in NTN control planes introduces vulnerabilities such as spoofing, jamming, and cyberattacks on programmable interfaces [19]. New applications such as cloudification of space, will require strict security measures to prevent any malicious code from being executed in space [106]. Due to rapid progress in the field of optical communication between satellites and between satellite and ground station, seamless and always on connectivity between the ground and the space vehicles is expected. However, this would require securing of the data transmission through these ubiquitous links and protecting them from threats in real-time [107].
4) **AI-Induced Risks:** AI plays a vital role in automating spectrum allocation, beamforming, and fault management in NTN. However, AI techniques face a wide range of challenges in NTN due to the unique features of non-terrestrial environments. The influence of changing atmospheric conditions, dynamic connectivity, inability of conventional AI techniques to adapt effectively to changing domains, reduced effectiveness of AI models due to constraints in transmission of data training sets through limited bandwidth, are some of these challenges [19]. Among security-related challenges, adversarial threats such as data poisoning, model evasion, model theft attacks, inference related attacks, or physical infrastructure threats, are the prominent threats that can compromise the network's integrity and security [108]. Additionally, ensuring the ro-

bustness, explainability, and transparency of AI models in critical applications such as satellite communications, remains a challenge [105]. Therefore, advanced encryption and AI-based anomaly detection are necessary to enhance security in AI-driven NTN systems.

5) **Authentication Across NTN-Terrestrial Domains:** As NTN evolve, new authentication mechanisms tailored to cross-domain communication between satellites, marine nodes, and terrestrial networks will be necessary [15]. Privacy is a major concern in NTN due to collection and transmission of data across multiple, potentially insecure domains which necessitate strong encryption and authentication protocols. Privacy is another major concern in NTN due to collection and transmission of data across multiple, potentially insecure domains which necessitate strong encryption and authentication protocols.
6) **Lack of Security Standard Measures:** Unlike traditional security measures used for terrestrial systems, non-terrestrial networks usually prioritize availability and safety over confidentiality, and integrity aspects of communication, which will potentially by exploited by attackers. Moreover, the lack of tracking and mitigating vulnerabilities in NTN will further alleviate the security problem in these networks.
7) **Lack of Cyber Resilience Standards:** It is essential for space and airborne networks to develop comprehensive and resilient engineering standards to handle unique challenges that comes with their execution such as faults induced by radiation, lack of physical accessibility during repairs, and long term reliability requirements.
8) **Quantum threats:** To secure non-terrestrial communications in future quantum era, it is necessary to implement quantum-resistant techniques such as secure encryption algorithms and protection of sensitive data such as encryption keys encryption keys. Moreover, to update encryption algorithms for satellites during its lifespan, it is essential to use secure protocols.

There is a need for a strong, scalable and flexible security solutions to handle the wide range of adversaries that might attack NTN. Based on these challenges discussed earlier, the following design principles are essential for a robust and secure 6G NTN.

1) **Secure and Robust AI/ML Models:** To ensure tamper-resistant, explainable, and trustworthy AI decision-making under adversarial conditions, it is essential to build secured and robust AI/ML models. Robust AI models in NTN would be able to reliably function and adapt to unpredictable, dynamic atmospheric conditions and changing domains without any discontinuity of service [105, 109].
2) **Standardization and Interoperability Frameworks:** To enable seamless orchestration across LEO/MEO/GEO satellites, UAVs, HAPS, terrestrial components, and different open standards involved, strict security assurances are necessary that meets regulatory standards and provides interoperability among different cybersecurity frameworks [108]. To ensure that enabling technologies for NTN are secured in presence of vulnerabilities such as high transmission delays, it is necessary to design and test these networks aided by 6G enabling technologies such as O-RAN-aided NTN [19].
3) **Blockchain-based Authentication:** In decentralized NTN systems, blockchain-can be leveraged to design authentication, access control and identity management techniques for verification of user and device identities. Blockchains can also be used for immutable and transparent data sharing, which in turn ensures data integrity and secure consensus in distributed systems [110].
4) **Dynamic Security and QoS Enforcement:** To support service-level isolation and strict performance guarantees with respect to security, in real-time for diverse NTN applications, traditional security methods are relatively static. For such demanding scenarios in NTN, dynamic slicing and security changes that adapt to real-time slicing is necessary. Such mechanisms can secure independent slices created and modified in real-time, which in turn is crucial in enhancing the overall security of the network under dynamic conditions.
5) **Distributed Edge Intelligence and Federated Learning:** To reduce latency and enhance data privacy through localized processing, especially in disconnected environments, distributed edge intelligence and federated learning can play a significant role.
6) **End-to-End Security Architectures:** Tailored to the dynamic, multi-segment, and multi-domain nature of NTN, designing end-to-end security frameworks that includes secure bootstrapping, trust management, and encryption schemes are essential [19].
7) **Privacy Preserving Solutions:** In a network with extended set of vulnerabilities due to long distances of transmission, it is important to secure sensitive information transmitted across. Therefore, it is significant to explore the integration of privacy-preserving mechanisms like federated learning, Differential Privacy (DP), semantic communications, and homomorphic encryption with the security architecture of NTN.
8) **AI-based Cyber Defense:** A critical emerging security measure in the non-terrestrial domain is the development of AI-enabled autonomous defense systems which mainly represents self-healing constellations. The satellites with such a cyber defense system can detect and neutralize threats autonomously, in real-time and adjusts their defense accordingly. Moreover, satellites can also share these threats to their neighbor satellites whom they trust. Such AI-enabled autonomous cyber security systems can potentially mitigate attacks in satellites with faster responses and can impact the security in NTN networks.

These requirements highlight the necessity for a co-designed approach combining communications, AI, and cybersecurity disciplines to realize the vision of resilient and intelligent 6G NTN.

4) Newer Frequency Spectrum Bands: To cater to the demands of faster data rate, higher capacities, and lower latency, advanced applications of 6G networks, the incorporation of new frequency bands, and the overall spectrum management will become even more crucial. Some of the new frequency

bands that will be extensively used in 6G technology are the mmWave, THz, and the Optical spectrum bands. During 5G spectrum sharing, it was found that a lot of the assigned bands were left underutilized. In 6G, the limitation of resources and need for higher data rates and capacities is anticipated to widen, due to which spectrum sharing will have a more important role to play for better resource efficiency. Due to the incorporation of the new frequency bands and the spectrum management features like spectrum sharing, several security-related attacks may arise in 6G networks. Some of the key threats and the requirements necessary to counter these attacks are described below.

1) **Security in THz Communication:** Incorporating the THz band into the spectrum would be able to provide a solution to the limitation in capacity of spectrum resources in future wireless networks. These communications have a shorter wavelength than their mmWave counterparts and therefore, can produce highly directional transmission [111], significantly mitigating inter-cell interference and the chances of the communication being listened to. Although the THz communications are assumed to be more secure, they are prone to being intercepted by eavesdroppers during LoS transmissions. Therefore, to incorporate security features that can combat these threats, there is a need for physical layer security techniques [112] that enhance security features by exploiting the physical characteristics of the wireless channels.
2) **Security in Optical Wireless Communication Technologies:** Optical communication technologies, such as VLC, LiFi, and molecular communications (MC) [113], will potentially contribute to increasing the attack surfaces of 6G networks. In VLC or hybrid VLC-RF systems, malicious transmitters can pass undetected. A highly directed transmitter, that uses optical beamforming techniques, increases the successful attack probability. This would lead to such networks being vulnerable to jamming or data modification attacks. When the nodes involved in these communication technologies are deployed in public areas and/or are in the presence of large windows in the coverage areas, they become as vulnerable as RF nodes and suffer from eavesdropping attacks in the presence of cooperating eavesdroppers. Similar attacks occur for high-throughput indoor VLC systems [113].
3) **Security in Spectrum Sharing:** Spectrum sharing mechanisms are required to be designed for optimal resource allocation, enhance access to resources and enable sharing of spectrum among multiple stakeholders in a dynamic environment. While executing this kind of sharing of spectrum, it is necessary to guarantee fairness, transparency and security among the participants [30].

5) 6G Massive MIMO: mMIMO systems are a cornerstone to 6G wireless infrastructure, offering enhanced spectral efficiency, precise beamforming, and energy-efficient spatial multiplexing [117]. In contrast to 5G, where mMIMO implementations typically involve fewer antennas and operate primarily in sub-6 GHz bands, 6G is expected to expand into ultra-massive arrays in mmWave, THz frequencies, and deeply integrated AI-driven beam management, to meet extreme performance goals such as speeds of the order of Terabits per second (Tbps), immersive connectivity and ubiquitious AI. These deployments which are also called Extreme mMIMO or 6G mMIMO, although aims to achieve extreme performance goals, will also significantly contribute to increasing the attack surface in future communication networks.

This architectural shift heightens vulnerabilities particularly to adversarial ML attacks targeting channel estimation and beam prediction. Moreover, the finer spatial resolution enabled by 6G mMIMO systems intensifies privacy concerns, as it allows more precise side-channel inferences on user mobility and data flows than the coarser beamforming architectures typical of 5G. The increasing complexity and dynamic nature of 6G's AI-native wireless environments further expand potential vectors for attack [1].

Key security threats in 6G mMIMO deployments include:

1) Eavesdropping and Spoofing Attacks during uplink training and downlink transmission, particularly targeting Channel State Information (CSI) estimation and beamforming process [114].
2) Pilot Contamination and Injection, where attackers manipulate pilot signals to corrupt CSI and degrade beamforming accuracy [118].
3) ML Attacks, including adversarial input perturbation, model inversion, and poisoning, particularly in AI-based beam prediction pipelines [115].
4) Side-Channel Inference, which leverages spatial signal patterns to deduce device location, mobility patterns, or application profiles [116].

To mitigate these evolving threats, 6G mMIMO systems require a multi-layered security approach that combines physical-layer defenses with intelligent control:

1) **Physical Layer Security (PLS):** Deploy secure precoding, artificial noise injection, and channel-based key generation to enhance confidentiality and counter passive eavesdropping [114, 118].
2) **Robust Pilot Design:** Employ randomized, encrypted, or non-orthogonal pilot sequences to mitigate pilot contamination and impersonation attacks [116].
3) **AI-Aware Security Hardening:** Secure ML pipelines for beam prediction and channel estimation against poisoning, model stealing, and adversarial perturbations [115].
4) **Context-Aware Beam Control:** Dynamically adapt beam patterns based on environmental sensing and threat profiling to limit exposure to hostile regions [117].
5) **JCAS:** Integrated sensing capabilities to detect abnormal spatial activity indicative of jamming, spoofing, or pilot interference [114].

As 6G moves towards ultra-dense, AI-driven deployments, real-time distributed threat detection and secure, scalable mMIMO coordination will become critical. Future research must bridge the gap between physical-layer cryptography and system-level resilience, especially in scenarios involving large-scale antenna systems and AI-augmented radio intelligence [1].

TABLE II: Summary of Physical Layer Threats, and Security Requirements.

Technology	Purpose	Key Threats	Security Requirements / Countermeasures
RIS *[81], [82], [80]*	Programmable wireless reflection for coverage enhancement	Eavesdropping, rogue/illegal RIS (IRIS), signal leakage, side-channel attacks	Hardware attestation, encrypted control-plane, artificial noise injection, jamming, secure beam control
JCAS *[85], [88], [91], [95], [27],*	Unified communication and radar sensing integration	Leakage, spoofing, replay, jamming, privacy breaches, data poisoning, weak authentication	Secure waveform design, federated learning, SPCTM for consent, privacy quantification frameworks, physical-layer authentication
NTNs *[104], [19], [108]*	Global, seamless coverage via satellite, UAVs, HAPS	Long-distance interception, spoofing, AI poisoning, SDN/NFV vulnerabilities	Robust AI/ML, federated edge learning, dynamic slicing, end-to-end trust and encryption, multi-domain authentication
THz / mmWave *[111], [112], [113]*	High-rate, low-latency communication in extreme bands	THz LoS eavesdropping, VLC spoofing, jamming, insecure spectrum sharing	Physical-layer security (PLS), beamforming countermeasures, dynamic and fair spectrum protocols
6G mMIMO *[114], [115], [116]*	Energy-efficient spatial multiplexing and beamforming	Pilot contamination, CSI spoofing, ML model inversion, side-channel inference	Secure precoding, encrypted/random pilots, adversarial-robust ML, JCAS-integrated threat detection

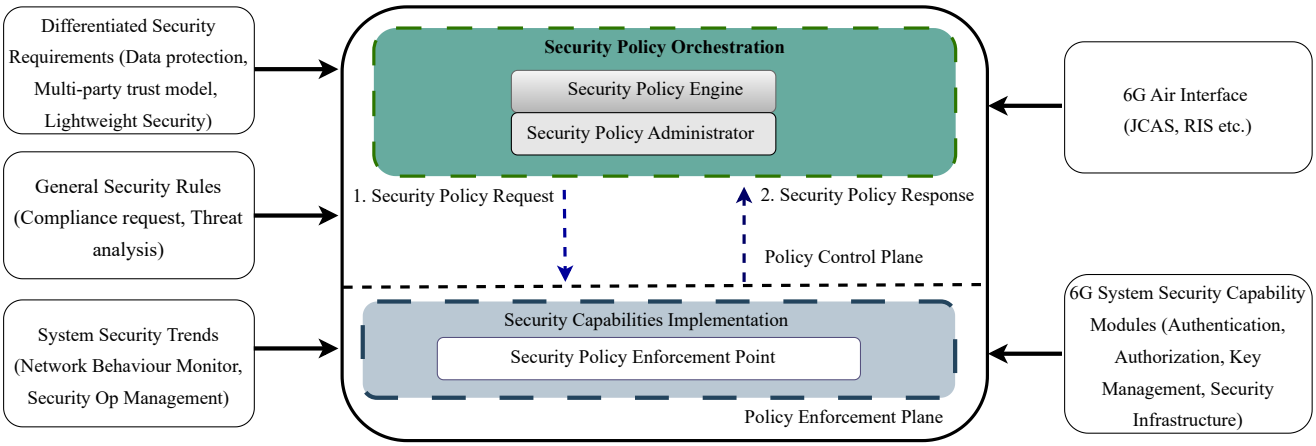

Figure 9: Intelligent ZTA based 6G Security[30].

The physical-layer threats in 6G networks are summarized in Table II.

B. Architectural Threats

6G applications would necessitate automated and multilateral security features to support the novel applications envisioned. In this section we aim to identify the network and architectural enablers of 6G networks and explore the security and privacy-related vulnerabilities that might arise in them [93]. If we compare to the security and privacy frameworks in 5G networks, 6G networks will require a framework where security cloudification in 5G will need to upgrade to security automation in 6G, where zero trust security would need to enhanced to intelligent zero trust security, traditional network management and orchestration to ZSM, high to ultra high confidentiality and integrity, lightweight security to ultra light security, more real-time and energy efficient security features)[19].

Some of the potential key technologies that are expected to define the 6G security architecture are Intelligent ZTA, ZSM, O-RAN, 6G Network Slicing, Distributed and Scalable Architectures. We discuss next, the network and architectural vulnerabilities that will arise from these enablers.

1) Intelligent Zero Trust Architecture (ZTA): In current and future networks, unlike in the previous generation networks, the origination of security threats is expected from within the network [51] in addition to threats from beyond the network perimeters. Therefore, ZTA is a cybersecurity approach that is used to address and evaluate the potential risks in a network and their access/restriction to the network [119]. The core principle of ZTA is to "never trust, always verify" every user, device, and application for dynamic protection of digital resources in local networks [51]. To enable this principle, features that are essential in ZTA [119] are described below.

(a) The Continuous Diagnostics and Mitigation (CDM) program, which monitors the ZTA continuously and predicts threats based on traffic patterns and exchanges of messages between devices [120].
(b) The Security Information and Event Management (SIEM) system, which does real-time collection and aggregation of information, that creates an organization's comprehensive security posture. Further, by using advanced techniques like correlation and analysis of security events, new threats, trends or abnormalities are detected or predicted within the system [121].
(c) Threat intelligence is a framework that helps an organi-

zation to assess potential security risks to their networks, previously known threats along with the tactics, techniques and procedures (TTPs) they used, and, emerging threats which were possibly not identifiable earlier [122]. Threat intelligence can be applied to risk management solutions such as stakeholder risk analysis, and creating cyber threat profile. Therefore, collaboration between these two systems can improve informed decisions and risk exposure for a more secured system.

(d) The threat models in ZTA are different in ZTA from the ones in traditional environments, because unlike in the latter case, where the focus was on the perimeter, in ZTA, the modeling paradigm has to be redefined such that, identity is the new perimeter, access is granular and dynamic, and attack surfaces are abstracted [123].

(e) Defining of access control strategies are necessary through which the user's identity is established, and the user's privileges for conducting of different operations involving protected resources, are determined. Strong authentication for users and devices in critical infrastructures, context-aware and continuous authentication, defining of risk-aware access control, are some of the prerequisites of access control system in ZTA.

(f) Network segmentation and software-defined perimeters provides a granular security approach where every connection is treated as potentially hostile, and strict access policies are implemented, irrespective of their origin. Furthermore, lateral movement of risks in networks if compromised, are minimized by implementing network segmentation [119].

(g) AI/ML-enabled security automation in ZTA enables automatic detection of threats, development of flexible and adaptive responses to threats, and provides predictive performance analysis.

(h) Intent-based policies for security and trust management using high levels of intelligence, analytics, and orchestration are helpful in automatic translation of high-level objectives in security and trust to specific, low-level configurations needed to achieve them, eliminating the need for any manual execution of the individual tasks.

However, the existing ZTA cannot handle new security-related challenges that will potentially emerge in 6G networks [119, 124]. Some of these challenges include the massive distribution of diverse devices interacting with the network potentially will produce a massive workload in posture scrutinization, the current access-control strategies used to deal with resources and services may not be able to cope with ultra-large scalability and complexity of 6G networks, the cross-domain authorization and decentralization of the current, logically-centralized, trust management system [125] necessary in more open 6G networks with decentralized architectures involving multiple domains, and the end-to-end encryption requirements under resource constrained environments in future networks. Therefore, it will be useful to embed AI into the ZTA, to achieve an intelligent security architecture for dealing with internal and/or external known threats or zero-day attacks [51]. Embedding intelligence in ZTA can enable supporting of intelligent security policies, orchestration of security policies flexibly and dynamically based on the new scenarios and developments in the security architecture, configuration of security functions intelligently to meet the security requirements, and maintenance of backward compatibility properties [30].

Several centralized and distributed frameworks have been proposed in [30, 51, 124] for designing dynamic secure access control architecture through collaborations among domains in ZTA. A few of the important design aspects of intelligent ZTA for 6G and future networks are,

(i) Distributed and logical architecture: The distributed and logical architecture, as discussed in [30], allows for the design of subsystems that are both flexible and versatile (as shown in Figure 9) and the core components of this architecture are Security Policy Engine (SPE), Security Policy Administrator (SPA) and Security Policy Enforcement Point (SPEP). The SPE develops security policies based on inputs of the architecture. The SPA provides communication path between SPE and SPEP and to provide both input and output. The SPEP is involved in providing differentiated security services for each subsystem. Moreover, to incorporate dynamic security principles and new capabilities into the architecture, a security variable in addition to a system variable is used. Both of these variables are adjusted to achieve necessary security policies intelligently.

(ii) Decentralized identity management: The decentralized identity management provides and maintains a unified identity system due to heterogeneous frameworks, diversified network operators and suppliers of devices. Decentralized identifiers in the form of digital signatures are necessary for authentication in local communities using a local controller. Apart from easing the access control of diversified UE in 6G networks, this feature promotes elasticity and scalability of a unified identity scheme [126].

(iii) Dynamic trust evaluation: The third aspect of ZTA design in 6G networks is trust evaluation system. The trust value in ZTA networks are based on observation of historical behaviors and values recommended by third parties. Therefore, the trust of a UE is determined by the determination of trustworthiness in the home community through identity, authentication, and self-evaluation, followed by determination of trustworthiness in the accessed community, and finally by evaluation of trust of the guest UE using the two previous values [127]. ML- based algorithms can be employed to further evaluate dynamic trust attributes where trust scores for entities/agents requesting for access to network resources could be derived from real-time behavioral analysis of the network traffic data in addition to historical data. This way a dynamic trust evaluation system will potentially empower intelligent ZTA to make more informed and real-time decisions [128].

(iv) ML/AI-based detection mechanisms: Developing intelligent intrusion detection systems based on ML/AI, can enable continuous learning and adapting to new,

evolving patterns of attack, identification and mitigating of intrusions and anomalies in the system. For instance, the integration of the Deep Learning (DL) model called transformer, enhances anomaly detection capabilities in ZTA [129], especially in the O-RAN, and thus, strengthens ZTA security.

(v) Integration of PQC: With the advent of quantum computing, new challenges are expected to emerge, especially with respect to safeguarding of sensitive information in the network. In these circumstances, it is necessary to evaluate the security vulnerabilities of current cryptographic frameworks and strengthen the defense against future potential attacks through the integration of quantum resistant algorithms to ZTA security models. A layered defense system with continuous verification and access controls that constantly adapts to dynamic changes is essential for preempting and counteracting sophisticated threats in the era of quantum computing. That will ensure an overarching and robust security architecture for future networks [130].

2) ZSM: To handle the exponential growth in volume of data and increased complexity in future 6G networks, the emerging paradigm of ZSM, a state-of-the-art network automation framework originally proposed and updated by the ETSI [131], offers automated self-management and self-healing in networks, resulting in reduced human interventions, enhanced performance and reduced network management costs [132]. These functionalities by ZSM cannot be offered by traditional and static Network Management and Orchestration (MANO) [133] approaches in networks. The diverse network automation solutions can be realized by leveraging advanced ML technologies to enable intelligent decision-making in the management of resources and ensuring the necessary security of the networks. Unlike traditional ML approaches which requires significant human intervention, domain expertise and are susceptible to degradation in performance due to unexpected environmental changes etc. when deploying and developing ML models, automated ML is considered to be a promising solution for data-driven network services in ZTAs of ZSM in handling those challenges [134]. While allowing network operators to deploy and manage network configurations with accuracy, reliability and speed, ZSM also minimizes the risks of security breaches. For e.g., in [135], ZSM automates the supply chain for securely onboarding the devices in an IoT network, thereby minimizing human intervention. This reduces the possibilities of any configuration error, and ensures that each device is authenticated, securely booted and checked against any relevant security policies before it joins the network.

However, technologies that enable ZSM create potential security risks and can hinder the security-enabling functionalities of ZSM. Some of the enablers of ZSM that potentially create threats within it are Open API, Intents, Automated Closed Loop, SDN/NFV, AL/ML [132]. Threats due to Open AI include Man-in-the-Middle (MITM), DoS, Identity attack, Buffer Overflow, SQL Injection, Script Insertion, Application and data attack. Threats due to AI/ML are Adversarial attacks, Model Extraction and Model Inversion Attacks. SDN/NFV-related attacks are Privilege Escalation and Spoofing. Data exposure and tampering are Intent-related threats. Automated Closed Loops generates Deception attacks apart from MITM and Dos attacks.

To protect networks from cyber attacks in 6G networks with a massive number of heterogeneous mobile devices, the three main requirements are innovative authentication and access control solutions, intrusion detection and/or mitigation mechanisms, and AI/ML-based decision making frameworks. In 6G networks, the use of traditional cryptography-based authentication methods, such as device authentication and IDS, are expected to be challenging because of issues like distribution and management of cryptographic keys, and computational complexity associated with key generation and detection. Therefore, the design of innovative security solutions, such as Physical Layer Authentication (PLA), PLS, Physical Layer Key Generation (PLKG) and Cross Layer Intrusion Detection Systems (CLIDs) are necessary [136]. PLA schemes are used to verify the authenticity of network devices based on their physical layer characteristics [137]. PLS ensures that the transmission between entities is kept confidential by leveraging the physical layer characteristics inherent to them, avoiding the need to share secret keys. PLKG uses the physical layer properties among entities to extract random keys. CLIDs are IDSs that integrate information from multiple layers of the protocol stack to detect and mitigate cyber attacks [136]. Moreover, automating these solutions to automated PLA and CLIDs is essential for automatic threat detection and authentication in ZTNs in 6G environments. Finally, to safeguard against unknown and emerging attacks and hence enhance the security posture of organizations, they must incorporate AL/ML-based security decisions and updates into the ZSM framework.

3) Open RAN (O-RAN): O-RAN are central to 6G's vision of disaggregated, intelligent and flexible RANs, allowing openness and interoperability for multi-vendor ecosystems [138]. Unlike in 5G, where O-RAN primarily emphasizes interface standardization and basic virtualization, 6G incorporates advanced AI-driven control loops and cloud-native elements. This evolution increases the risk of real-time manipulation of xApps/rApps and magnifies supply chain vulnerabilities across a broader ecosystem. Additionally, the deeper integration of ML in 6G enables potential inference attacks on user data flows that are less prevalent in 5G's less intelligent architectures. While O-RAN enhances flexibility, innovation and cost efficiency, it also introduces new security, privacy, and trust challenges due to the increased attack surface and reliance on open interfaces [31].

Key security threats include attacks on open and standardized interfaces (E2, A1 etc..), manipulation of AI/ML models within near-real-time and non-real-time control applications (xApps/rApps), and vulnerabilities in cloud-native infrastructures such as container breakout and lateral movement [18, 138]. The presence of supply chain vulnerabilities from diverse hardware/software providers complicates trust management, raising concerns and risks about firmware backdoors, insecure update mechanisms, and abuse of exposed APIs [139, 140].

TABLE III: Summary of Architectural Threats and Security Requirements in 6G Networks

Technology	Purpose	Key Features	Security Challenges	Security Requirements / Countermeasures
ZTA *[51], [119], [126], [127], [130]*	Secure, dynamic access control; assumes breach by default	Least privilege, continuous verification, distributed architecture, decentralized identity, trust evaluation	Insider threats, MITM, credential theft, device vulnerabilities, API abuse, zero-day attacks	Post-quantum crypto, AI/ML detection, CDM, SIEM, dynamic trust, game-theoretic ML
ZSM *[135], [132], [136], [137]*	Autonomous network and service management	Self-healing/config, ML-driven ops, reduced human intervention	Threats via Open APIs, AI/ML model attacks, SDN/NFV exploits, Intent tampering	PLA, CLID, PLKG, automated AI-based intrusion response, secure onboarding
O-RAN *[31], [18], [139], [138], [140]*	Open, modular, intelligent RAN for multi-vendor ecosystems	Disaggregated architecture, AI-powered xApps/rApps, cloud-native infra	Interface attacks (E2, A1), ML poisoning, supply chain threats, lateral movement	ZTA, runtime ML monitoring, secure APIs, end-to-end encryption, trusted updates
Network Slicing *[26]*	Logical partitioning of networks into isolated slices with specific QoS/security	Slice-level control, SDN orchestration, multi-domain support	Cross-slice attacks, resource starvation, orchestration hijack, edge inference attacks	OAuth, TLS, federated trust, edge privacy (homomorphic encryption), ML anomaly detection

To mitigate these risks, 6G O-RAN security strategies must incorporate: **(1)** ZTA for continuous authentication and authorization. **(2)** AI-driven threat detection and runtime security monitoring for virtualized O-RAN deployments.

Additionally, end-to-end encryption, secure update mechanisms, supply chain integrity verification, robust API security, and AI-based risk mitigation will be essential for scalable and secure O-RAN deployments. However, challenges remain in achieving interoperable security across vendors and ensuring real-time anomaly detection in cloud-based RAN environments.

4) Network Slicing: Network slicing partitions network resources into logically isolated virtual networks, each serving specific QoS and security requirements. Critical security pillars include performance isolation, robust slice-specific security policies preventing cross-slice breaches, and comprehensive, independent management of each slice. Mechanisms such as mutual authentication via TLS, OAuth-based authorization, and secure NAS signaling are employed to ensure the integrity, confidentiality, and control of slice operations.

While this architecture introduces unprecedented flexibility, it also brings a new dimension of security and privacy risk due to its reliance on SDN, virtualization, and multi-domain orchestration [26].

To safeguard network slices, security requirements must address the unique threats posed by logical resource isolation, slice multiplexing, and dynamic reconfiguration.

Core threats include:

1) Cross-slice attacks, where adversaries exploit one slice to access or disrupt another [26].
2) Slice-specific resource starvation, undermining performance guarantees in critical services [141].
3) Unauthorized access to slice orchestration functions, risking configuration poisoning and service hijacking [142].
4) Data leakage and inference attacks, especially at the edge where slices intersect with AI and contextual user data [21, 143].

In response, the following security and privacy requirements are essential:

1) Performance and Security Isolation: Enforce strong logical and performance isolation using SDN controllers and hypervisors to prevent lateral movement or cross-slice contamination [26].
2) Slice-Aware Authentication and Authorization: Implement slice-specific identity and access control using technologies like OAuth 2.0 and TLS-based mutual authentication [144].
3) Cross-Domain Trust Management: Enable secure orchestration across federated slice deployments with distributed trust frameworks and slice lifecycle attestation [141].
4) Edge-Aware Privacy Protection: Apply privacy-preserving AI and decentralized privacy policies (e.g., homomorphic encryption, federated identity) to protect sensitive edge-processed data [21].
5) Anomaly Detection and Risk-Adaptive Security: Employ intelligent monitoring and ML-based threat detection to identify misbehaving slices or side-channel activities in real time [142].

Emerging frameworks such as RIGOUROUS propose using slicing itself as a defense mechanism – by dynamically adapting slice boundaries and access privileges in response to evolving cyber threats [142]. However, open research challenges remain in balancing security enforcement with dynamic reconfigurability and ensuring privacy compliance across multi-stakeholder infrastructures [143].

The architectural layer threats arising from different enablers of 6G networks are summarized in Table III.

C. Application-Layer Threats in 6G

The 6G applications have very demanding performance requirements, which are provided by highly complex applications with highly malicious actors in the network. This leads to stringent security requirements in these networks. To understand the security and privacy threats in these applications, we discuss the threat landscape for digital twins, distributed learning, V2X, and IoE networks. Although these applications are not enabling technologies, it is necessary to identify and find countermeasures for making these applications secure and resilient, which finally makes them enablers of secured 6G technology.

1) Digital Twins: In response to the rapidly evolving demands driven by emerging applications such as autonomous vehicles, smart healthcare, XR, and intelligent industrial systems, the wireless communication landscape is undergoing a significant transformation. These applications collectively represent the IoE, requiring mMTC, URLLC, and considerably higher data rates, surpassing the capabilities of existing 5G networks [145, 146]. Consequently, the evolution towards 6G envisions the integration of communication, computation, and sensing into a unified and intelligent network framework.

Within this evolving paradigm, Digital Twin (DT) technology emerges as a transformative enabler by providing a real-time, high-fidelity virtual representation of physical entities and processes. In the context of 6G, DTs have the potential to significantly enhance wireless systems by enabling precise simulation, real-time monitoring, predictive optimization, and adaptive control of network operations [145]. This capability becomes increasingly critical as 6G leverages higher frequency bands, such as mmWave and terahertz (THz), which exhibit susceptibility to environmental factors, signal attenuation, and propagation uncertainties [147]. DTs, by continuously mirroring real-world conditions, can dynamically adjust system parameters, optimizing network reliability and reducing latency in highly variable environments [148].

The integration of DTs within wireless communication systems addresses several core operational challenges. Firstly, DTs facilitate the proactive simulation of network behaviours prior to physical deployment, enabling system validation, performance prediction, and optimized resource allocation. Secondly, DTs support real-time fault detection and predictive maintenance by continuously analyzing data streams from physical network components. Finally, DT-based virtual testbeds allow rapid evaluation and refinement of novel communication protocols, network configurations, and operational scenarios in a safe, controlled, and scalable environment [149].

Moreover, DT technology enables intelligent orchestration of complex 6G networks, particularly beneficial in areas such as network slicing, edge computing integration, and adaptive antenna configurations [150, 147]. For instance, DTs can simulate various slicing strategies to optimize quality-of-service (QoS) guarantees and dynamically allocate resources in virtualized networks [148]. Additionally, DT-driven models significantly improve spectrum management and interference mitigation, particularly in dense deployments typical of smart cities and industrial environments. Additionally, ultra-dense networks (UDNs) and emerging paradigms like Open Radio Access Networks (Open RAN) introduce architectural and operational complexity. While Open RAN fosters flexibility and vendor neutrality, it also increases integration challenges and potential vulnerabilities [151]. DTs provide the system-level visibility and control necessary to ensure performance and security across heterogeneous and dynamic environments.

As DTs become integral to the realization of intelligent and connected 6G networks, ensuring their security and privacy is critical. The extensive use of DTs, coupled with their real-time data dependency, significantly increases the potential attack surface, demanding stringent security measures. The remaining section identifies major threats related to the integration of digital twins within the 6G ecosystem and outlines the key security requirements necessary to counteract or prevent these threats. The complex DT-driven 6G ecosystem introduces numerous sophisticated threats, some of which are specifically amplified by emerging technologies. Using the three-layered architecture discussed in [152], the DT system in 6G can be composed of three main layers: the Physical Space (PS), the Intermediate Layer, and the Digital Space (DS). Each layer faces distinct vulnerabilities and summarized as below: The Physical Space (PS) Layer represents the foundational tier of DT architecture, responsible for real-time data acquisition and control of Physical Entities (PEs) and their environments via sensory devices [152]. It also executes commands received from higher layers and ensures data validation and quality assurance. Given its direct interaction with the physical world, the PS Layer is highly vulnerable to a wide range of security threats that can compromise DT accuracy and reliability. These threat includes:

(a) Data Acquisition Threats: Multiple attacks target the data collection process, including data tampering, software-based exploitation, physical damage to sensors, sensitive data exfiltration, Sybil, eavesdropping, objective replication, MITM, and impersonation attacks [152]. These attacks can degrade data integrity, delay system responses, or allow malicious command injections.

(b) Data Validation and Quality Assurance Threats: Adversaries may intentionally inject low-quality or unauthenticated data to disrupt the consistency and fidelity of virtual representations in the digital space. This degrades model accuracy, operational reliability, and simulation capabilities [152, 153].

The Intermediate Layer (P2D) is a pivotal conduit between the PS and DS layers in the DT architecture. It manages data synchronization, aggregation, analysis, and decision feedback, primarily via Physical-to-Digital (P2D) communication [152]. Due to its central role, this layer is exposed to multiple security and privacy threats affecting system accuracy, confidentiality, and resilience. The potential threats are summarized as:

(a) Desynchronization Attacks via P2D Communication: Attackers may interfere with synchronization frequency or packet timing to break consistency between the physical and digital spaces. In ultra-low-latency environments enabled by 6G, even minor disruptions can lead to cascading failures [153].

(b) Communication Poisoning: Attackers may inject poisoned data during P2D updates, compromising the reliability of predictions or control signals sent back to the physical system [146].

The Digital Space (DS) Layer represents the highest tier of the DT architecture, where PEs are mirrored as Virtual Representations (VRs). Drawing data from the Intermediate Layer or directly from other VRs, this layer facilitates visualization, behaviour, monitoring, decision-making, and inter-VR communication [152]. As the core of intelligent operations, the DS layer is critical for analysis and control; however, it also introduces a substantial attack surface with potential repercussions on both digital and physical domains. These attacks are summarized as follows:

(a) Evil DTs (Malicious Clones): Adversaries may create fake or cloned VRs to impersonate legitimate digital twins, relay incorrect decisions, or silently gather sensitive data. These evil twins can disrupt system behavior without triggering alarms [154].

(b) Identity-based Attacks: Impersonation and Sybil attacks within D2D communication channels can undermine trust, mislead decision processes, or facilitate unauthorized access to shared resources [155].

(c) Free-Riding and Model Exploitation: Selfish or compromised VRs may consume DS services without contribut-

ing meaningful information, undermining collaborative intelligence and potentially skewing distributed learning models [145].

(d) Quantum Hacking Threats: With quantum computing advancements, attackers may exploit quantum algorithms (such as Shor's algorithm) to decrypt traditionally secure communication channels between DT entities and network nodes, severely compromising sensitive information and undermining data security assurances [154].

(e) AI-driven Adversarial Attacks: Malicious entities could leverage AI-based attack vectors, including adversarial machine learning and model poisoning, compromising the predictive capabilities of DTs. Such attacks can mislead decision-making processes or degrade network performance, severely impacting system reliability and accuracy [154, 155].

(f) Unauthorized Access and Privilege Escalation: Weak access control policies could allow attackers to gain unauthorized entry into DT systems, enabling them to manipulate sensitive operations or extract confidential data, leading to compromised system integrity [155].

(g) Synchronization and Timing Attacks: Disruptions in synchronization between DT and their physical counterparts through timing manipulation or communication interference could lead to inconsistent states, causing operational failures or unsafe conditions, especially in latency-critical 6G applications [154].

(h) Denial-of-Service (DoS) Attacks: DT systems require continuous availability; thus, DoS or DDoS attacks can critically disrupt services by overwhelming computational or communication resources, severely impairing system availability and reliability [156]. The integration of DTs with 6G networks unlocks immense potential but also introduces amplified risks due to the characteristics of ultra-low latency, AI-native intelligence, and massive connectivity. DTs must be designed with built-in security features across all architectural layers, addressing both inherited and emergent threats. Ensuring secure communication between physical and digital spaces, defending against evil digital twins, resisting quantum threats, and enforcing zero-trust access are essential steps toward realizing secure, resilient, and scalable digital-twin-enabled 6G systems. The successful deployment of DT technology within 6G networks necessitates addressing several stringent security requirements:

1) **Real-Time Data Integrity:** DTs heavily depend on continuous data streams from physical entities, sensors, and network elements. Ensuring data integrity against manipulation or falsification is crucial to maintaining the reliability and accuracy of DT simulations and predictions [157, 158].
2) **Confidentiality and Privacy:** DTs frequently process sensitive personal, operational, and contextual data. Robust encryption and privacy-preserving mechanisms must be integrated to prevent unauthorized data access and leakage, protecting user identities and operational secrets, particularly in healthcare and critical infrastructure scenarios [145].
3) **Quantum-Resistant Encryption:** The anticipated advent of quantum computing poses a significant risk to current cryptographic standards employed in DT data streams. Thus, DT-based 6G networks must integrate post-quantum cryptographic techniques to ensure resilience against quantum-enabled hacking attacks targeting sensitive communication channels [159, 152].
4) **Secure P2D and D2D Communication:** DT systems depend on continuous, high-fidelity communication across multiple layers. P2D links must be protected against tampering or delay to preserve synchronization between physical entities and their virtual counterparts. D2D links, used for coordination among virtual resources, must guarantee confidentiality and integrity to prevent model poisoning and data leakage [160].
5) **Secure Synchronization Protocols:** Synchronization between physical systems and digital models must be robust against delay injection, desynchronization, and replay attacks. Protocols must preserve consistency and integrity despite adversarial attempts to forge or delay updates [145].
6) **AI-Driven Adaptive Security:** With AI being a core enabler of both DTs and 6G, adversaries may exploit ML models through adversarial samples or model inversion. defense mechanisms must include real-time threat detection using federated or continual learning to adapt against evolving attack patterns [146].
7) **Zero-Trust Architecture:** The pervasive nature of IoT and edge devices within DT frameworks requires strict access control policies under a zero-trust model. By rigorously verifying device identities and continuously validating trustworthiness, zero-trust architectures significantly reduce risks related to unauthorized access, privilege escalation, and supply-chain compromises [153].
8) **Data Quality Validation and Provenance Assurance:** Given 6Gs massive data throughput and real-time constraints, DTs must enforce strict data validation and provenance checks at the edge to detect injected, redundant, or low-quality sensor data [145].

2) Distributed Learning: Distributed learning is a decentralized paradigm in which multiple clients collaboratively train machine learning (ML) models without transferring their raw data to a central server. Among various distributed learning approaches, FL is positioned as a critical enabler for security-centric intelligence in 6G networks as shown in Figure 10. In contrast to traditional centralized learning paradigms where data from diverse sources are aggregated on a centralized server, FL facilitates collaborative model training directly at the edge nodes (ENs), preserving local data privacy and significantly reducing communication overhead [161]. Given the envisioned ultra-dense connectivity, ubiquitous intelligence, and stringent latency requirements of 6G communication systems, FL emerges as a promising solution to securely leverage distributed, heterogeneous datasets generated at network edges, such as IoT sensors, autonomous vehicles, smartphones, and industrial endpoints [162, 22].

The drive to implement FL in 6G networks arises mainly from the need to utilize abundant edge-generated data while adhering to privacy requirements and respecting data protection regulations, such as the GDPR [163]. By keeping raw

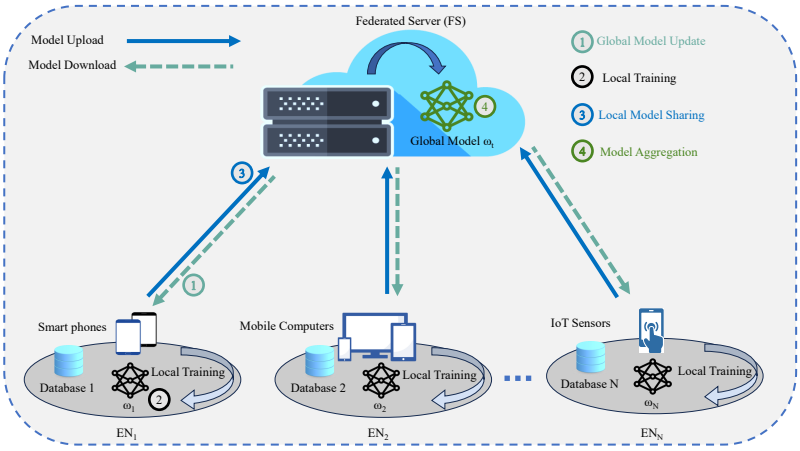

Figure 10: The generic framework and training process of FL.

data confined to local devices and transmitting only model updates, FL mitigates risks associated with data breaches and unauthorized access, offering privacy by design and robust security in collaborative 6G-enabled learning ecosystems.

Despite these benefits, the decentralized and large-scale nature of FL introduces significant security and privacy challenges. The following section outlines key security requirements and analyzes the threat landscape of FL when deployed in 6G networks. FL, despite inherently preserving data privacy by design, is not immune to critical vulnerabilities and security threats, particularly within the context of future 6G networks. The unprecedented scale, ultra-high density, dynamic heterogeneity, and stringent latency requirements envisioned for 6G significantly amplify existing FL vulnerabilities. As billions of diverse edge nodes, including smartphones, IoT sensors, autonomous vehicles, and industrial devices, collaboratively engage in distributed intelligence, potential adversaries gain increased opportunities to exploit security gaps, compromise model integrity, or breach privacy protections [164, 165].

In particular, 6G use cases ranging from semantic sensing and digital twins to autonomous vehicular systems and ultra-dense IoT introduce sensitive and mission-critical data flows that are frequently processed at the edge [23, 166]. In such contexts, FL becomes susceptible to both performance degradation attacks (e.g., poisoning and backdoors) and privacy breaches (e.g., gradient leakage and model inversion), which can compromise the integrity, availability, and confidentiality of the global model [167]. Broadly, adversarial attacks in FL can be classified into two main categories, i.e., performance attacks and privacy attacks [23, 168]. Performance attacks aim to degrade model accuracy or robustness, while privacy attacks seek to infer sensitive information from model updates. Understanding these attack types and their operational mechanisms is crucial for implementing effective defenses in FL systems.

Therefore, effectively understanding these vulnerabilities within FL becomes vital for securing 6G ecosystems, where reliability, privacy preservation, and robustness are fundamental to the envisioned intelligent, ultra-connected digital future. This subsection explores the critical privacy and security vulnerabilities of FL in the context of 6G networks. We highlight essential privacy challenges and the need to protect client data in untrustworthy environments.

Performance attacks primarily aim to degrade the predictive capabilities, accuracy, or robustness of FL models. Within the context of 6G's heterogeneous edge ecosystems, two prominent performance attacks include data poisoning and model poisoning.

1) **Data Poisoning Attacks:** In a 6G scenario, data poisoning refers to the injection of malicious or erroneous data by compromised edge nodes. An adversary may strategically participate as a legitimate client and insert the manipulated data in the training set. A common example is label flipping, where attackers intentionally mislabel data samples, causing incorrect model generalizations without altering the model architecture itself [169, 170]. Another form is the backdoor attack, where attackers insert specific trigger patterns into the data to distort predictions during model deployment [171]. Such attacks are highly effective within the large-scale, distributed setting of 6G networks, where detecting subtle, localized manipulations becomes increasingly challenging due to massive participation and data heterogeneity [172].
2) **Model Poisoning Attacks:** Model poisoning involves manipulating gradient updates or parameters sent to the aggregator node or peers, directly targeting the integrity of the global model. In centralized 6G FL with edge aggregators, this attack can inject targeted or untargeted gradients that degrade performance or embed adversarial objectives, such as biased outcomes for specific inputs [173, 174]. Model poisoning is notably difficult to detect since compromised gradient updates often closely resemble legitimate contributions, complicating conventional anomaly detection methods [169, 170].

Privacy attacks exploit shared model updates to infer sensitive data used by participating nodes. Given the sensitivity of data handled by 6G-enabled applications such as healthcare, autonomous systems, and personal devices, these threats are especially critical.

1) **Model Inversion Attacks:** These attacks attempt to reconstruct private client data from shared model parameters

or gradients. In the 6G context, adversaries can leverage advanced generative adversarial networks (GANs) and reconstruction algorithms on intercepted model parameters to closely approximate sensitive datasets, posing severe privacy risks in critical sectors such as telemedicine and smart city surveillance [175, 176].

2) **Membership Inference Attacks:** Membership inference attacks aim to deduce whether specific data instances were used in training by analysing gradient updates or aggregated parameters. Such inference can inadvertently reveal sensitive individual-level information, significantly breaching privacy in 6G environments characterized by pervasive data collection, such as personal health monitoring or financial applications [177].
3) **Gradient Leakage Attacks:** Gradient leakage involves exploiting information within gradients shared during FL training rounds. Attackers can reconstruct sensitive information from gradients, particularly when the number of participating devices is limited or data diversity is high, making this attack particularly potent in the sparse or selectively connected 6G edge scenarios [177]. Privacy-preserving methods, including differential privacy or gradient perturbation, are essential to mitigate these attacks.

To ensure the secure, resilient, and privacy-preserving deployment of FL in 6G environments, the following requirements must be satisfied:

1) **Data Privacy Preservation:** FL must ensure that client data remains confidential and cannot be inferred from model updates. DP and gradient perturbation are essential for minimizing leakage [178].
2) **Secure Aggregation and Model Sharing:** Communications between clients and aggregators must be encrypted and resilient to inference attacks. Protocols like Secure Multi-Party Computation (SMPC) and Homomorphic Encryption (HE) enable privacy-preserving model aggregation without exposing sensitive intermediate data [179].
3) **Resilience to Malicious Clients:** The presence of untrustworthy or compromised clients necessitates robust aggregation strategies capable of identifying and mitigating Byzantine behaviour (e.g., poisoning attacks). Techniques such as Krum, Trimmed Mean, or clustering-based anomaly detection are essential [23].
4) **Post-Quantum Security:** With the advancement of quantum computing, traditional cryptographic protocols may become obsolete. FL systems must integrate quantum-resistant algorithms to ensure long-term confidentiality of model updates and aggregation operations [159].
5) **Authentication and Trust Management:** Client identity must be verified to prevent Sybil and impersonation attacks. Blockchain or zero-trust frameworks can enhance trust across decentralized networks [153].
6) **Scalability and Communication Efficiency:** Given the expected scale of 6G edge networks, FL must minimize communication overhead. Model compression, update sparsification, and asynchronous training can significantly reduce the bandwidth requirements and energy consumption of distributed training.

The impact of adversarial threats in FL within 6G networks significantly varies based on the complexity, type of attack, and attacker resources. Given the above challenges, preserving privacy and security within FL-enabled 6G systems requires achieving three fundamental objectives: (a) minimizing information leakage, (b) ensuring data confidentiality, and (c) maintaining the integrity of distributed model training.

1) **Minimizing Information Leakage:** Preventing adversaries from reconstructing sensitive information by limiting inference potential from shared model updates through DP, which injects controlled noise to safeguard privacy without sacrificing utility significantly [178].
2) **Ensuring Data Confidentiality:** Protecting sensitive client data during aggregation or transmission. Techniques like Secure Multi-Party Computation (SMPC) and Homomorphic Encryption (HE) enable secure computation on encrypted data, minimizing the exposure of raw data in untrustworthy environments typical in decentralized 6G scenarios [179].
3) **Maintaining Learning Integrity:** Securing the FL training process from compromised updates. Robust aggregation methods, including anomaly detection and secure weighted aggregation, are vital for maintaining model reliability in the adversarial landscape anticipated for 6G networks.

3) AI Agents: AI agents are software entities that are capable of autonomously and iteratively performing tasks and making decisions based on pre-defined inputs in dynamic environments. Large language models (LLMs) functioning as the "brains" are integrated onto AI agents which give them the capability to interact iteratively with changing environments, perceive feedback and come to decisions in real-time. The AI agents are either LLM-based or RL-based agents, and these two categories of agents form a comprehensive framework of AI agents that complement each other, where LLMs are involved in multimodal reasoning and planning while RL lead to adaptive decisions and dynamic improvements. Although there has been considerable progress in the development of algorithms to execute tasks that involve AI agents, the security and privacy vulnerabilities and safeguarding measures related to them have been less explored.

Threats on AI Agent System: The threats associated with AI agent systems can be categorized into (a) RL-related risks and (b) LLM-related risks. The RL-related threats for AI agents are unintended behaviours arising from dynamic states and actions that originate from external dynamic feedback in an AI Agent System. These unintended behaviours include undesired, unsafe and unethical outcomes in the security and privacy of these systems. Some of the security-related issues include poisoning attacks, imperceptible perturbations that influence reward functions to act in a way that creates anomalies in the system. Among privacy attacks on AI agents, attackers use inverse RL to derive the reward functions and perform further security attacks. Detecting these attacks is more challenging because, unlike attacks on LLMs, the target consists of the reward functions, which are characterized by numerical signals, making it difficult for humans to detect. In LLM models, the brain module within the AI agents

is responsible for reasoning, planning and decision-making. However, the AI agents suffer from reduced trustworthiness due to less transparency, backdoor attacks [180], misalignment [181], hallucination [182] and planning threats [12] in the form of erroneous plans resulting from complex and long-term planning of tasks. These threats are addressed as LLM-related risks in the AI agent system.

Furthermore, based on their source positions, the threats to AI agents can be classified into (i) intra-execution threats, and (ii) interaction threats. Intra-execution represents the internal functionalities of a single AI agent architecture and includes the three key processes of perception, brain, and action. Attacks due to perception mainly refer to attacks due to prompts in AI agents, which are also called adversarial attacks. These include the prompt injection attacks and jail breaks. Threats on brain include backdoor, misalignment, hallucination and planning attacks. The invisible yet complex processes of internal executions in AI agents, which makes monitoring of internal states challenging and vulnerable to security threats, are called actions. The threats on action can be categorized as either Agent2Tools threats [12] or supply chain threats [183]. Interaction threats are of the following kinds.

(a) Threats on Agent2environment: These are threats due to the interaction of AI agents with the environment. These threats arise from dynamic and backward passes, where evolving states or adversarial feedback manipulate the agents toward taking unintended actions that are designed by the attackers. Some of the key environment attacks are indirect prompt injection attacks, threats due to RL environment, threats due to physical environment, threats due to Simulated and Sandbox environment, threats due to computed resources management environment etc..

(b) Threats on Agent2Agent: In a multiple-agent AI system, several agents work collaboratively to achieve more complex objectives and superior problem-solving capabilities than single-agent systems. However, they increase the threat surfaces to AI agents. The two kinds of threats these interactions could create are cooperative interaction threats and competitive interaction threats.

(c) Threats on Memory: The interaction between memory and AI agents during the processing of agent usage can introduce security threats, which need to be carefully managed. These threats are classified into short-term memory threats and long-term memory threats. Short-term memory attacks are due to the limited working memory capacity constraint of AI agents that prevents complex sequential reasoning and knowledge sharing in multi-agent systems. Long-term memory relies heavily on vector databases for storage and retrieval. Some of the threats that long-term interactions can lead to are the injection of poison samples into the vector database by the indexing process, embedding inversion attacks that reconstruct and extract private information stored in the long-term memory, and generation threats against hallucinations and misalignment.

Security and Privacy Requirements: Based on the threat surfaces on AI agents as explained earlier, the following requirements will be necessary to counteract the risks associated with these systems.

(a) **Prevention and detection-based strategies:** The prompt injection attacks can be counteracted using prevention-based strategies and detection-based strategies. Prevention-based strategies include paraphrasing, retokenization [106], use of delimiters [184], employ layered defense such as sandwich prevention [185], appending extra instructions to neutralize injected instructions. On the other hand, detection-based strategies are calculating perplexity (PPL) [186] to identify anomalies, analyzing text in smaller windows for localized issues [106], leveraging the brain component, for naive detection, validating responses against task requirements [187], and using known-answer instructions [12] to confirm adherence to the intended task.

(b) **Enhance robustness of LLMs:** Jailbreak attacks due to weak robustness of AI agents, especially due to LLMs, can be mitigated using input and output filtering [188] that enhances the robustness of LLMs. However, these methods lead to high computational overhead and utility of the model getting reduced.

(c) **Alignment strategies:** Hallucination attacks can be counteracted through alignment, collaborations among agents, RAG, post-correction of hallucinations, and internal constraints. The alignment of AI agents is achieved through supervised methods such as fine-tuning Reinforcement learning from Human Feedback (RLHF).

(d) **Prevention of planning attacks, Agent2Tool passive threats and supply chain threats:** Planning attacks in AI agent systems can be prevented by establishing policy-based constitutional guidelines and human users constructing a context-free grammar (CFG) as the formal language to represent constraints for the agent. The passive mode threats in Agent2Tool are more challenging to defend, because these attacks are usually the outcomes of the AI agent's incomplete development and testing. Moreover, supply chain threats can be handled by implementing stricter supply chain auditing policies and policies for agents to use only trusted tools.

(e) **Prevention of indirect prompt attacks:** The developers can prevent AI agents from executing external harmful data by explicitly imposing constraints on the interaction between AI agents and external entities. The prompt injection attacks can also be mitigated by enabling the AI agents to enhance their ability to spot external input sources. This can be done by the use of secure and insecure tokens, data marking, encoding, fine-tuning AI agents for indirect prompt injection, prompt engineering, and post-training classifier-based security approaches.

(f) **Prevention of RL-related attacks:** The RL-related attacks can be mitigated using methods such as differential privacy, cryptography and adversarial learning.

(g) **Enforcing ethical guidelines:** Rigorous ethical guidelines and mechanisms to ensure the responsible use of simulated environments in AI agents are essential to counter these threats

(h) **Ensure reliable execution through reliable hardware and software:** To counter AI agent-related threats, the

safety and security of the hardware and advanced processing of data are critical to avoid or minimize incorrect actions that might cause irreversible harm.

4) V2X Networks: The successful integration of 6G connectivity with the Intelligent Transport System (ITS) promises to create a future of highly efficient, well-connected, well-coordinated and safe mobility networks. 6G V2X will support a communication network with high mobility and low latency enabling a comprehensive communication network consisting of Vehicles-to-Vehicles (V2V), Vehicles-to-Infrastructure (V2I), Vehicles-to-Pedestrians (V2P), and Vehicles-to-Networks (V2N) communications.

However, necessary advancements in V2X technologies are required as it will act as an enabling technology in pace with the 6G era. Due to factors like urbanization, advancement in technologies and higher standards of living, it is expected that there will be a rapid growth of autonomous vehicles in 6G V2X networks, which will make it necessary for these networks to become ubiquitous and more intelligent compared to the previous generation of networks. Moreover, due to the rising demand for emerging services in V2X communications such as 3D displays, holographic control displays, immersive entertainment, wireless brain-vehicle interfacing, and advanced in-car information, etc. the capacity and performance limits of these networks will be more challenged than before [189]. The 6G-V2X networks are envisioned to evolve into new paradigms of Internet of Vehicles (IoV), Connected Autonomous Vehicles (CAVs), Internet of Vehicles (IoV), Intra-vehicular communication, and V2V communication, where it will be necessary for the future vehicles on the road to be equipped with additional functionalities of precise sensing, enhanced computing, communication, self-learning intelligence, control, storage, and the capability to support ultra-reliable, hyperfast, ultra-low latency massive data exchanges [112]. To achieve these goals, advancements in the areas of communications, computation, and security related to V2X networks are necessary. Some of the main security threats in 6G V2X are expected to be due to current limitations in connectivity and computational performance, and the unpredictable nature of these attacks [190]. For e.g., although over-the-air software updates for protection against real-time attacks are being increasingly standardized, most vehicles fail to receive timely updates on their onboard systems, which makes them prone to new security assaults. The vehicles' limited computational performance is another drawback in these networks that makes them more vulnerable to security attacks as compared to computers/ devices with high computational and processing capabilities. There are different points of entries in a V2X systems where the hackers can attack in the next moment, because of which it is difficult for vehicular manufacturers to predict these attacks in advance [24]. In 6G V2X networks, in addition to Dedicated Short-Range Communications (DSRC) and cellular-based C-V2X technologies that were used in the previous generation V2X networks, the incorporation of new frequency bands such as mmWave, optical bands and quantum communications will create more attack surfaces [191] than before.

Next, we discuss a few attack scenarios based on the CIA[3] (Confidentiality, Integrity, Availability, Authentication, and Access Control) model-based security analysis that will arise in 6G V2X networks. Some of the pertinent threats in these networks would be,

(a) Confidentiality-related Attacks: In V2X networks, some of the threats related to compromising confidentiality in such networks are eavesdropping [192] and sniffing [15]. By compromising confidentiality in V2X networks, the attackers can access user identity and/or track their moving location information, and use this information for malicious intents such as stalking or physical attacks [193]. Some of the confidentiality-related threats expected in 6G V2X networks are According to ITU the standards that have been defined as requirements for countering confidentiality attacks are (a) prevent sharing of information between vehicles, vehicles and infrastructures, vehicles and road users, with unauthorized users and (b) inability of any unauthorized entity to extract and reveal the identity of the concerned individual from any personal identifiable information they might get access to. Due to the heterogeneity of involved networks and the application of novel techniques such as AI, quantum computing [189], etc., ensuring confidentiality in 6G V2X networks is expected to be extremely complex and highly challenging. Some of the solutions to preserve confidentiality in V2X networks are anonymization [194], pseudonymization [195], using information other than personal information for identification. For security and privacy guarantees in 6G V2X networks, attribute signatures, Multi-Receiver Encryption (MRE), and message authentication code for authenticating users can be used jointly [189]. However, using technologies like MRE would need to meet the challenge of increased processing and network bandwidth capabilities of the network. Other attacks that can be a threat to data confidentiality in V2X systems are physical attacks, which can be counteracted using physical layer security mechanisms [196].

(b) Integrity-related Attacks: Ensuring the reliability and accuracy of data exchanged in V2X communications is necessary for the safety and effectiveness of V2X communication systems, and any tampering of data could lead to potential accidents and system failures in V2X networks [189]. Some of the threats compromising integrity in V2X networks are message tampering [197], timing [198], replay [199], and bush telegraph. In 6G V2X networks, it will be necessary to verify the integrity of real-time sensor data and detect and localize any tampering of data. Blockchain-based multi-layered data integrity frameworks can store secure and tamper-proof data in a decentralized and immutable ledger [200]. Such frameworks would, however, be computationally expensive and would need to achieve interoperability among various protocols. Future networks must design evolved digital signatures for V2X networks to resist attacks such as brute-force attacks [201], side-channel attacks [202], or other quantum computing-based attacks, which are generally expected to be prevalent in 6G networks and able to decode any traditionally encrypted techniques of protecting the integrity of data [198]. Another important aspect is the standardization of protocols and data formats in the context of data integrity and interoperability to support the increasing number of diverse devices that

might participate in V2X networks. Additionally, 6G NR V2X communication standards [189] developed for 6G networks will require that the design of this new standard for V2X networks ensures real-data transmission and their reliability and security.

(c) Availability-related Attacks: In terms of availability, ensuring real-time data transmission and high network availability in 6G V2X communication systems will ensure that the real-time data is accessible and usable. Some of the threats towards availability in V2X networks are DoS, malware, and blackhole attacks [17]. 6G networks are expected to include new technologies such as Non Orthogonal Multiple Access (NOMA), RIS, and intelligent beamforming, which will help attain the future generation QoS in terms of data availability. However, these networks will have to handle high-speed, reliable communication services among vehicles and roadside units. To maintain data availability in such time-critical and high-mobility environments, it is essential to incorporate redundancy and fault-tolerant mechanisms to handle failures of devices/parts of the network and minimize downtime [203]. QoS mechanisms are essential to incorporate in 6G V2X networks to ensure that time-critical applications such a collision avoidance are prioritized. Moreover, ubiquitous real-time monitoring techniques are necessary to support the growing number of users and handle increasing volumes of data exchanged without compromising the availability of data. Finally, the V2X networks must be resilient to interference from other wireless networks and environmental obstacles.

(d) Authentication-related Attacks: The authentication-related attacks that can arise in 6G V2X networks are sybil [204], wormhole [205], and masquerade attacks [24]. The authentication mechanisms in 6G V2X must be designed to incur minimum delay to ensure that data is transmitted in real-time. The authentication mechanisms must protect the data and key distribution while maintaining anonymity and resistance to protocol attacks. It will be more challenging in 6G networks because the authentication mechanism must be scalable and interoperable with heterogeneous networks involved. Due to the limited computational resources of vehicles/devices involved in V2X networks, the designed authentication mechanisms need to be resource-efficient and lightweight. Lightweight cryptographic algorithms, secure key management, and adoption of digital signature certificates are some of the techniques to authenticate data and ensure tamper-proof data transmission in future V2X networks. Blockchain technology and aggregated signatures could be used individually or together for batch authentication in 6G V2X networks [206]. However, implementing aggregated signatures is complex and creates performance overhead due to more computation and communication necessary for the collection of signatures, which will affect the system's authentication performance as a whole.

5) Internet of Everything (IoE) networks: 6G networks will potentially enable emerging disruptive massive IoT applications that are beyond the capabilities of 5G networks due to their inherent limitations. The 6G networks are expected to support a wide array of devices, and the rapid proliferation and interconnection of a massive number of 6G-enabled IoT devices will likely lead to increased security and privacy vulnerabilities [207]. Some of these potential threats are discussed below.

(a) Lightweight security framework: A significant proportion of 6G IoE devices is expected to comprise ultra-low power and zero power products where energy is harnessed from the device's surroundings. These devices have very limited resources in which to implement security mechanisms that typically require computational complexity [30]. Consequently, there is a need to develop a lightweight security framework with minimum or zero power consumption that will protect network communication between devices. The challenge is to ensure the framework offers trustworthy access and data authorization mechanisms, despite device limitations. The framework should protect any data transmission from interception, manipulation, or interference by an attacker and offer defenses against spoofing and replay attacks. New more energy-efficient security mechanisms will be needed.

(b) Multi-Party Trust Model: 6G offers an open, distributed IoE network, integrating multiple domains and entities; unfortunately, the security of the network's channel is not guaranteed. A new security authentication scheme is required that applies the zero-trust model. According to NIST, the meaning of "trustworthiness" in 6G telecommunications is composed of five aspects: security (confidentiality, integrity and availability), privacy, reliability, resilience and safety. A three-way trust model exists between access devices, users and operators, evolving into a multi-party trust model that includes multiple terminals, multiple users and multiple network access nodes.

(c) Data protection and user information privacy: The evolution of 6G connection technologies is enabling data transmission protection capabilities to migrate down from the higher stack layers in order to achieve improved security. However, the focus on security protection is moving to that of protection of data and its privacy. This shift in focus is due to the security requirements of new services. Unauthorized access or eavesdropping of services on IoT devices in IIoT and intelligent logistic scenarios could result in loss or compromise of essential service information, potentially resulting in exposing sensitive and private data, violating privacy or damaging businesses. Recognizing data protection and privacy as integral elements of the network architecture is crucial, requiring development of frameworks that address data protection needs at every layer of the network stack. With the anticipated use of AI in the majority of 6G sub-systems using data for network optimization and performance enhancements etc, ensuring compliance with data protection regulations such as GDPR will be challenging.

(d) Intelligent orchestration of security features to support dynamic and diverse services: In order to support intelligent security policies and to orchestrate the policies flexibly and dynamically, careful consideration should be given to the 6G security architecture. The architecture should be able to configure security functions intelligently in order to meet the security requirements of diversified subsystems, applications, and services and to protect data assets. Importantly, the intelligent security architecture should be based on zero trust. OPPO [30]

TABLE IV: Summary of Application-Layer Threats and Security Requirements in 6G Networks

Technology	Purpose / Use	Key Threats	Security Requirements / Countermeasures
DTs *[152], [153], [146]*	Real-time mirroring of physical entities for simulation and control	Data tampering, desynchronization, evil twins, AI and quantum attacks, impersonation, DoS	Zero-trust access, secure P2D/D2D communication, post-quantum encryption, provenance validation, adaptive AI-based security
DL *[164], [165]*	Distributed model training without data centralization	Data/model poisoning, model inversion, membership inference, gradient leakage	Differential privacy, secure aggregation (SMPC, HE), robust aggregators (Krum, Trimmed Mean), post-quantum resilience
Agentic AI *[180], [12]*	Autonomous performance and decision making decisions in dynamic environments	Security attacks like poisoning attacks, imperceptible perturbations, and reduced trustworthiness	Prevention and detection-based strategies such as calculation of PPL, retokenization, sandwich prevention
V2X Networks *[190], [24], [191]*	Vehicle-to-everything communication (V2V, V2I, V2P, V2N)	Eavesdropping, spoofing, replay, DoS, integrity tampering, Sybil and masquerade attacks	Lightweight cryptography, blockchain-based integrity, pseudonymization, message authentication, redundancy, QoS guarantees, aggregated signatures
IoE *[207], [30]*	Ultra-connected 6G ecosystem with low-/zero-power devices	Spoofing, replay, interception, user privacy compromise, limited device resources	Lightweight security design, multi-party trust models, zero-trust architecture, privacy-aware data protection at all layers

suggest three core components for the architecture; a SPE for developing security policies, a SPEP component for providing differentiated security capabilities for each subsystem, and a SPA for establishing a communication path between SPE and SPEP and to provide input and output.

The application layer-related threats are summarized in Table IV.

D. Quantum Threats in 6G

With the advent of 6G, there will be an exponential increase in speed and volume of data flowing across, accompanied by highly complex applications running on these networks in real-time. This will create vast amounts of sensitive data to flow through these networks. Moreover, due to the distributed and disaggregated composition of 6G networks, data processing will occur both at the Cloud and at the network edges. As a result, points with security vulnerabilities that can cause catastrophic consequences on the system are expected to increase to a much larger extent. The current 5G networks use cryptographic tools which are vulnerable to future quantum attacks. To protect these systems and the sensitive data flowing across them, quantum-resistant security in 6G networks is essential, which is capable of securing data against both classical and quantum adversaries [208].

Quantum-resistant security is a security framework to counteract against quantum attacks which originate from quantum computers. Quantum computers can solve computational problems much faster than classical computers. Although the rapid development of quantum computers will improve computation in future networks, they will also be capable of breaking the current security protocols of telecommunication networks. for e.g., the Shor algorithm [209] can potentially compromise popular public key cryptography systems essential for authentication such as the asymmetric key cryptography method Rivest-Shamir-Adleman (RSA), Elliptic-curve cryptography (ECC) or Diffie-Hellman key exchange protocol. This can be a huge threat to the confidentiality and security of present-day security frameworks in the future. Although we don't have operational, fault-tolerant quantum computers yet, they still pose a real threat to our present networks. For instance, hackers are already involved in a process called 'store and decrypt', which refers to storing data that can't be decrypted today, but storage is done for when quantum computers become accessible so that the data can be decrypted retroactively. Enormous damage can occur, such as exposing consumer data, data related to critical communications infrastructures, or data which is required to be securely stored for a long period, such as in the case of industries such as government communications, healthcare, finance, etc.. Therefore, it is urgently necessary to find solutions to prevent and promptly counteract such attacks in 6G networks when they arise.

Some of the key aspects of future networks that are vulnerable to quantum attacks are summarized below.

(a) Authentication at the Core: The Public Key Infrastructure (PKI) is responsible for authentication at the core of wireless networks. But PKI is based on RSA and ECC, both of which are cryptographic protocols that can be compromised through quantum attacks. Therefore, this will endanger the security of every device authenticated on a 6G network.

(b) Security in Virtual Private Networks (VPNs): Traditional VPNs encryptions provide robust security for communications between core network elements and devices. However, VPNs usually use RSA or ECC cryptographic methods, which makes them potentially susceptible to quantum attacks in the future.

(c) Edge Computing: With the use of diverse and massive devices and distributed architectures in 6G networks, the application of edge computing and edge intelligence will be a defining characteristic of these networks. Therefore, data processing will be distributed across a massive number of edge nodes, often closer to the user. These edge nodes will therefore need to be equipped with quantum-safe encryption so that the sensitive data related to end users are processed and transmitted securely.

To prepare the 6G networks for a post-quantum world, the requirements can be categorized as:

(a) Cryptographic Inventory for Quantum Risk: Cryptographic inventories need to be maintained across networks to assess each network's vulnerability to quantum attacks and prepare for a post-quantum phase. This means identifying all cryptographic assets, their locations and algorithms used, so that migration to quantum-resistant options can be executed with priority when such circumstances arise.

(b) Hybrid Encryption Models: To prepare for a quantum-resistant network which is also compatible with current networks, hybrid encryption models can be designed that combine classical cryptography with post-quantum algorithms. For e.g., the hybrid approach that uses a quantum-resistant cryptographic algorithm called CRYSTALS-Kyber for key exchange while keeping Advanced Encryption Standard (AES) for symmetric encryption. However, these approaches need to be managed carefully, especially when migration to a post-quantum environment occurs, because adversaries can exploit the weakest link.
(c) Cryptographic Agility: For adapting flexibly to new encryption standards, especially since quantum-safe algorithms are evolving, it becomes necessary to build systems that can easily switch between different encryption methods if required. This is called cryptographic agility, and it allows for a smooth and secure transition to a quantum-safe cryptography environment.
(d) Pilot Quantum-Safe Networks: Before rolling out quantum networks, it becomes important to pilot, deploy, test and evaluate their performance and compatibility, mainly focusing on critical components like the base stations, edge nodes and VPN tunnels. This will help in securing these networks and the critical infrastructures within these networks.
(e) Quantum Key Distribution (QKD): Most of the encryption needs for 6G can be handled by PQC. PQC aims to create cryptographic algorithms which even quantum computers will not be able to crack. However, QKD that applies quantum mechanics to develop unbreakable encryption keys, can potentially provide another layer of security for sensitive and/or high-priority communications

VI. Potential Technologies to Enhance Security and Privacy of 6G Networks

Based on our discussion on potential threat landscape in 6G networks in the previous section and vulnerabilities in 5G networks, earlier, we have identified a few key technologies that will potentially support in counteracting security and privacy-related threats in future networks. In this section, we discuss them in detail to explore their functional principles, use cases, and the different techniques expected to be used within their technical boundaries to handle different threats in the network. The key technical solutions considered here are the blockchains and distributed Ledgers, post-quantum cryptography, physical layer security, and federated learning.

A. Blockchains

Blockchain is a Distributed Ledger Technology (DLT) that achieves secure, efficient and transparent data interchange and value transfer through a decentralized approach of providing immutable, distributed records for user identities. Blockchains utilize a chain of blocks that store transactions securely and distributively and these transactions are stored in sequential order, cryptographically linked and cannot be undone. In 6G networks, where decentralized environments are expected to be extensively used over centralized systems, the decentralized nature of blockchains/DLTs can offer high security and reliability to the networks and thereby accommodate new use case scenarios and applications. Apart from enhancing security by incorporating network transaction records and identity verification processes into blockchains, they improve speed of transactions and creates a trust framework that mitigates the risk of data frauds and tampering. Some of the key potential benefits of using blockchains in 6G is protecting confidentiality and integrity, guaranteeing of mutual trust, high privacy preservation, enhance the communication reliability of 6G key entities and single-failure disruption prevention. The fundamental components of blockchain include distributed ledger structure, cryptographic algorithms, consensus mechanisms, and smart contracts [210]. Distributed ledgers optimized resource management which is fair, traceable and occurs in real-time. The data security can be strengthened further by using hybrid and/or lightweight encryption algorithms with key management mechanisms. Through consensus mechanisms, blockchains can enhance the network's resilience by achieving consistency of the state of the network and trustworthiness. Smart contracts enable automatic decisions and execution mechanisms, which leads to faster, more efficient management of network service response, and strict control of data access and exchange authorization.

Some of the key benefits of using blockchains/DLTs for enhancing security and privacy in 6G networks are described below.
(a) Identity Management: 6G networks will see operators joining to collaborate and offer seamless connectivity among users, which will give rise to the challenge of security authentication and authorization mechanisms for identity management among multiple trust domains. The centralized identity infrastructure in limited and trusted domain, cannot support cross-domain interoperability, diverse data protection laws, diverse certification requirements etc. Blockchain-based identity management that can create a process of verification which is mutually secured between different networks and their distinct trust domains, and allows them to operate independent of a third party of supervision [126]. Pseudo-name management and decentralized Identity management are two example scenarios that are recommended for managing identities among multiple domains in 6G networks.
(b) Security and Privacy Countermeasures: With 6G networks having features such as the requirements of extremely high reliability and massive connectivity among heterogeneous nodes, it will be necessary for these networks to have highly intelligent security countermeasures for sophisticated attackers. Blockchains/DLTs can protect the network against eavesdropping, hijacking, Sybil attacks owing to its properties of non-repudiation, transparency,immutability. Moreover, access control, authentication and accountability in such a demanding environment will be potentially ensured by executing optimal constructed smart contracts on the blockchain [15].
(c) Public Key encryption: In 6G networks, to safeguard the data transmission across the extensive set of interconnected devices from attacks such as MiTM and eavesdropping, public key encryptions are essential. It is necessary to securely manage the public keys used for security procedures because any compromise of these keys can put the entire system at risk,

leading to the attackers having unauthorized access to sensitive data and enabling them to impersonate privileged users. By providing tamper-proof blocks that establish a trust chain for public keys, blockchains/DLTs offer a decentralized platform for robust security of data transmission, along with storage and access of public keys [211].

(d) Mutual authentication: Unlike the mutual authentication method based on traditional symmetric key approach in 5G networks, the confidentiality and integrity of 6G networks can be ensured by implementing blockchain-based mutual authentication mechanisms which assures mutual trust, preservation of privacy, and countermeasures for single point of failures etc. [212]. The blockchains support various architectures that include private, public, consortium and hybrid [213]. The impact of security attacks on these architectures can vary and therefore, it is necessary to select the right blockchain for each 6G application to minimize the impact of some attacks [18].

6G networks are anticipated to be able to support a large number of heterogeneous devices and infrastructures with improved security and efficiency across a variety of resources, including spectrum, computational power, and storage [214, 215, 3]. However, a number of trust-related problems that are frequently overlooked in network designs impede this objective [216]. Building on its characteristics of decentralization, transparency, anonymity, immutability, traceability, and resilience, blockchain can foster cooperative trust between disparate network entities and enable features like trustworthy data interaction, efficient resource sharing, secure access control, privacy protection, and wireless network tracing, certification, and supervision. The capacity to create a foundation of trust without the need for centralized management is the main advantage of blockchain for 6G security. Traditional security methods depend on trusted third parties, which leads to single points of failure and frequently prevents cross-network collaboration [217]. Blockchain, on the other hand, establishes a distributed trust environment in which network entities can independently verify information. Secure interactions across heterogeneous networks owned by various operators, vendors, and service providers are made possible in 6G environments by blockchains [218]. Blockchain generates immutable records of security-related events, transactions, and conditions that all involved parties may independently confirm. While cryptographic techniques preserve the required privacy, this transparency increases security visibility. For spectrum sharing challenges, blockchain offers transparent, tamper-proof records of spectrum allocation and usage [184, 219]. This allows for effective dynamic spectrum access across several operators while preventing unauthorized access. Without any centralized coordination, smart contracts can ensure regulatory compliance and automate spectrum trading. For ultra-dense networks with massive connectivity, blockchain enables decentralized authentication and authorization systems that scale horizontally instead of depending on centralized servers. This addresses the distributed access authentication requirements identified for ultra-massive connection in 6G networks [3, 220]. In JCAS scenarios, blockchain can preserve consent registries for sensing operations and guarantee the authenticity of sensing signals. This satisfies a number of JCAS security factors, which include preventing the leakage of sensing information and authenticating the origin of sensing signals [206, 200]. For O-RAN and network slicing security, blockchain can provide secure cross-slice resource sharing while confirming and enforcing network slice isolation. Comprehensive security monitoring across dispersed network components is supported by the immutable audit trails in blockchain [221, 222].

B. Post-Quantum Security

Although 5G and 6G networks are designed for real-time performance that supports critical tasks like autonomous mobility, remote surgery, and industrial control, they often involve the continuous exchange of sensitive operational data, including command signals, status telemetry, and sensor streams[223, 3]. Even though this data is short-lived in transmission, it is frequently logged, analysed, or retained for auditing, diagnostics, or compliance, making it an attractive target for harvest-now, decrypt-later attacks[224]. In such scenarios, adversaries intercept encrypted traffic today, planning to decrypt it in the future once large-scale quantum computers become viable. This threat is driven by quantum algorithms like Shors, which can efficiently break public-key schemes such as RSA and ECC [225, 226]. Since these cryptosystems underpin authentication, key exchange, and integrity in current mobile networks [227, 228], attacking them using a quantum computer would undermine the entire trust layer. To address this, two quantum-resistant approaches are emerging: PQC, based on hard classical problems, and QKD, which ensures secure key exchange using quantum physics [229, 230, 231]. These technologies offer complementary defenses and will be further discussed in the following sections. QKD, as the the most developed application of Quantum Communications, offers a fundamentally different approach to security by leveraging quantum mechanical principles such as superposition and measurement-induced disturbance [230]. It enables two parties to establish shared symmetric keys (used for information-theoretic encryption) based on Heisenberg's uncertain principle even in the presence of quantum-capable adversaries [232, 233, 234]. QKD protocols are categorized into several families: discrete-variable (DV) QKD, including BB84 [232], decoy-state [235], and measurement-device-independent (MDI) QKD [236]; continuous-variable (CV) QKD, which utilizes standard telecom hardware [237, 238]; and twin-field (TF) QKD, which surpasses traditional repeaterless limits [239].

Advancements in integrated photonics [240, 241, 242, 243, 244], low-noise single-photon detectors [245], and quantum-dot-based photon sources [246, 247] are enhancing the feasibility of QKD, particularly for 6G systems that demand scalable and energy- efficient solutions. However, long-distance QKD still relies on trusted nodes, which are unsuitable for dynamic, federated 6G networks [248]. Overcoming this limitation necessitates the development of quantum repeaters, entanglement distribu- tion, and memory-based relays [249, 250, 251]. Recent progress includes spin-photon interfaces [252], long-lived quantum memories [253], and multi-kilometer repeater links [254]. These are motivated by ultimate bounds

like the PLOB limit [255] and guiding the development of advanced repeater-based quantum networks [256].

The maturity of QKD deployment is evident in testbeds such as SECOQC [257], the Tokyo QKD Network [258], BT's UK trials [259], satellite-based demonstrations [260], and the recent feasibility study over a 224 km undersea link between the UK and Ireland [261]. Standardization efforts are advancing through organizations like ITU-T, ETSI ISG-QKD, and ISO/IEC JTC 1 [66, 262, 67], aiming to establish interoperable and certifiable frameworks. These experimental and institutional initiatives indicate a broad momentum toward QKD as a foundational layer in secure 6G communications [263]. While QKD is already viable in high-assurance backbones, scaling it remains a priority as networks transition toward virtualized, latency-critical 6G architectures. Recent advancements include the demonstration of twin-field QKD over 600 km [264], and the development of simplified transmitters for modulator-free QKD [265].

While QKD provides long-term security grounded in quantum physics, it faces deployment challenges in large-scale 6G environments [266]. In parallel, PQC offers algorithmic alternatives to RSA and ECC, designed to resist attacks from quantum computers [267, 268, 269]. PQC includes diverse families: lattice-based (Kyber, Dilithium), code-based (Classic McEliece), hash-based (SPHINCS+), multivariate (Rainbow), and isogeny-based (SIKE) [267, 269]. NISTs selection of Kyber and Dilithium for standardization [268] has accelerated adoption, with PQC already being piloted in 5G infrastructure, VPNs, TLS stacks, and embedded IoT modules [268, 270].

However, PQC still relies on hardness assumptions and thus lacks unconditional security. To hedge against this limitation, hybrid architectures that blend PQC with QKD are gaining momentum [271, 272]. In such designs, the two techniques can run in parallel on the same network. QKD distributes symmetric keys between trusted backbone nodes while PQC authenticates, negotiates sessions, and protects traffic that reaches mobile or otherwise untrustworthy devices [272, 273]. In addition, they can be stacked on a single link, with QKD continuously refreshing payload-encryption keys and PQC supplying an independent key-exchange and signature layer, so that the compromise of either mechanism alone cannot break end-to-end security [274, 275].

Moreover, the field faces a pressing challenge: designing a coordinated migration path from current public-key systems to quantum-safe alternatives [276, 277]. Given the long operational lifespans and interdependencies of telecom and critical infrastructure, migration strategies must be risk-aware and flexible. The concept of crypto-agilitythe ability to replace cryptographic algorithms without redesigning entire systemsis therefore essential [277, 278].

C. Physical Layer Security

PLS aims to secure wireless communication at the lower physical layer by exploiting the inherent characteristics and randomness of the wireless communication channel itself, such as fading, noise, and interference, dispersion, and diversity, rather than relying solely on classic cryptographic methods [279] that assume computational hardness of one-way functions, assume eavesdroppers have limited computation power, and are implemented at higher layers. If an adversary knows keys for encryption or can invert such functions (e.g., use quantum computing),then the systems that deploy the cryptographic algorithms are not secure. To address these challenges, longer keys, and more complex key generation and management are required. All these will add up to the cost and may cause more waste of resources, but they still cannot guarantee absolute security. The extra complexity of longer keys and new algorithms will also need more computation power and add extra delay, which may make it difficult or even impossible to be deployed in resource-constrained, power-limited, or latency-sensitive devices, such as massive low-cost IoT devices in 6G.

Due to enhanced security requirements for highly diverse applications, strict QoS demands such as ultra-low latency and extreme high reliability for XR and remote surgery, highly dynamic and heterogeneous wireless networks, massive number of low-cost IoT sensor devices, and evolving threats (such as from AI/ML) in 6G, PLS is emerging as a complementary approach to add an extra layer security. PLS can resist some physical layer attacks such as spoofing, eavesdropping, and jamming (while conventional cryptography is not able to do so), can be key-less (so no complex key management), is quantum-resistant (because it is not based on computational hardness), and has low computational complexity and latency which makes it intrinsically suitable for IoT devices and heterogeneous wireless networks in 6G.

For PLS, we consider a general system model illustrated in Figure 11 where a transmitter (Alice) sends a message X^n of length n, encoded from a plaintext M, to its intended receiver (Bob) through a main channel, while Bob receives Y^n and decodes it to get a corresponding $\hat{M}$. Alice and Bob are the legitimate transmitter and receiver. At the same time, a malicious eavesdropper (Eve) receives encoded messages Z^n through a wiretap channel [280]. The link between Alice and Bob is called the Transmitter-Receiver (TR) link and the link between Alice and Eve is called the Transmitter-Eavesdropper (TE) link. PLS aims to ensure that Bob can successfully decode the signal ($\hat{M} = M$) while preventing Eve from doing so. PLS often assumes the eavesdropper has unlimited computational power (instead of computational complexity assumptions) and is based on information-theoretic security or unconditional security [281], a paradigm of security focusing on the fundamental limits of information leakage based on information theory [282]. It aims to provide security that is provably unbreakable regardless of the eavesdropper's computational resources, such as Shannon's perfect secrecy [282] (where the eavesdropper cannot gain any information by observing received signals Z^n or mutual independence between M and Z^n), weak secrecy [280] and strong secrecy [283] (or statistical independence and asymptotically secure).

PLS techniques for confidentiality. In general, PLS techniques are categorized into key-based and key-less (Signal-to-Interference-and-Noise Ratio or SINR-based) approaches [284].

Key-based PLS techniques rely on spatially and temporally

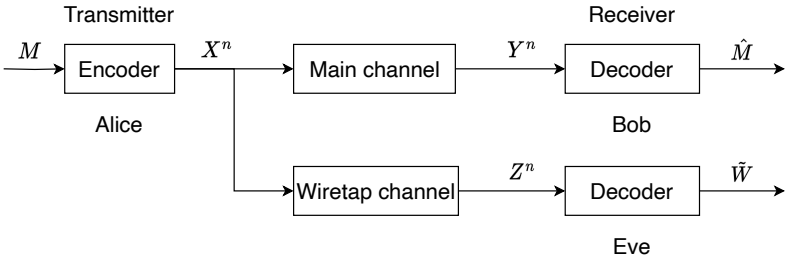

Figure 11: A general model considered in PLS.

channel decorrelation, reciprocity, and randomness (variation) in communication channel, including Shannon's pre-shared secret keys [282], secret key generation in the presence of a passive eavesdropper [285, 286, 287] or an active eavesdropper [288] even when Eve's channel is less-noisy than Bob's main channel, secure key agreement protocols [289] to use Low-Density Parity-Check (LDPC) code and multi-level coding. These work form the foundation for secret key agreement using PLS and bridged the gap between PLS and classic cryptography to use the physical layer as randomness source for secret keys. In terms of randomness source, the variations used for the key extraction include fading, interference, dispersion and noise that exists in reciprocal wireless channels; channel Received Signal Strength Indicator (RSSI), CSI, channel phases, multipath channel angles, and channel response such as unclonability in Physically Unclonable Function (PUF) [290, 291]; multiple antennas, such as MIMO, to increase common randomness for legitimate users.

Secure communication can also be achieved through a variety of Signal-to-Noise Ratio (SNR) or Signal-to-Interference-plus-Noise Ratio (SINR) based *key-less PLS techniques*. Wyner's wiretap channel model [280], where the eavesdropper's channel is (probabilistically) degraded or noisier (lower SNR) than the main channel, lays a foundation for key-less security. For 6G related wireless communication, the Gaussian wiretap channel or Additive White Gaussian Noise (AWGN) [292] is the most basic model where Alice sends a confidential message to Bob over a main AWGN channel, while Eve receives the same transmission over a separate AWGN wiretap channel. The main and wiretap channels are characterized by their respective channel gains and noise variances [293]. Other wireless wiretap channel models include Multi-Antenna (MIMO) wiretap channels [289], fading wiretap channels [289, 293], channel with partial CSI, and other more complex channel models such as non-degraded broadcast channel [294] for multi-user scenarios, multiple access channel [295] (where multiple transmitters send message to a single receiver), interfere channel [296, 297] (where multiple TR links transmit messages at the same time and interfere each other), and relay channel with trusted and untrustworthy relays [298, 299].

Key-less PLS techniques can be classified into channel code, channel adaptation, and artificial injection (of noise, jamming, and interfering) [284, 300]. Error correction codes, LDPC codes [301], lattice codes [302], polar codes [303], and spread spectrum coding [304, 305] are some investigated channel code schemes. Adaptation techniques include adaptive coding and modulation, optimal power allocation, beamforming, precoding, antenna selection, waveform and pulse shaping, and adaptive interleaving etc. Artificial injection uses noise [306, 307] or jamming [308, 309] interference to make the condition of TE links worse while not affecting the TR links. Injection methods can be time-domain, frequency-domain, or space-domain based [284, 300].

PLS for authentication, identification, and availability. While a large amount of work in PLS target at confidentiality, the PLS techniques to achieve authentication, identification, and availability have also received considerable attention to verify the identity of communicating entities by exploiting the inherent properties of the physical layer. The majority of work leverage the uniqueness and reciprocity of the wireless channel between two legitimate parties to verify their identities such as CSI [310], Received Signal Strength (RSS) (similarity and temporal variation based [311]), and location [312]. Hardware characteristics can also be used to identify users or devices such as RF fingerprinting [313] and PUF [314]. Identification and authentication can be achieved with confidentiality together, for example, through watermarking and jamming [309]. Availability allows authorized users to access and maintain communication whenever required, and its violation often results from the DoS attacks. Techniques include Frequency-Hopping Spread-Spectrum (FHSS) [315] to continuously and rapidly change the central frequency following a random (but known to the legitimate receiver) pattern (so a jamming attack cannot disrupt the transmission) and Direct-Sequence Spread-Spectrum (DSSS) [316] to spread the spectrum of signal over a wide frequency bandwidth using a pseudo-noise (PN) code, which makes the jammer much hard to disrupt the transmission due to a much higher power required.

PLS in emerging technologies and use cases in 5G and 6G. PLS has been already investigated and applied to *emerging technologies* such as VLC, Cell-free massive MIMO (CF-mMIMO), RIS, THz, NOMA, NTN, and mMTC etc., and *new use cases* such as UAV [317], Body Area Network (BAN) [284], V2X [318], and IoT, for 5G and 6G.

CF-mMIMO is vulnerable to active eavesdropping attacks such as active pilot contamination attacks [319, 320] where an (single-antenna) active eavesdropper sends an imitated legitimate user pilot sequence during the uplink training phase to contaminate the channel estimates at the Access Points (APs), which results in the downlink precoders at the APs to use the contaminated estimates and misdirect the APs to beamform

secure information toward the active eavesdropper instead of the legitimate users. The attack causes a substantial secrecy rate loss [320]. Various PLS approaches have been proposed to mitigate the attacks, such as a more accurate channel estimation algorithm [321] that is based on non-overlapping angle of arrival between legitimate users and Eves to differentiate them (so mitigate the impact of the pilot contamination), the use of fingerprint positioning to estimate the location of users and Eves [322], the consideration of information transmission with energy transfer together where an active eavesdropper can also actively harvest energy [323], and the leverage of RIS to limit information leakage [324]. While these work consider a single-antenna active Eve, [325] proposes a precoding optimization in CPU to use the partial CSIs (shared by APs) of serving users for the maximization of the secret rate under required minimum rate for users and power constrains of APs, in the context of a user-centric approach to deploy CF-mMIMO in the presence of more challenging multiple collusive Eves. The simulation result of the work indicates user-centric is promising to implement CF-mMIMO securely. [326] considers downlink secure transmissions for a UE-centric model where each UE is served by a subset of APs in scalable CF-mMIMO in the presence of multiple passive Eves. The work evaluates the secrecy performance for two fading channels using a stochastic geometry approach where the locations of APs, UEs, and Eves are modelled as independent homogeneous Poisson point processes. Its simulation results show that the existence of an optimal design for the density of APs and the number of antennas for each AP to achieve the best secrecy transmission rate, with a further improvement using artificial noise injection. For some applications, such as healthcare information systems, that require a safe zone (e.g. a hospital), PLS can be integrated with CF-mMIMO to use precise beamforming towards legitimate users in the zone and amplify artificial noise outside the zone towards Eves to maximise the secret rate, as presented in [327]. Other work [328, 329] exploit secure communication in CF-mMIMO using hardware impairments such as distortion of oscillators and phase noise.

VLC, offering a large available frequency spectrum and high data rates, has inherent security *benefits* thanks to confined light signals within physical areas and *challenges* due to its open and broadcast nature. PLS for Radio Frequency (RF) wireless networks can be adapted to address these challenges. [318] gives a comprehensive review of the applications of PLS in VLC and discuss secrecy performance in different wiretap system models for MIMO, Multiple-Input Single-Output (MISO), Single-Input Single-Output (SISO), and hybrid RF/VLC when considering both single-user and multiple-user scenarios in the presence of (one or more) Eves. While multiple light sources are usually required for multiple-user VLC, [330] proposes a relay-aided and cooperative jamming-based PLS scheme for the specific scenarios with only a single light source. To analyse security performance, the locations of relays and Eves are modelled as Poisson point processes. Monte Carlo simulations are used for evaluation. VLC can also be implemented using RGB LEDs where communication is secured against eavesdropping attacks using watermarking and jamming in separate red and blue light channels [331] while jamming can be aided by RIS [332]. The use of RIS to assist PLS in indoor VLC systems using beamforming-optimization, interference-management, and intelligent-signal-manipulation is reviewed in [333]. The minimum secrecy rate and the minimum secrecy energy efficiency can be maximized by jointly optimizing VLC AP power allocation, RIS association, and RIS elements orientation angles in rate-splitting multiple access and power-domain NOMA schemes, as presented in [334].

THz can achieve very high data rate and use extremely directional and narrow beams, which helps to reduce the areas where Eves can locate to intercept messages. If, however, Eves locate inside the narrow beams or around the legitimate receivers, they can still eavesdrop the transmission messages. THz is also blockage-prone [335]. So an active Eva may intentionally block parts of transmission links and have impact on availability. To protect against such attacks and provide robust security measures, PLS techniques can (1) leverage unique THz channel properties for security such as abundant spectrum [335], frequency- and distance-dependent molecular absorption loss [336], and channel sparsity [337], and (2) enhance security by signal processing, such as further beamforming [335], RIS-assisted beamforming [338], frequency diverse array (FDA)-based beamforming [335], and Deep Neural Network (DNN)-based and Artificial Noise (AN)-assisted [339].

The non-orthogonal nature of NOMA, while offering spectral efficiency gains through sharing, introduces unique security challenges (e.g., Eves can intercept more signals, potentially leading to a greater leakage of confidential information due to spectrum sharing, and strong users can decode the signals of weak users by successive interference cancellation - SIC [340]), concerning external passive eavesdropping and particularly internal active eavesdropping (by normal or strong users) [284]. PLS offers an efficient and cost-effective alternative or complement to upper-layer cryptographic techniques for securing NOMA communications. It provides a set of NOMA specific techniques, such as leveraging multiuser interference to degrade Eves' reception capabilities, intelligent power allocation, beamforming, signal transformation, user scheduling and grouping, cooperative nodes and relays, and integration with other emerging technologies like RIS [341], to address these vulnerabilities and ensure secure communication in NOMA-based wireless network [340]. AI and ML techniques are being increasingly used to optimize PLS strategies in NOMA, particularly for complex tasks like dynamic resource management, power allocation, user grouping, and identifying potential security threats [340].

PLS offers a promising approach to enhance the security of IoT systems by addressing the unique challenges related to resource constraints (limited processing capabilities, storage memory, and battery power), scalability, heterogeneity, and wireless communication inherent in these networks. By leveraging the physical characteristics of the communication channel, PLS can provide lightweight (less overhead and simple encoding techniques), energy-efficient, low-latency, and adaptive security solutions, often without the complexities of traditional key management. Most PLS techniques discussed previously

can be applied to IoT systems. The survey papers [342, 343] give a review of the application of PLS in IoT. Keyless PLS techniques avoid the challenges of secret key management and distribution, which makes them particularly suitable for large-scale and resource-constrained IoT devices. These devices can cooperate together to achieve secrecy requirements [343], such as cooperative jamming [344] and secure relay selection [345] to allow low-power IoT devices to combat more powerful eavesdroppers.

AI and ML are playing an increasingly significant role in PLS, offering new possibilities for enhancing security in wireless communication systems, particularly in the context of 6G and beyond [346]. It could involve the integration of AI/ML with PLS in air interfaces and system models, shared key agreement in O-RAN, intelligent codebook generation, detection and optimization, low-latency secure information exchange (such as in ultra-reliable low-latency communication) [347], intelligent physical layer authentication [300], secure resource allocation [340], attack detection and defense [346], context-aware security [348], intelligent physical layer key generation [346], to name a few.

D. Federated Learning-based Privacy Securing Techniques

To address inherent privacy and security vulnerabilities within FL in the context of 6G networks, several advanced defense mechanisms are being actively explored. These include privacy-preserving cryptographic solutions, differential privacy techniques, robust aggregation, and trusted computing frameworks.

(a) Privacy-Preserving Mechanisms

(i) Homomorphic Encryption (HE): HE facilitates computation on encrypted data without decryption, preserving confidentiality during collaborative training. In 6G FL, HE allows edge nodes (ENs) to transmit encrypted model updates, enabling secure aggregation at server-side without revealing local data [349, 350].

(ii) Secure Multi-Party Computation (SMPC): SMPC enables multiple clients in 6G networks to collaboratively compute global models without exposing individual local datasets. Each client's data is partitioned into secret shares, computed securely in a distributed manner, significantly enhancing privacy in decentralized 6G architectures [351, 352].

(iii) Differential Privacy (DP): DP ensures robust privacy protection in 6G FL by adding calibrated noise to model updates, effectively mitigating inference and reconstruction attacks. Due to lower computational demands, DP is particularly suitable for resource-constrained 6G edge environments.

(iv) Federated Knowledge Distillation (FedKD): FedKD transfers knowledge from sophisticated global models to lightweight local models, enhancing computational efficiency and reducing communication overhead, essential for latency-sensitive 6G applications [353, 354, 355]. FedKD employs gradient encryption and compression, significantly reducing sensitive information leakage.

(v) Trusted Execution Environments (TEEs): TEEs provide hardware-enforced secure enclaves for computation, ensuring the integrity and confidentiality of model updates and training processes in 6G FL scenarios. Frameworks like IntelSGX [356] and PPFL [357] leverage TEEs for robust protection against tampering and unauthorized access, essential for critical applications such as healthcare and autonomous systems in 6G networks. TEE is leveraged for implementing the privacy of data during computation using confidential computing. Confidential computing is a means to secure sensitive workloads of data and AI models in use, apart from data at rest and in transit. The advantage of confidential computing over traditional encryption is that it ensures the privacy of data undergoing computation [13], whether it is in untrustworthy environments like the cloud, the hybrid cloud or on-premises.

(b) Defense against Model and Data Attack: In addition to privacy-preserving methods, several defense mechanisms aim to enhance model robustness against adversarial manipulations in FL. These techniques focus on detecting and neutralizing malicious updates, ensuring the reliability and stability of the global model.

(i) Anomaly Detection: Anomaly detection methods identify malicious updates through statistical and machine-learning-based techniques, which are crucial in the highly dynamic 6G FL environment. Techniques such as LoMar [358], FederatedReverse [359], and DDaBA [360] provide adaptive detection capabilities, enhancing global model resilience against data poisoning and model poisoning attacks.

(ii) Robust Aggregation Techniques: Robust aggregation strategies like Multi-Krum [361], FoolsGold [362], and clustering-based methods address vulnerabilities arising from malicious or anomalous client updates in heterogeneous 6G edge devices. These methods maintain aggregation integrity, ensuring stable performance across decentralized and diverse FL deployments.

(iii) Model Pruning: Pruning reduces the complexity and attack surface of FL models by eliminating redundant or insignificant parameters, enhancing robustness against adversarial manipulations [363, 364]. Structured and unstructured pruning techniques minimize computational and communication overhead, critical for efficient deployment on resource-constrained 6G edge devices [365, 366].

(iv) Regularization: Regularization approaches stabilize FL training by penalizing overly complex or suspicious client updates, significantly mitigating the impact of model poisoning and data poisoning attacks. Techniques such as local self-regularization (LSR) [367] and contractible regularization (ConTre) [368] reinforce the robustness and generalization capabilities of 6G FL models, addressing data heterogeneity and adversarial threats.

E. Discussion and Future Research Problems

In the previous sections, we explored the security and privacy vulnerabilities that are expected in 6G networks, starting from threats inherent in pre-6G networks, threats due to new architecture of 6G networks and threats expected in each enabling technologies. Based on this analysis of the threat surfaces, in the current section, we focused on specific key technologies that will potentially enhance security and privacy aspects in 6G. However, several new research studies will

arise due to the incorporation of these technologies in 6G frameworks. We explore these future research ideas in this subsection.

(a) Blockchains: To incorporate intelligence and adaptability in the security of 6G networks, future research could explore the integration of AI and blockchains. Some areas where these two technologies can combine are applying machine learning techniques for the selection and processing of data in blockchain nodes, use blockchains and AI together for intelligent network management and security mechanisms etc. [210]. As 6G networks would encompass the terrestrial, space, aerial, underground, and underwater, the design of the security and privacy aspects of these networks is pivotal. Thus, it is necessary to devise new consensus protocols that are more secure, efficient, and privacy-preserving, and aligned with the demands of these networks. Some of the pertinent research areas related to this aspect are to enhance the resilience and interference resistance of consensus protocols by leveraging cryptographic techniques, designing innovative consensus protocols adaptable to the new 6G architecture, and creating ways to expedite blockchain transactions and data processing while keeping the strict security prerequisites intact [369]. The traditional public key encryption algorithms prevalent in current networks will become vulnerable to attacks in the future when quantum computing technology is used extensively. Therefore, a significant research direction is to explore the integration of blockchain with quantum security technology to enhance network security for 6G networks [370]. For instance, exploring the use of encryption methods based on QKD to improve the security of the communication and storage processes of blockchain. Moreover, quantum random number generators can generate high-quality random numbers to enhance the randomness and hence the security of blockchains.

(b) Post-Quantum Security: While QKD provides long-term security grounded in quantum physics, it faces deployment challenges in large-scale 6G environments. In parallel, PQC offers algorithmic alternatives to RSA and ECC, designed to resist attacks from quantum computers [267, 268, 269]. However, PQC still relies on hardness assumptions and does not offer unconditional security. To mitigate future risks, hybrid architectures combining PQC and QKD are gaining attention [271, 272]. Moreover, the field faces a pressing challenge: designing a coordinated migration path from current public-key systems to quantum-safe alternatives [276, 277]. Given the long operational lifespans and interdependencies of telecom and critical infrastructure, migration strategies must be risk-aware and flexible. The concept of crypto-agilitythe ability to replace cryptographic algorithms without redesigning entire systemsis therefore essential [277, 278].

(c) Physical Layer Security: PLS has already been intensively studied, but there are still many challenges, from fundamental theory to practical implementation and application in emerging technologies, to be addressed before it becomes a widely adopted security mechanism in 5G, 6G and beyond. It is essential to address the design of robust PLS techniques for challenging channel conditions such as imperfect or partial CSI, Eve's better channel than the legitimate one, simple environment like line-of-sight (LOS) scenarios where channel characteristics between TR and TE links can be very similar. A holistic stack of PLS techniques to protect a large variety of devices in heterogeneous communication systems in 5G and 6G against mixed attacks are crucial. Currently, the primary focus of research is on particular networks or individual scenarios against limited combination of attacks such as passive and active eavesdropping, and DoS. Integration between PLS and classic cryptography to provide comprehensive security protection cross different network layers. Practical application and deployment of PLS in emerging technologies and use cases need to be explored before implementing them in real-world scenarios. Other research directions are the joint design of communication systems to achieve a good balance between security, reliability, throughput, and latency etc., synergizing security and other Quality-of-Services (QoS) such as energy efficiency and service availability. leveraging AI and ML to enhance PLS, and realizing practical AI-based PLS solutions for real-world networks to address potential new threats introduced by AI, context-aware intelligent AI-based PLS solutions, standardization of PLS to make it a mandatory or core feature set within major mainstream communication standards.

(d) Federated Learning-based Privacy Securing Techniques: While HE provides strong theoretical security, its high computational overhead poses practical challenges in ultra-low-latency scenarios and computationally constrained devices common in 6G deployments [371, 372]. In SMPC, the intensive communication overhead limits scalability, particularly when managing large-scale FL deployments common in 6G ecosystems [373]. DP faces challenges such as privacy degradation over multiple training iterations, necessitating techniques like privacy amplification and subsampling to maintain efficacy [178, 179, 374]. The protection of FedKD against sophisticated inference attacks is limited by the complexity of the global model and knowledge transfer accuracy [164]. TEE implementations face limitations regarding scalability and memory constraints.

VII. Conclusions

This paper presents a systematic survey of potential security and privacy attacks in future 6G networks, by focusing on the threat surfaces in each of the 6G enabling technologies, and mapping them to countermeasures based on a few key technologies whose principles and functionalities are described. Several hundred papers are summarized, categorized and explained, which will be a beneficial resource for researchers in this field to explore and inspire further development of security and privacy ensuring procedures in 6G networks. Moreover, this survey includes both peer-reviewed research and publications from standardization bodies, which produces a well-rounded and robust resource for researchers who are seeking to gain both theoretical and practical insights into security and privacy aspects of future communication networks. The discussion on open research problems involving these security and privacy solutions helps give a perspective on the attack surfaces across different technologies and the gaps that remain unbridged to handle these threats, for future research prospects.

References

[1] Van-Linh Nguyen et al. "Security and privacy for 6G: A survey on prospective technologies and challenges". In: *IEEE Communications Surveys & Tutorials* 23.4 (2021), pp. 2384–2428.

[2] Mengmeng Yang et al. *From 5G to 6G: A Survey on Security, Privacy, and Standardization Pathways*. 2024. arXiv: 2410.21986 [cs.CR]. URL: https://arxiv.org/abs/2410.21986.

[3] Walid Saad, Mehdi Bennis, and Mingzhe Chen. "A vision of 6G wireless systems: Applications, trends, technologies, and open research problems". In: *IEEE Network* 34.3 (2019), pp. 134–142.

[4] Hexa-X-II Consortium. *Deliverable D1.2 – 6G Use Cases and Requirements*. Technical Report D1.2. Hexa-X-II Project, Dec. 2023. URL: https://hexa-x-ii.eu/wp-content/uploads/2024/01/Hexa-X-II_D1.2.pdf.

[5] *Framework and overall objectives of the future development of IMT for 2030 and beyond*. Tech. rep. Recommendation ITU-R M.2160. International Telecommunication Union, Radiocommunication Sector (ITU-R), 2023. URL: https://www.itu.int/en/ITU-R/Pages/default.aspx.

[6] Bomin Mao et al. "Security and Privacy on 6G Network Edge: A Survey". In: *IEEE Communications Surveys & Tutorials* 25.2 (2023), pp. 1095–1127. DOI: 10.1109/COMST.2023.3244674.

[7] European Union Agency for Cybersecurity (ENISA). "Space Threat Landscape Report". In: (Mar. 2025). URL: https://www.enisa.europa.eu/sites/default/files/2025-03/Space_Threat_Landscape_Report_fin.pdf.

[8] telecomHall Forum. *NTN Security Challenges*. Apr. 2025. URL: https://www.telecomhall.net/t/ntn-security-challenges/33316.

[9] Zhiyun Jiang et al. "A LEO Satellite Handover Strategy Based on Graph and Multiobjective Multiagent Path Finding". In: *Journal of Aerospace Engineering* (2023). URL: https://onlinelibrary.wiley.com/doi/10.1155/2023/1111557.

[10] *O-RAN ALLIANCE White Paper: O-RAN Architecture and Security for Vertical Industries*. Tech. rep. O-RAN ALLIANCE, Jan. 2025. URL: https://www.o-ran.org/o-ran-resources.

[11] *Security in 6G: Architecture and Technology Considerations*. Tech. rep. Ericsson, 2024.

[12] Zehang Deng et al. "Ai agents under threat: A survey of key security challenges and future pathways". In: *ACM Computing Surveys* 57.7 (2025), pp. 1–36.

[13] *NVIDIA Confidential Computing*. URL: https://www.nvidia.com/en-gb/data-center/solutions/confidential-computing/.

[14] Ijaz Ahmad et al. "Security for 5G and beyond". In: *IEEE Communications Surveys & Tutorials* 21.4 (2019), pp. 3682–3722.

[15] Shimaa A Abdel Hakeem, Hanan H Hussein, and HyungWon Kim. "Security requirements and challenges of 6G technologies and applications". In: *Sensors* 22.5 (2022), p. 1969.

[16] Faisal Naeem et al. "Security and privacy for reconfigurable intelligent surface in 6G: A review of prospective applications and challenges". In: *IEEE Open Journal of the Communications Society* 4 (2023), pp. 1196–1217.

[17] Myoungsu Kim et al. "Security of 6G-enabled vehicle-to-everything communication in emerging federated learning and blockchain technologies". In: *IEEE Access* 12 (2023), pp. 33972–34001.

[18] Pawani Porambage et al. "Security, Privacy, and Trust for Open Radio Access Networks in 6G". In: *IEEE Open Journal of the Communications Society* (2024).

[19] Cong T Nguyen et al. "Emerging technologies for 6G non-terrestrial-networks: From academia to industrial applications". In: *IEEE Open Journal of the Communications Society* (2024).

[20] Mohamed Amine Ferrag et al. "Edge learning for 6G-enabled internet of things: A comprehensive survey of vulnerabilities, datasets, and defenses". In: *IEEE Communications Surveys & Tutorials* 25.4 (2023), pp. 2654–2713.

[21] Bomin Mao et al. "Security and privacy on 6G network edge: A survey". In: *IEEE communications surveys & tutorials* 25.2 (2023), pp. 1095–1127.

[22] Dinh C Nguyen et al. "Federated learning for internet of things: A comprehensive survey". In: *IEEE Communications Surveys & Tutorials* 23.3 (2021), pp. 1622–1658.

[23] Liangqi Yuan et al. "Decentralized federated learning: A survey and perspective". In: *IEEE Internet of Things Journal* (2024).

[24] Eslam Farsimadan, Leila Moradi, and Francesco Palmieri. "A Review on Security Challenges in V2X Communications Technology for VANETs". In: *IEEE Access* (2025).

[25] Xiaozhen Lu et al. "Reinforcement Learning-Based Physical Cross-Layer Security and Privacy in 6G". In: *IEEE Communications Surveys & Tutorials* 25.1 (2023), pp. 425–466. DOI: 10.1109/COMST.2022.3224279.

[26] Chamitha De Alwis et al. "A Survey on Network Slicing Security: Attacks, Challenges, Solutions and Research Directions". In: *IEEE Communications Surveys & Tutorials* (2023).

[27] Prajnamaya Dass et al. "Addressing privacy concerns in joint communication and sensing for 6G networks: challenges and prospects". In: *Annual Privacy Forum*. Springer. 2024, pp. 87–111.

[28] Yousef Sanjalawe et al. "A Review of 6G and AI Convergence: Enhancing Communication Networks With Artificial Intelligence". In: *IEEE Open Journal of the Communications Society* 6 (2025), pp. 2308–2355.

[29] Huawei. "Partnering with the Industry for 5G Security Assurance". In: *Huawei White Paper* (2021). URL: https://www-file.huawei.com/-/media/corporate/pdf/trust-center/huawei-5g-security-white-paper-4th.pdf.

[30] OPPO. *6G Security Architecture: Intelligent Security Built on Zero Trust*. 2025. URL: https://www.oppo.com/content/dam/oppo/common/mkt/footer/OPPO-6G-Security-WhitePaper-EN.pdf.

[31] Paul Scalise et al. "A Systematic Survey on 5G and 6G Security Considerations, Challenges, Trends, and Research Areas". In: *Future Internet* 16.3 (2024), p. 67.

[32] Gabrial Brown et al. "Service-based architecture for 5g core networks". In: *Huawei White Paper* 1 (2017).

[33] Sanjay M Vidhani and Amarsinh V Vidhate. "Security Challenges in 5G Network: A technical features survey and analysis". In: *2022 5th international conference on advances in science and technology (ICAST)*. IEEE. 2022, pp. 592–597.

[34] Rabia Khan et al. "A survey on security and privacy of 5G technologies: Potential solutions, recent advancements, and future directions". In: *IEEE Communications Surveys & Tutorials* 22.1 (2019), pp. 196–248.

[35] Syed Rafiul Hussain et al. "Privacy attacks to the 4G and 5G cellular paging protocols using side channel information". In: *Network and distributed systems security (NDSS) symposium2019* (2019).

[36] Roger Piqueras Jover and Vuk Marojevic. "Security and protocol exploit analysis of the 5G specifications". In: *IEEE Access* 7 (2019), pp. 24956–24963.

[37] Yuchen Wang, Zhenfeng Zhang, and Yongquan Xie. "Privacy-Preserving and Standard-Compatible AKA Protocol for 5G". In: *30th USENIX Security Symposium (USENIX Security 21)*. USENIX Association, Aug. 2021, pp. 3595–3612. ISBN: 978-1-939133-24-3. URL: https://www.usenix.org/conference/usenixsecurity21/presentation/wang-yuchen.

[38] Patrik Teppo and Karl Norman. "Security in 5G RAN and core deployments". In: *Ericsson White Paper* (2020). URL: https://www.ericsson.com/en/reports-and-papers/white-papers/security-in-5g-ran-and-core-deployments.

[39] Rafael F Schaefer, Gayan Amarasuriya, and H Vincent Poor. "Physical layer security in massive MIMO systems". In: *2017 51st Asilomar conference on signals, systems, and computers*. IEEE. 2017, pp. 3–8.

[40] Said El Kafhali, Iman El Mir, and Mohamed Hanini. "Security threats, defense mechanisms, challenges, and future directions in cloud computing". In: *Archives of Computational Methods in Engineering* 29.1 (2022), pp. 223–246.

[41] Yinghui Zhang et al. "Robust and universal seamless handover authentication in 5G HetNets". In: *IEEE Transactions on Dependable and Secure Computing* 18.2 (2019), pp. 858–874.

[42] Ericsson. *Evolving the security posture for critical infrastructure*. Apr. 2025. URL: https://www.ericsson.com/en/blog/north-america/2025/evolving-the-security-posture-for-critical-infrastructure.

[43] *EUROPEAN VISION FOR THE 6G NETWORK ECOSYSTEM*. Tech. rep. 6G-IA Vision Working Group, 2024. URL: https://doi.org/10.5281/zenodo.13708424.

[44] *Advancing the Technologies of the 6G Future: The Next G Alliance Technology Working Group*. Tech. rep. The Next G Alliance Technology Working Group, 2024. URL: https://nextgalliance.org/advancing-the-technologies-of-the-6g-future-the-next-g-alliance-technology-working-group/.

[45] Mikko A Uusitalo et al. "6G vision, value, use cases and technologies from European 6G flagship project Hexa-X". In: *IEEE access* 9 (2021), pp. 160004–160020.

[46] Seda Doan-Tusha, Hüseyin Arslan, et al. "6G vision: An ultra-flexible perspective". In: *arXiv preprint arXiv:2009.07597* (2020).

[47] Henk Wymeersch et al. "Joint communication and sensing for 6g-a cross-layer perspective". In: *2024 IEEE 4th International Symposium on Joint Communications & Sensing (JC&S)*. IEEE. 2024, pp. 01–06.

[48] Fengxiao Tang et al. "The roadmap of communication and networking in 6G for the metaverse". In: *IEEE Wireless Communications* 30.4 (2022), pp. 72–81.

[49] Xianbin Wang et al. "Realizing 6G: The operational goals, enabling technologies of future networks, and value-oriented intelligent multi-dimensional multiple access". In: *IEEE Network* 37.1 (2023), pp. 10–17.

[50] Jakob Hoydis et al. "Toward a 6G AI-native air interface". In: *IEEE Communications Magazine* 59.5 (2021), pp. 76–81.

[51] Xu Chen et al. "Zero trust architecture for 6G security". In: *IEEE Network* 38.4 (2023), pp. 224–232.

[52] Zhuoran Duan et al. "Agile Orchestration at Will: An Entire Smart Service-Based Security Architecture Towards 6G". In: *arXiv preprint arXiv:2505.22963* (2025).

[53] *NFV evolution:Towards the Telco Cloud*. Tech. rep. ETSI ISG NFV, 2025. URL: https://www.etsi.org/images/files/ETSIWhitePapers/ETSI-WP-65-NFV-evolution-Towards_the_Telco_Cloud.pdf.

[54] *ISG ZSM Activity Report 2023*. Tech. rep. ETSI ISG ZSM, 2023. URL: https://www.etsi.org/committee-activity/activity-report-zsm.

[55] Dario Sabella et al. *MEC security;Status of standards support and future evolutions*. Tech. rep. 2022.

[56] *Technical Committee (TC) Securing Artificial Intelligence (SAI) Activity Report 2023*. Tech. rep. ETSI ISG SAI, 2023. URL: https://www.etsi.org/committee-activity/activity-report-sai.

[57] *Experiential Networked Intelligence (ENI); Study on AI Agents based Next-generation Network Slicing*. Tech. rep. ETSI ISG ENI, 2025. URL: https://www.etsi.org/deliver/etsi_gr/ENI/001_099/051/04.01.01_60/gr_ENI051v040101p.pdf.

[58] ETSI. *ETSI GR ISC 001 :Integrated Sensing And Communications (ISAC); Use Cases and Deployment Scenarios*. Technical Report ETSI GR ISC 001 V1.1.1 (2025-03). ETSI, 2025. URL: https://www.etsi.org/deliver/etsi_gr/ISC/001_099/001/01.01.01_60/gr_ISC001v010101p.pdf.

[59] ETSI. *ETSI GR ISC 004: Integrated Sensing And Communications (ISAC); Security, Privacy, Trustworthiness and Sustainability*. Technical Report ETSI GR ISC 004 V1.1.1 (2026-02). ETSI, 2026. URL: https://www.etsi.org/deliver/etsi_gr/ISC/001_099/004/01.01.01_60/gr_ISC004v010101p.pdf.

[60] Matti Hämäläinen et al. "ETSI SmartBAN Architecture: The Global Vision for Smart Body Area Networks". In: *IEEE Access* 8 (2020), pp. 150611–150625. DOI: 10.1109/ACCESS.2020.3016705.

[61] Lorenzo Mucchi et al. "Physical-Layer Security in 6G Networks". In: *IEEE Open Journal of the Communications Society* 2 (2021), pp. 1901–1914. ISSN: 2644-125X. DOI: 10.1109/OJCOMS.2021.3103735. URL: https://ieeexplore.ieee.org/document/9509581/authors#authors (visited on 03/18/2025).

[62] *Industry Specification Group (ISG) on Quantum Key Distribution for Users (QKD) Activity Report 2023*. Tech. rep. ETSI ISG QKD, 2023. URL: https://www.etsi.org/committee-activity/activity-report-qkd.

[63] *Rel-18 Security feature summary*. Tech. rep. 3GPP SA3, 2023. URL: https://www.3gpp.org/technologies/rel18-sec.

[64] *The next wave of 5G 3GPP Release 19*. Tech. rep. 3GPP Rel19, 2023. URL: https://www.ericsson.com/en/blog/2023/12/3gpp-release-19.

[65] 3GPP. *Study on Ambient power-enabled Internet of Things (Release 19)*. Technical Report TR 22.840. 3GPP, 2023. URL: https://www.3gpp.org/ftp/Specs/archive/22_series/22.840/.

[66] ITU-T Study Group 13. *Standardization of quantum key distribution and relevant technologies*. ITU-T Technical Report. 2022. URL: https://www.itu.int/en/ITU-T/focusgroups/qit4n/Pages/default.aspx.

[67] ISO/IEC JTC 1/SC 27. *Security requirements for quantum key distribution*. ISO/IEC WD 23837-1. 2022.

[68] *Data protection and privacy*. Tech. rep. ITU, 2023. URL: https://www.itu.int/en/about/Documents/ITU-Data-Protection-and-Privacy-Policy.pdf.

[69] NIST. *NIST Releases First 3 Finalized Post-Quantum Encryption Standards*. News Report. NIST, 2024. URL: https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards.

[70] 3GPP. *3GPP: Feasibility Study on Integrated Sensing and Communication (Release 19)*. Technical Report TR 22.837. 3GPP, 2024. URL: https://www.etsi.org/deliver/etsi_gr/ISC/001_099/001/01.01.01_60/gr_ISC001v010101p.pdf.

[71] *IETF:Security & privacy*. Tech. rep. IETF. URL: https://www.ietf.org/technologies/security/.

[72] AI-RAN Alliance WG3. *AI-on-RAN: Enabling Monetizable Differentiated Connectivity for AI; Security, Privacy, Trustworthiness and Sustainability*. White Paper. AI RAn Alliance, 2026. URL: https://ai-ran.org/documents/AI-RAN-WG3-AI-on-RAN-Whitepaper.pdf.

[73] *O-RAN Specifications Lead the Telecom Industry towards Open and Intelligent Radio Access Networks*. URL: https://www.o-ran.org/specifications.

[74] *The O-RAN ALLIANCE Security Working Group Continues to Advance O-RAN Security*. URL: https://www.o-ran.org/blog/the-o-ran-alliance-security-working-group-continues-to-advance-o-ran-security.

[75] Ericsson. "https://www.ericsson.com/en/blog/2023/10/hexa-x-and-data-protection-evolution-in-6g". In: *Ericsson Blog* (2020). URL: https://www.ericsson.com/en/blog/2023/10/hexa-x-and-data-protection-evolution-in-6g.

[76] Hexa-X. *Hexa-X deliverables*. Tech. rep. URL: https://hexa-x.eu/deliverables/.

[77] *COST Action CA22168: PHYSICAL LAYER SECURITY FOR TRUSTWORTHY AND RESILIENT 6G SYSTEMS (6G-PHYSEC)*. Tech. rep. COST, 2023. URL: https://6gphysec.org/.

[78] *CA22168 - Working Groups*. Tech. rep. COST, 2023.

[79] Bartlomiej Siniarski et al. "ROBUST-6G: Smart, Automated, and Reliable Security Service Platform for 6G". In: *2024 Fifteenth International Conference on Ubiquitous and Future Networks (ICUFN)*. 2024, pp. 384–389. DOI: 10.1109/ICUFN61752.2024.10624832.

[80] Jindan Xu et al. "Reconfiguring wireless environments via intelligent surfaces for 6G: Reflection, modulation, and security". In: *Science China Information Sciences* 66.3 (2023), p. 130304.

[81] Zhe Zhang et al. "Improving physical layer security for reconfigurable intelligent surface aided NOMA 6G networks". In: *IEEE Transactions on Vehicular Technology* 70.5 (2021), pp. 4451–4463.

[82] Waqas Khalid et al. "Reconfigurable intelligent surface for physical layer security in 6G-IoT: Designs, issues, and advances". In: *IEEE Internet of Things Journal* 11.2 (2023), pp. 3599–3613.

[83] Bo Liu et al. "Architecture for cellular enabled integrated communication and sensing services". In: *China Communications* 20.9 (2023), pp. 59–77.

[84] Thorsten Wild, Volker Braun, and Harish Viswanathan. "Joint design of communication and sensing for beyond 5G and 6G systems". In: *IEEE Access* 9 (2021), pp. 30845–30857.

[85] Carlos Baquero Barneto et al. "Full duplex radio/radar technology: The enabler for advanced joint communication and sensing". In: *IEEE Wireless Communications* 28.1 (2021), pp. 82–88.

[86] Diana PM Osorio et al. "The Rise of Networked ISAC: Emerging Aspects and Challenges". In: *IEEE Open Journal of the Communications Society* (2025).

[87] Zhongxiang Wei et al. "Toward multi-functional 6G wireless networks: Integrating sensing, communication, and security". In: *IEEE Communications Magazine* 60.4 (2022), pp. 65–71.

[88] Henrik Åkesson and Diana Pamela Moya Osorio. "Privacy-Preserving Framework for Cell-Free MIMO ISAC Systems". In: *arXiv preprint arXiv:2409.12874* (2024).

[89] Onur Günlü et al. "Secure joint communication and sensing". In: *2022 IEEE International Symposium on Information Theory (ISIT)*. IEEE. 2022, pp. 844–849.

[90] Prateek Kapoor, Ankur Vora, and Kyoung-Don Kang. "Detecting and mitigating spoofing attack against an automotive radar". In: *2018 IEEE 88th Vehicular Technology Conference (VTC-Fall)*. IEEE. 2018, pp. 1–6.

[91] Haji M Furqan et al. "Wireless communication, sensing, and REM: A security perspective". In: *IEEE Open Journal of the Communications Society* 2 (2021), pp. 287–321.

[92] Shihang Lu et al. "Integrated sensing and communications: Recent advances and ten open challenges". In: *IEEE Internet of Things Journal* 11.11 (2024), pp. 19094–19120.

[93] Arsenia Chorti et al. "Context-aware security for 6G wireless: The role of physical layer security". In: *IEEE Communications Standards Magazine* 6.1 (2022), pp. 102–108.

[94] Guangxu Zhu et al. "Pushing AI to wireless network edge: An overview on integrated sensing, communication, and computation towards 6G". In: *Science China Information Sciences* 66.3 (2023), p. 130301.

[95] Kaiqian Qu et al. "Privacy and security in ubiquitous integrated sensing and communication: Threats, challenges and future directions". In: *IEEE Internet of Things Magazine* 7.4 (2024), pp. 52–58.

[96] Chetan Kumar, Sean Marston, and Ravi Sen. "Cyber-physical systems (CPS) security: state of the art and research opportunities for information systems academics". In: *Communications of the Association for Information Systems* 47.1 (2020), p. 36.

[97] Harald Gjermundrød, Ioanna Dionysiou, and Kyriakos Costa. "privacyTracker: a privacy-by-design GDPR-compliant framework with verifiable data traceability controls". In: *Current Trends in Web Engineering: ICWE 2016 International Workshops, DUI, TELERISE, SoWeMine, and Liquid Web, Lugano, Switzerland, June 6-9, 2016. Revised Selected Papers 16*. Springer. 2016, pp. 3–15.

[98] Mengxuan Du et al. "Integrated sensing, communication and computation for over-the-air federated learning in 6G wireless networks". In: *IEEE Internet of Things Journal* (2024).

[99] Yihua Ma et al. "Highly efficient waveform design and hybrid duplex for joint communication and sensing". In: *IEEE Internet of Things Journal* 10.19 (2023), pp. 17369–17381.

[100] Elmehdi Illi et al. "Physical layer security for authentication, confidentiality, and malicious node detection: a paradigm shift in securing IoT networks". In: *IEEE Communications Surveys & Tutorials* 26.1 (2023), pp. 347–388.

[101] Xu Chen et al. "Multiple signal classification based joint communication and sensing system". In: *IEEE Transactions on Wireless Communications* 22.10 (2023), pp. 6504–6517.

[102] Vyron Kampourakis, Vasileios Gkioulos, and Sokratis Katsikas. "A systematic literature review on wireless security testbeds in the cyber-physical realm". In: *Computers & Security* 133 (2023), p. 103383.

[103] Afsana Sharmin et al. "Cyber Attacks on Space Information Networks: Vulnerabilities, Threats, and Countermeasures for Satellite Security". In: *Journal of Cybersecurity and Privacy* 5.3 (2025), p. 76.

[104] Asim Ul Haq et al. "Need of UAVs and Physical Layer Security in Next-Generation Non-Terrestrial Wireless Networks: Potential Challenges and Open Issues". In: *IEEE Open Journal of Vehicular Technology* 6 (2025), pp. 554–595. DOI: 10.1109/OJVT.2025.3525781.

[105] A. Iqbal et al. "Empowering non-terrestrial networks with artificial intelligence: A survey". In: *IEEE Access* 11 (2023), pp. 100986–101006.

[106] Jani Suomalainen and Ijaz Ahmad. "Cybersecurity for Machines in Satellite–Terrestrial Networks". In: *Integration of MTC and Satellites for IoT toward 6G Era* (2024), pp. 245–271.

[107] Olfa Ben Yahia et al. "Physical layer security framework for optical non-terrestrial networks". In: *2021 28th International Conference on Telecommunications (ICT)*. IEEE. 2021, pp. 162–166.

[108] Sasa Maric et al. "System Security Framework for 5G Advanced/6G IoT Integrated Terrestrial Network-Non-Terrestrial Network (TN-NTN) with AI-Enabled Cloud Security". In: *arXiv preprint arXiv:2508.05707* (2025).

[109] Maira Khalid et al. "Deep learning techniques for enhanced security and privacy in 6G terrestrialnonterrestrial network architecture". In: *The Journal of Supercomputing* 81 (Mar. 2025). DOI: 10.1007/s11227-025-07097-x.

[110] Seungbin Lee and Jiyoon Kim. "Survey on Security for Non-Terrestrial Networks". In: *Research Briefs on Information and Communication Technology Evolution* 10 (2024), pp. 111–123.

[111] Zhengquan Zhang et al. "6G wireless networks: Vision, requirements, architecture, and key technologies". In: *IEEE vehicular technology magazine* 14.3 (2019), pp. 28–41.

[112] Diana Pamela Moya Osorio et al. "Towards 6G-enabled internet of vehicles: Security and privacy". In: *IEEE Open Journal of the Communications Society* 3 (2022), pp. 82–105.

[113] Pawani Porambage et al. "6G Security Challenges and Potential Solutions". In: *2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)*. 2021, pp. 622–627. DOI: 10.1109/EuCNC/6GSummit51104.2021.9482609.

[114] Lorenzo Mucchi et al. "Physical-layer security in 6G networks". In: *IEEE Open Journal of the Communications Society* 2 (2021), pp. 1901–1914.

[115] Ferhat Ozgur Catak et al. "Security concerns on machine learning solutions for 6G networks in mmWave beam prediction". In: *Physical Communication* 52 (2022), p. 101626.

[116] Miroslav Mitev et al. “What physical layer security can do for 6G security”. In: *IEEE Open Journal of Vehicular Technology* 4 (2023), pp. 375–388.

[117] Yiming Huo et al. “Technology trends for massive MIMO towards 6G”. In: *Sensors* 23.13 (2023), p. 6062.

[118] Fauzia Irram et al. “Physical layer security for beyond 5G/6G networks: Emerging technologies and future directions”. In: *Journal of Network and Computer Applications* 206 (2022), p. 103431.

[119] Nurun Nahar et al. “A Survey on Zero Trust Architecture: Applications and Challenges of 6G Networks”. In: *IEEE Access* (2024).

[120] P SumanPrakash et al. “Learning-driven Continuous Diagnostics and Mitigation program for secure edge management through Zero-Trust Architecture”. In: *Computer Communications* 220 (2024), pp. 94–107.

[121] Laxmi Ahuja, Sonali Vashisth, and Ayush Thakur. “Integrating SIEM with Zero Trust Architecture”. In: *2025 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE)*. IEEE. 2025, pp. 1–6.

[122] V Stafford. “Zero trust architecture”. In: *NIST special publication* 800.207 (2020), pp. 800–207.

[123] M. Eckhart. *Advanced Threat Modeling for Zero Trust Architectures*. Nov. 2025. URL: https://www.linkedin.com/in/the-modern-cybersecurity-thought-leadership/.

[124] Hichem Sedjelmaci, Kamel Tourki, and Nirwan Ansari. “Enabling 6G security: The synergy of zero trust architecture and artificial intelligence”. In: *IEEE Network* 38.3 (2023), pp. 171–177.

[125] Mir Ghoraishi et al. “iTrust6G: Zero-Trust Security for 6G Networks”. In: *methods* 5 (), p. 6.

[126] Sandro Rodriguez Garzon, Hakan Yildiz, and Axel Küpper. “Decentralized identifiers and self-sovereign identity in 6g”. In: *IEEE Network* 36.4 (2022), pp. 142–148.

[127] Yuntao Wang et al. “Challenges and solutions in autonomous driving: A blockchain approach”. In: *IEEE Network* 34.4 (2020), pp. 218–226.

[128] Yu Chih Wei and Tak Wai Yu. “Zero trust framework in financial sector: The handling of machine learning based trust management”. In: *2023 International Conference on Consumer Electronics-Taiwan (ICCE-Taiwan)*. IEEE. 2023, pp. 211–212.

[129] Demostenes Zegarra Rodriguez et al. “Attentive transformer deep learning algorithm for intrusion detection on IoT systems using automatic Xplainable feature selection”. In: *Plos one* 18.10 (2023), e0286652.

[130] Nonso Okika et al. “Assessing the vulnerability of traditional and post-quantum cryptographic systems through penetration testing and strengthening cyber defenses with zero trust security in the era of quantum computing”. In: *International Journal of Innovative Science and Research Technology* 10.2 (2025).

[131] Estefania Coronado et al. “Zero touch management: A survey of network automation solutions for 5G and 6G networks”. In: *IEEE Communications Surveys & Tutorials* 24.4 (2022), pp. 2535–2578.

[132] Mirna El Rajab, Li Yang, and Abdallah Shami. “Zero-touch networks: Towards next-generation network automation”. In: *Computer Networks* 243 (2024), p. 110294.

[133] Chafika Benzaid and Tarik Taleb. “AI-driven zero touch network and service management in 5G and beyond: Challenges and research directions”. In: *Ieee Network* 34.2 (2020), pp. 186–194.

[134] Li Yang and Abdallah Shami. “IoT data analytics in dynamic environments: From an automated machine learning perspective”. In: *Engineering Applications of Artificial Intelligence* 116 (2022), p. 105366.

[135] Sushil Shakya, Robert Abbas, and Sasa Maric. “A Novel Zero-Touch, Zero-Trust, AI/ML Enablement Framework for IoT Network Security”. In: *arXiv preprint arXiv:2502.03614* (2025).

[136] Li Yang et al. “Towards zero touch networks: Cross-layer automated security solutions for 6G wireless networks”. In: *IEEE Transactions on Communications* (2025).

[137] Lin Bai et al. “Physical layer authentication in wireless communication networks: A survey”. In: *Journal of Communications and Information Networks* 5.3 (2020), pp. 237–264.

[138] Michele Polese et al. “Understanding O-RAN: Architecture, interfaces, algorithms, security, and research challenges”. In: *IEEE Communications Surveys & Tutorials* 25.2 (2023), pp. 1376–1411.

[139] Madhusanka Liyanage et al. “Open RAN security: Challenges and opportunities”. In: *Journal of Network and Computer Applications* 214 (2023), p. 103621.

[140] Eric Hanselman. *Security Benefits of Open Virtualized RAN*. Tech. rep. 451 Research, May 2020. URL: https://www.cisco.com/c/dam/en/us/solutions/service-provider/pdfs/5g-network-architecture/white-paper-sp-open-vran-security-benefits.pdf.

[141] Jiadai Wang et al. “Intelligent network slicing for B5G and 6G: Resource allocation, service provisioning, and security”. In: *IEEE Wireless Communications* 31.3 (2024), pp. 271–277.

[142] Antonio Matencio Escolar et al. “Network slicing as 6G security mechanism to mitigate cyber-attacks: the RIGOUROUS approach”. In: *2024 IEEE 10th International Conference on Network Softwarization (NetSoft)*. IEEE. 2024, pp. 387–392.

[143] Peng Li and Jianing Du. “Brand Design Data Security and Privacy Protection Under 6G Network Slicing Architecture”. In: *International Journal of Network Management* 35.2 (2025), e70009.

[144] Mohammad Asif Habibi et al. “Toward an open, intelligent, and end-to-end architectural framework for network slicing in 6G communication systems”. In: *IEEE Open Journal of the Communications Society* 4 (2023), pp. 1615–1658.

[145] Latif U Khan et al. “Digital twin of wireless systems: Overview, taxonomy, challenges, and opportunities”. In: *IEEE Communications Surveys and Tutorials* 24.4 (2022), pp. 2230–2254.

[146] Huan X Nguyen et al. “Digital twin for 5G and beyond”. In: *IEEE Communications Magazine* 59.2 (2021), pp. 10–15.

[147] Gouranga Charan, Muhammad Alrabeiah, and Ahmed Alkhateeb. “Vision-aided 6G wireless communications: Blockage prediction and proactive handoff”. In: *IEEE Transactions on Vehicular Technology* 70.10 (2021), pp. 10193–10208.

[148] Paul Almasan et al. “Network digital twin: Context, enabling technologies, and opportunities”. In: *IEEE Communications Magazine* 60.11 (2022), pp. 22–27.

[149] Yuanhao Cui et al. “On the Physical Layer of Digital Twin: An Integrated Sensing and Communications Perspective”. In: *IEEE Journal on Selected Areas in Communications* 41.11 (2023), pp. 3474–3490. DOI: 10.1109/JSAC.2023.3314826.

[150] Ahmed Alkhateeb, Shuaifeng Jiang, and Gouranga Charan. “Real-Time Digital Twins: Vision and Research Directions for 6G and Beyond”. In: *IEEE Communications Magazine* 61.11 (2023), pp. 128–134. DOI: 10.1109/MCOM.001.2200866.

[151] Ozgur Umut Akgul et al. “Discussion on 6G Architecture Evolution: Challenges and Emerging Technology Trends”. In: *2024 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)*. 2024, pp. 664–669. DOI: 10.1109/EuCNC/6GSummit60053.2024.10597056.

[152] Hyeran Mun et al. “A Comprehensive Survey on Digital Twin: Focusing on Security Threats and Requirements”. In: *IEEE Access* 13 (2025), pp. 73362–73390. DOI: 10.1109/ACCESS.2025.3563621.

[153] Yuntao Wang et al. “A Survey on Digital Twins: Architecture, Enabling Technologies, Security and Privacy, and Future Prospects”. In: *IEEE Internet of Things Journal* 10.17 (2023), pp. 14965–14987. DOI: 10.1109/JIOT.2023.3263909.

[154] Yidan Pan et al. “A Survey on Digital Twin Networks: Architecture, Technologies, Applications and Open Issues”. In: *IEEE Internet of Things Journal* (2025), pp. 1–1. DOI: 10.1109/JIOT.2025.3565265.

[155] Yiwen Wu, Ke Zhang, and Yan Zhang. “Digital twin networks: A survey”. In: *IEEE Internet of Things Journal* 8.18 (2021), pp. 13789–13804.

[156] Sana Hafeez et al. “Blockchain-Assisted UAV Communication Systems: A Comprehensive Survey”. In: *IEEE Open Journal of Vehicular Technology* 4 (2023), pp. 558–580. DOI: 10.1109/OJVT.2023.3295208.

[157] Wenshuai Liu et al. “When Digital Twin Meets 6G: Concepts, Obstacles, and Research Prospects”. In: *IEEE Communications Magazine* 63.3 (2025), pp. 16–22. DOI: 10.1109/MCOM.001.2400202.

[158] Ezekiel B Ouedraogo et al. “Digital Twin Data Management: A Comprehensive Review”. In: *IEEE Transactions on Big Data* (2025).

[159] Tiago M Fernandez-Carames and Paula Fraga-Lamas. “Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks”. In: *IEEE access* 8 (2020), pp. 21091–21116.

[160] Muhammad Sheraz et al. “A Comprehensive Survey on Revolutionizing Connectivity Through Artificial Intelligence-Enabled Digital Twin Network in 6G”. In: *IEEE Access* 12 (2024), pp. 49184–49215. DOI: 10.1109/ACCESS.2024.3384272.

[161] Jakub Konen et al. “Federated learning: Strategies for improving communication efficiency”. In: *arXiv preprint arXiv:1610.05492* (2016). URL: https://doi.org/10.48550/arXiv.1610.05492.

[162] Mohammed Aledhari et al. “Federated learning: A survey on enabling technologies, protocols, and applications”. In: *IEEE Access* 8 (2020), pp. 140699–140725.

[163] Bart Custers et al. *EU personal data protection in policy and practice*. Vol. 29. Springer, 2019.

[164] Habib Ullah Manzoor et al. “A Survey of Security Strategies in Federated Learning: Defending Models, Data, and Privacy”. In: *Future Internet* 16.10 (2024). ISSN: 1999-5903. DOI: 10.3390/fi16100374. URL: https://www.mdpi.com/1999-5903/16/10/374.

[165] Viraaji Mothukuri et al. “A survey on security and privacy of federated learning”. In: *Future Generation Computer Systems* 115 (2021), pp. 619–640.

[166] Xin Gu et al. “A review of privacy enhancement methods for federated learning in healthcare systems”. In: *International Journal of Environmental Research and Public Health* 20.15 (2023), p. 6539.

[167] Shuang Dai and Fanlin Meng. “Addressing modern and practical challenges in machine learning: A survey of online federated and transfer learning”. In: *Applied Intelligence* 53.9 (2023), pp. 11045–11072.

[168] Ehsan Hallaji et al. “Decentralized Federated Learning: A Survey on Security and Privacy”. In: *IEEE Transactions on Big Data* 10.2 (2024), pp. 194–213. DOI: 10.1109/TBDATA.2024.3362191.

[169] Ehsan Hallaji, Roozbeh Razavi-Far, and Mehrdad Saif. “Federated and transfer learning: A survey on adversaries and defense mechanisms”. In: *Federated and Transfer Learning*. Springer, 2022, pp. 29–55.

[170] Ehsan Hallaji et al. “Label noise analysis meets adversarial training: A defense against label poisoning in federated learning”. In: *Knowledge-Based Systems* 266 (2023), p. 110384. ISSN: 0950-7051. DOI: https://doi.org/10.1016/j.knosys.2023.110384. URL: https://www.sciencedirect.com/science/article/pii/S095070512300134X.

[171] Sebastien Andreina et al. “BaFFLe: Backdoor Detection via Feedback-based Federated Learning”. In: *2021 IEEE 41st International Conference on Distributed Computing Systems (ICDCS)*. 2021, pp. 852–863. DOI: 10.1109/ICDCS51616.2021.00086.

[172] Elan Rosenfeld et al. “Certified Robustness to Label-Flipping Attacks via Randomized Smoothing”. In: *Proceedings of the 37th International Conference on Machine Learning*. Ed. by Hal Daumé III and Aarti Singh. Vol. 119. Proceedings of Machine Learning Research. PMLR, 13–18 Jul 2020, pp. 8230–8241. URL: https://proceedings.mlr.press/v119/rosenfeld20b.html.

[173] Xingchen Zhou et al. “Deep Model Poisoning Attack on Federated Learning”. In: *Future Internet* 13.3 (2021). ISSN: 1999-5903. URL: https://www.mdpi.com/1999-5903/13/3/73.

[174] Yang Liu et al. “Vertical federated learning: Concepts, advances, and challenges”. In: *IEEE Transactions on Knowledge and Data Engineering* (2024).

[175] Jiahui Geng et al. “Improved Gradient Inversion Attacks and Defenses in Federated Learning”. In: *IEEE Transactions on Big Data* (2023), pp. 1–13. DOI: 10.1109/TBDATA.2023.3239116.

[176] Yu Sun et al. “Client-Side Gradient Inversion Attack in Federated Learning Using Secure Aggregation”. In: *IEEE Internet of Things Journal* 11.17 (2024), pp. 28774–28786. DOI: 10.1109/JIOT.2024.3405939.

[177] Bosen Rao et al. “Privacy Inference Attack and Defense in Centralized and Federated Learning: A Comprehensive Survey”. In: *IEEE Transactions on Artificial Intelligence* (2024), pp. 1–22. DOI: 10.1109/TAI.2024.3363670.

[178] Kang Wei et al. “Federated Learning With Differential Privacy: Algorithms and Performance Analysis”. In: *IEEE Transactions on Information Forensics and Security* 15 (2020), pp. 3454–3469. DOI: 10.1109/TIFS.2020.2988575.

[179] Kummari Naveen Kumar, Chalavadi Krishna Mohan, and Linga Reddy Cenkeramaddi. “The Impact of Adversarial Attacks on Federated Learning: A Survey”. In: *IEEE Transactions on Pattern Analysis and Machine Intelligence* 46.5 (2024), pp. 2672–2691. DOI: 10.1109/TPAMI.2023.3322785.

[180] Wenkai Yang et al. “Watch out for your agents! investigating backdoor threats to llm-based agents”. In: *Advances in Neural Information Processing Systems* 37 (2024), pp. 100938–100964.

[181] Minrui Xu et al. “When large language model agents meet 6G networks: Perception, grounding, and alignment”. In: *IEEE Wireless Communications* (2024).

[182] Feibo Jiang et al. “Large language model enhanced multi-agent systems for 6G communications”. In: *IEEE Wireless Communications* (2024).

[183] Lewis Hammond et al. “Multi-agent risks from advanced ai”. In: *arXiv preprint arXiv:2502.14143* (2025).

[184] Martin BH Weiss et al. “On the application of blockchains to spectrum management”. In: *IEEE Transactions on Cognitive Communications and Networking* 5.2 (2019), pp. 193–205.

[185] L. Prompting. *Sandwich defense*. Tech. rep. Accessed: 2026-01-16. 2023. URL: https://learnprompting.org/docs/%20prompt%20hacking/defensive%20measures/sandwich%20defense.

[186] Neel Jain et al. *Baseline defenses for adversarial attacks against aligned language models*. Tech. rep. 2023.

[187] Jose Selvi. *Exploring Prompt Injection Attacks*. Tech. rep. Accessed: 2026-01-16. 2022. URL: https://nccgroup.com/au/research-blog/%20exploring-prompt-injection-attacks/.

[188] Benji Peng et al. “Jailbreaking and mitigation of vulnerabilities in large language models”. In: *arXiv preprint arXiv:2410.15236* (2024).

[189] Md Noor-A-Rahim et al. “6G for vehicle-to-everything (V2X) communications: Enabling technologies, challenges, and opportunities”. In: *Proceedings of the IEEE* 110.6 (2022), pp. 712–734.

[190] Fatima Salahdine, Tao Han, and Ning Zhang. “Security in 5G and beyond recent advances and future challenges”. In: *Security and Privacy* 6.1 (2023), e271.

[191] Selma Yahia, Valeria Loscri, and Prakriti Saxena. “Enhancing Security in 6G Vehicular Networks: Leveraging VLC and MMW Integration and Cooperative Relaying Technique”. In: *2023 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech)*. IEEE. 2023, pp. 0711–0716.

[192] Kaigui Bian, Gaoxiang Zhang, and Lingyang Song. “Toward secure crowd sensing in vehicle-to-everything networks”. In: *IEEE Network* 32.2 (2017), pp. 126–131.

[193] Manabu Tsukada et al. “Misbehavior detection using collective perception under privacy considerations”. In: *2022 IEEE 19th Annual Consumer Communications & Networking Conference (CCNC)*. IEEE. 2022, pp. 808–814.

[194] Andres Vejar, Faysal Marzuk, and Piotr Choda. “k-anonymity in Resource Allocation for Vehicle-to-Everything (V2X) Systems”. In: *Journal of Telecommunications and Information Technology* Special Issue (Feb. 2025), pp. 1–4. DOI: 10.26636/jtit.2025.FITCE2024.1998. URL: https://jtit.pl/jtit/article/view/1998.

[195] Sujash Naskar et al. “Pseudo-Random Identification and Efficient Privacy-Preserving V2X Communication for IoV Networks”. In: *IEEE Access* (2024).

[196] Yiliang Liu, Hsiao-Hwa Chen, and Liangmin Wang. “Physical Layer Security for Next Generation Wireless Networks: Theories, Technologies, and Challenges”. In: *IEEE Communications Surveys & Tutorials* 19.1 (2017), pp. 347–376. ISSN: 1553-877X. DOI: 10.1109/COMST.2016.2598968. URL: https://ieeexplore.ieee.org/document/7539590 (visited on 03/04/2024).

[197] Vinay Rishiwal et al. “Exploring secure V2X communication networks for human-centric security and privacy in smart cities”. In: *IEEE Access* (2024).

[198] Muhammad Awais Khan et al. “Robust, resilient and reliable architecture for v2x communications”. In: *IEEE Transactions on Intelligent Transportation Systems* 22.7 (2021), pp. 4414–4430.

[199] Roshan Sedar et al. “A comprehensive survey of V2X cybersecurity mechanisms and future research paths”. In: *IEEE Open Journal of the Communications Society* 4 (2023), pp. 325–391.

[200] Zhihao Ma et al. “A blockchain-based trusted data management scheme in edge computing”. In: *IEEE Transactions on Industrial Informatics* 16.3 (2020), pp. 2013–2021.

[201] Aymene Selamnia et al. “Edge computing-enabled intrusion detection for c-v2x networks using federated learning”. In: *GLOBECOM 2022-2022 IEEE Global Communications Conference*. IEEE. 2022, pp. 2080–2085.

[202] Yijie Xun, Jiajia Liu, and Yanning Zhang. “Side-channel analysis for intelligent and connected vehicle security: A new perspective”. In: *Ieee Network* 34.2 (2019), pp. 150–157.

[203] Ladan Khaloopour et al. “Resilience-by-design in 6G networks: Literature review and novel enabling concepts”. In: *IEEE access* (2024).

[204] Halit Bugra Tulay and Can Emre Koksal. “Sybil attack detection based on signal clustering in vehicular networks”. In: *IEEE Transactions on Machine Learning in Communications and Networking* 2 (2024), pp. 753–765.

[205] Kevin Herman Muraro Gularte et al. “Safeguarding the V2X pathways: Exploring the cybersecurity landscape through systematic review”. In: *IEEE Access* 12 (2024), pp. 72871–72895.

[206] Zhe Yang et al. “Blockchain-based decentralized trust management in vehicular networks”. In: *IEEE Internet of Things Journal* 6.2 (2019), pp. 1495–1505.

[207] Maria Papaioannou, Georgios Mantas, and Jonathan Rodriguez. “An Overview of Security and Privacy Threats for Massive IoT Applications in the 6G Era”. In: *2024 IEEE 29th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*. 2024, pp. 1–6. DOI: 10.1109/CAMAD62243.2024.10942897.

[208] Chonggang Wang and Akbar Rahman. “Quantum-enabled 6G wireless networks: Opportunities and challenges”. In: *IEEE Wireless Communications* 29.1 (2022), pp. 58–69.

[209] Kumar Prateek et al. “Quantum secured 6G technology-based applications in Internet of Everything”. In: *Telecommunication Systems* 82.2 (2023), pp. 315–344.

[210] Khan Maaz Bin Hasan et al. “Blockchain technology meets 6 G wireless networks: A systematic survey”. In: *Alexandria Engineering Journal* 92 (2024), pp. 199–220.

[211] Tharaka Hewa et al. “The role of blockchain in 6G: Challenges, opportunities and research directions”. In: *2020 2nd 6G Wireless Summit (6G SUMMIT)* (2020), pp. 1–5.

[212] Taras Maksymyuk et al. “Blockchain-empowered framework for decentralized network management in 6G”. In: *IEEE Communications Magazine* 58.9 (2020), pp. 86–92.

[213] Harsh Desai, Murat Kantarcioglu, and Lalana Kagal. “A hybrid blockchain architecture for privacy-enabled and accountable auctions”. In: *2019 IEEE International Conference on Blockchain (Blockchain)*. IEEE. 2019, pp. 34–43.

[214] H Pennanen et al. “6g: The intelligent network of everything–a comprehensive vision, survey, and tutorial”. In: *arXiv preprint arXiv:2407.09398* (2024).

[215] Fatima Salahdine, Tao Han, and Ning Zhang. “5G, 6G, and Beyond: Recent advances and future challenges”. In: *Annals of Telecommunications* 78.9 (2023), pp. 525–549.

[216] Xiaohu You et al. “Towards 6G wireless communication networks: vision, enabling technologies, and new paradigm shifts”. In: *Science China Information Sciences* 64.1 (2021), pp. 1–74.

[217] Dinh C Nguyen et al. “Blockchain for 5G and beyond networks: A state of the art survey”. In: *Journal of Network and Computer Applications*. Vol. 166. 2020, p. 102693.

[218] Xintong Ling et al. “Blockchain radio access network (B-RAN): towards decentralized secure radio access paradigm”. In: *IEEE Access* 7 (2019), pp. 9714–9723.

[219] Zhengyu Zhou et al. “Blockchain-empowered secure spectrum sharing for 5G heterogeneous networks”. In: *IEEE Network* 34.1 (2020), pp. 24–31.

[220] Oscar Novo. “Blockchain meets IoT: An architecture for scalable access management in IoT”. In: *IEEE Internet of Things Journal* 5.2 (2018), pp. 1184–1195.

[221] Lanfranco Zanzi et al. “NSBchain: A secure blockchain framework for network slicing brokerage”. In: *ICC 2020-2020 IEEE International Conference on Communications (ICC)*. IEEE. 2020, pp. 1–7.

[222] Mohammed Amine Togou et al. “DBNS: A distributed blockchain-enabled network slicing framework for 5G networks”. In: *IEEE Communications Magazine* 58.11 (2020), pp. 90–96.

[223] Marco Giordani et al. “Toward 6G networks: Use cases and technologies”. In: *IEEE Communications Magazine* 58.3 (2020), pp. 55–61.

[224] Michele Mosca. “Cybersecurity in an era with quantum computers: Will we be ready?” In: *IEEE Security & Privacy* 16.5 (2018), pp. 38–41.

[225] Peter W. Shor. “Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer”. In: *SIAM Journal on Computing* 26.5 (1997), pp. 1484–1509.

[226] John Preskill. “Quantum computing in the NISQ era and beyond”. In: *Quantum* 2 (2018), p. 79.

[227] Ronald L. Rivest, Adi Shamir, and Leonard Adleman. “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems”. In: *Communications of the ACM* 21.2 (1978), pp. 120–126. DOI: 10.1145/359340.359342.

[228] 3GPP. *Security Architecture and Procedures for 5G System (Release 17)*. 3GPP TS 33.501 V17.3.0. 2022. URL: https://www.3gpp.org/DynaReport/33501.htm.

[229] Daniel J Bernstein, Johannes Buchmann, and Erik Dahmen. “Post-quantum cryptography”. In: *Springer Berlin Heidelberg*. Introduction to Post-Quantum Cryptography. 2009.

[230] Nicolas Gisin et al. “Quantum cryptography”. In: *Reviews of Modern Physics* 74.1 (2002), p. 145.

[231] Ericsson. *Quantum Computing and 5G/6G Security*. White Paper. Accessed: 2025-04-11. 2023. URL: https://www.ericsson.com/en/reports-and-papers/further-insights/quantum-computing-and-5g-6g-security.

[232] Charles H. Bennett and Gilles Brassard. “Quantum cryptography: Public key distribution and coin tossing”. In: *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*. IEEE. 1984, pp. 175–179.

[233] Valerio Scarani et al. “The security of practical quantum key distribution”. In: *Reviews of Modern Physics* 81.3 (2009), p. 1301.

[234] Renato Renner. “Security of quantum key distribution”. In: *International Journal of Quantum Information* 6.1 (2008), pp. 1–127.

[235] Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen. “Decoy state quantum key distribution”. In: *Physical Review Letters* 94.23 (2005), p. 230504.

[236] Hoi-Kwong Lo, Marcos Curty, and Bing Qi. “Measurement-device-independent quantum key distribution”. In: *Physical Review Letters* 108.13 (2012), p. 130503.

[237] Frédéric Grosshans and Philippe Grangier. “Continuous variable quantum cryptography using coherent states”. In: *Physical Review Letters* 88.5 (2002), p. 057902.

[238] Christian Weedbrook et al. “Gaussian quantum information”. In: *Reviews of Modern Physics* 84.2 (2012), p. 621.

[239] Marco Lucamarini et al. “Overcoming the rate–distance limit of quantum key distribution without quantum repeaters”. In: *Nature* 557.7705 (2018), pp. 400–403.

[240] Joshua W. Silverstone et al. “Silicon Quantum Photonics”. In: *IEEE Journal of Selected Topics in Quantum Electronics* 22.6 (Nov. 2016), pp. 390–402. ISSN: 1077-260X, 1558-4542. DOI: 10.1109/JSTQE.2016.2573218. (Visited on 06/30/2025).

[241] Y. Zhang, Y. Ding, et al. “An integrated silicon photonic chip platform for continuous-variable QKD”. In: *Nature Photonics* 13 (2019), pp. 839–842.

[242] Yoann Piétri et al. “Experimental Demonstration of Continuous-Variable Quantum Key Distribution with a Silicon Photonics Integrated Receiver”. In: *Optica Quantum* 2.6 (Dec. 2024), p. 428. ISSN: 2837-6714. DOI: 10.1364/OPTICAQ.534699. arXiv: 2311.03978 [quant-ph]. (Visited on 07/09/2025).

[243] Lang Li et al. “Continuous-Variable Quantum Key Distribution with on-Chip Light Sources”. In: *Photonics Research* 11.4 (Apr. 2023), p. 504. ISSN: 2327-9125. DOI: 10.1364/PRJ.473328. (Visited on 06/30/2025).

[244] Adnan A. E. Hajomer et al. *Chip-Based 16 GBaud Continuous-Variable Quantum Key Distribution*. Apr. 2025. DOI: 10.48550/arXiv.2504.09308. arXiv: 2504.09308 [quant-ph]. (Visited on 04/29/2025).

[245] A. Boaron et al. “Secure QKD over 421 km of optical fiber”. In: *Physical Review Letters* 121 (2018), p. 190502.

[246] P. Senellart, G. Solomon, and A. White. “High-performance semiconductor quantum-dot single-photon sources”. In: *Nature Nanotechnology* 12 (2017), pp. 1026–1039.

[247] L. Schweickert, K. D. Jöns, K. D. Zeuner, et al. “Near-unity indistinguishability single photon source for large-scale integrated quantum optics”. In: *Nature Communications* 9 (2018), pp. 1–7.

[248] E. Diamanti et al. “Practical challenges in quantum key distribution”. In: *npj Quantum Information* 2 (2016), p. 16025.

[249] H.-J. Briegel et al. “Quantum repeaters: The role of imperfect local operations in quantum communication”. In: *Physical Review Letters* 81.26 (1998), p. 5932.

[250] N. Sangouard et al. “Quantum repeaters based on atomic ensembles and linear optics”. In: *Reviews of Modern Physics* 83 (2011), p. 33.

[251] W. J. Munro et al. “Inside quantum repeaters”. In: *IEEE Journal of Selected Topics in Quantum Electronics* 21.3 (2015), pp. 78–90.

[252] M. K. Bhaskar et al. “Experimental demonstration of memory-enhanced quantum communication”. In: *Nature* 580 (2020), pp. 60–64.

[253] Pieter-Jan Stas et al. “Robust multi-qubit quantum network node with integrated error detection”. In: *Science* 378.6619 (2022), pp. 557–560. DOI: 10.1126/science.add9771. URL: https://www.science.org/doi/10.1126/science.add9771.

[254] Y. Yu et al. “Entanglement of two quantum memories via fibers over dozens of kilometers”. In: *Nature* 578.7794 (2020), pp. 240–245.

[255] S. Pirandola et al. “Fundamental limits of repeaterless quantum communications”. In: *Nature Communications* 8 (2017), p. 15043.

[256] M. Pompili et al. “Realization of a multinode quantum network of remote solid-state qubits”. In: *Science* 372.6539 (2021), pp. 259–264.

[257] Momtchil Peev et al. “The SECOQC quantum key distribution network in Vienna”. In: *New Journal of Physics* 11.7 (2009), p. 075001.

[258] M. Sasaki, M. Fujiwara, H. Ishizuka, et al. "Field test of quantum key distribution in the Tokyo QKD network". In: *Optics Express* 19.11 (2011), pp. 10387–10409.

[259] BT and Toshiba. *BT and Toshiba Launch First Commercial Trial of Quantum Secured Communication Services*. Press release. BT Group. Apr. 2022. URL: https://newsroom.bt.com/bt-and-toshiba-launch-first-commercial-trial-of-quantum-secured-communication-services/.

[260] Shengkai Liao et al. "Satellite-to-ground quantum key distribution". In: *Nature* 549.7670 (2017), pp. 43–47.

[261] Ben Amies-King et al. "Quantum Communications Feasibility Tests over a UK-Ireland 224 km Undersea Link". In: *Entropy* 25.12 (2023), p. 1572. DOI: 10.3390/e25121572. URL: https://www.mdpi.com/1099-4300/25/12/1572.

[262] ETSI Industry Specification Group (ISG) QSC. *Quantum Safe Cryptography and Security: An Introduction, Benefits, Enablers and Challenges*. ETSI White Paper No. 8. Available at: https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp8_qsafe.pdf. 2018.

[263] Michela Svaluto Moreolo et al. "SDN-enabled CV-QKD for Quantum Secure Communication in Open and Disaggregated 6G Networks". In: *Next-Generation Optical Communication: Components, Sub-Systems, and Systems XIII*. Vol. 12894. SPIE, Mar. 2024, pp. 119–128. DOI: 10.1117/12.3002510. (Visited on 07/25/2025).

[264] M. Pittaluga et al. "600 km repeater-like quantum communications with dual-band stabilization". In: *Nature Photonics* 15 (2021), pp. 530–535.

[265] Y. S. Lo et al. "Simplified intensity- and phase-modulated transmitter for modulator-free decoy-state quantum key distribution". In: *Optics Express* 31.12 (2023), pp. 19378–19389.

[266] Nick Aquina et al. "A Critical Analysis of Deployed Use Cases for Quantum Key Distribution and Comparison with Post-Quantum Cryptography". In: *EPJ Quantum Technology* 12.1 (Dec. 2025). ISSN: 2662-4400, 2196-0763. DOI: 10.1140/epjqt/s40507-025-00350-5. (Visited on 07/18/2025).

[267] Gorjan Alagic et al. *Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process*. NIST Interagency/Internal Report (NISTIR) 8309. National Institute of Standards and Technology, 2020. DOI: 10.6028/NIST.IR.8309. URL: https://doi.org/10.6028/NIST.IR.8309.

[268] Gorjan Alagic et al. *Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process*. NIST Interagency/Internal Report (NISTIR) 8413. National Institute of Standards and Technology, 2022. DOI: 10.6028/NIST.IR.8413. URL: https://doi.org/10.6028/NIST.IR.8413.

[269] Kanza Cherkaoui Dekkaki, Igor Tasic, and Maria-Dolores Cano. "Exploring Post-Quantum Cryptography: Review and Directions for the Transition Process". In: *Technologies* 12.12 (2024), p. 241. DOI: 10.3390/technologies12120241. URL: https://www.mdpi.com/2227-7080/12/12/241.

[270] Elif Dicle Demir, Buse Bilgin, and Mehmet Cengiz Onbasli. *Performance Analysis and Industry Deployment of Post-Quantum Cryptography Algorithms*. Mar. 2025. DOI: 10.48550/arXiv.2503.12952. arXiv: 2503.12952 [cs]. (Visited on 07/09/2025).

[271] Alexey K. Fedorov. "Deploying Hybrid Quantum-Secured Infrastructure for Applications: When Quantum and Post-Quantum Can Work Together". In: *Frontiers in Quantum Science and Technology* 2 (2023), p. 1164428. DOI: 10.3389/frqst.2023.1164428. URL: https://www.frontiersin.org/articles/10.3389/frqst.2023.1164428/full.

[272] Peng Zeng, Debdeep Bandyopadhyay, Juan A. M. Méndez, et al. "Practical Hybrid PQC-QKD Protocols with Enhanced Security and Performance". In: *arXiv preprint arXiv:2411.01086* (2024). URL: https://arxiv.org/pdf/2411.01086.pdf.

[273] Alexey K. Fedorov, Kirill V. Ushakov, and Evgeny O. Kiktenko. "Quantum and Post-Quantum Secure Communications for Critical Infrastructures". In: *Quantum Reports* 4.4 (2022), pp. 697–712. DOI: 10.3390/quantum4040045. URL: https://www.mdpi.com/2624-960X/4/4/45.

[274] Jaime S. Buruaga et al. "Versatile Quantum-Safe Hybrid Key Exchange and Its Application to MACsec". In: *EPJ Quantum Technology* 12.1 (Dec. 2025). ISSN: 2662-4400, 2196-0763. DOI: 10.1140/epjqt/s40507-025-00382-x. (Visited on 07/18/2025).

[275] Engin Zeydan et al. "Quantum Technologies for Beyond 5G and 6G Networks: Applications, Opportunities, and Challenges". In: *arXiv preprint arXiv:2504.17133* (2025). URL: https://arxiv.org/abs/2504.17133.

[276] Gorjan Alagic et al. *Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process*. NIST Interagency/Internal Report (NISTIR) 8240. National Institute of Standards and Technology, Jan. 2019. DOI: 10.6028/NIST.IR.8240. URL: https://doi.org/10.6028/NIST.IR.8240.

[277] William Newhouse et al. *Migration to Post-Quantum Cryptography: Preparation and Strategy*. NIST Special Publication 1800-38B. Preliminary Draft. National Institute of Standards and Technology, Dec. 2023. URL: https://www.nccoe.nist.gov/sites/default/files/2023-12/pqc-migration-nist-sp-1800-38b-preliminary-draft.pdf.

[278] European Union Agency for Cybersecurity (ENISA). *Post-Quantum Cryptography: Current State and Quantum Mitigation*. Tech. rep. ENISA, 2021. URL: https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation.

[279] Alfred J. Menezes, Scott A. Vanstone, and Paul C. Van Oorschot. *Handbook of Applied Cryptography*. 1st. USA: CRC Press, Inc., 1996. ISBN: 0849385237.

[280] A. D. Wyner. "The Wire-Tap Channel". In: *The Bell System Technical Journal* 54.8 (Oct. 1975), pp. 1355–1387. ISSN: 0005-8580. DOI: 10.1002/j.1538-7305.1975.tb02040.x. URL: https://ieeexplore.ieee.org/document/6772207 (visited on 03/18/2025).

[281] W. Diffie and M. Hellman. "New Directions in Cryptography". In: *IEEE Transactions on Information Theory* 22.6 (Nov. 1976), pp. 644–654. ISSN: 1557-9654. DOI: 10.1109/TIT.1976.1055638. URL: https://ieeexplore.ieee.org/document/1055638 (visited on 03/03/2024).

[282] C. E. Shannon. "A Mathematical Theory of Communication". In: *The Bell System Technical Journal* 27.3 (July 1948), pp. 379–423. ISSN: 0005-8580. DOI: 10.1002/j.1538-7305.1948.tb01338.x. URL: https://ieeexplore.ieee.org/document/6773024/?arnumber=6773024 (visited on 03/19/2025).

[283] I Csiszár. "Almost Independence and Secrecy Capacity". In: *Probl. Peredachi Inf.,* 32:1 (1996), pp. 48–57.

[284] Jehad M. Hamamreh, Haji M. Furqan, and Huseyin Arslan. "Classifications and Applications of Physical Layer Security Techniques for Confidentiality: A Comprehensive Survey". In: *IEEE Communications Surveys & Tutorials* 21.2 (2019), pp. 1773–1828. ISSN: 1553-877X. DOI: 10.1109/COMST.2018.2878035. URL: https://ieeexplore.ieee.org/document/8509094/?arnumber=8509094 (visited on 03/24/2025).

[285] U.M. Maurer. "Secret Key Agreement by Public Discussion from Common Information". In: *IEEE Transactions on Information Theory* 39.3 (May 1993), pp. 733–742. ISSN: 1557-9654. DOI: 10.1109/18.256484. URL: https://ieeexplore.ieee.org/document/256484/?arnumber=256484 (visited on 03/20/2025).

[286] R. Ahlswede and I. Csiszar. "Common Randomness in Information Theory and Cryptography. I. Secret Sharing". In: *IEEE Transactions on Information Theory* 39.4 (July 1993), pp. 1121–1132. ISSN: 1557-9654. DOI: 10.1109/18.243431. URL: https://ieeexplore.ieee.org/document/243431 (visited on 03/26/2025).

[287] R. Ahlswede and I. Csiszar. "Common Randomness in Information Theory and Cryptography. II. CR Capacity". In: *IEEE Transactions on Information Theory* 44.1 (Jan. 1998), pp. 225–240. ISSN: 1557-9654. DOI: 10.1109/18.651026. URL: https://ieeexplore.ieee.org/document/651026 (visited on 03/26/2025).

[288] U. Maurer and S. Wolf. "Secret-Key Agreement over Unauthenticated Public Channels .I. Definitions and a Completeness Result". In: *IEEE Transactions on Information Theory* 49.4 (Apr. 2003), pp. 822–831. ISSN: 1557-9654. DOI: 10.1109/TIT.2003.809563. URL: https://ieeexplore.ieee.org/document/1193793 (visited on 03/26/2025).

[289] Matthieu Bloch et al. "Wireless Information-Theoretic Security". In: *IEEE Transactions on Information Theory* 54.6 (June 2008), pp. 2515–2534. ISSN: 1557-9654. DOI: 10.1109/TIT.2008.921908. URL: https://ieeexplore.ieee.org/document/4529264/?arnumber=4529264 (visited on 03/18/2025).

[290] Alireza Shamsoshoara et al. "A Survey on Physical Unclonable Function (PUF)-Based Security Solutions for Internet of Things". In: *Computer Networks* 183 (Dec. 2020), p. 107593. ISSN: 1389-1286. DOI: 10.1016/j.comnet.2020.107593. URL: https://www.sciencedirect.com/science/article/pii/S1389128620312275 (visited on 03/27/2025).

[291] Tasneem Assaf et al. "High-Rate Secret Key Generation Using Physical Layer Security and Physical Unclonable Functions". In: *IEEE Open Journal of the Communications Society* 4 (2023), pp. 209–225. ISSN: 2644-125X. DOI: 10.1109/OJCOMS.2023.3234338. URL: https://ieeexplore.ieee.org/document/10007641/?arnumber=10007641 (visited on 03/27/2025).

[292] S. Leung-Yan-Cheong and M. Hellman. "The Gaussian Wire-Tap Channel". In: *IEEE Transactions on Information Theory* 24.4 (July 1978), pp. 451–456. ISSN: 1557-9654. DOI: 10.1109/TIT.1978.1055917. URL: https://ieeexplore.ieee.org/document/1055917/?arnumber=1055917 (visited on 03/21/2025).

[293] H. Vincent Poor and Rafael F. Schaefer. "Wireless Physical Layer Security". In: *Proceedings of the National Academy of Sciences* 114.1 (Jan. 2017), pp. 19–26. DOI: 10.1073/pnas.1618130114. URL: https://www.pnas.org/doi/10.1073/pnas.1618130114 (visited on 08/19/2024).

[294] I. Csiszar and J. Korner. "Broadcast Channels with Confidential Messages". In: *IEEE Transactions on Information Theory* 24.3 (May 1978), pp. 339–348. ISSN: 1557-9654. DOI: 10.1109/TIT.1978.1055892. URL: https://ieeexplore.ieee.org/document/1055892/?arnumber=1055892 (visited on 03/19/2025).

[295] Ruoheng Liu et al. "The Discrete Memoryless Multiple Access Channel with Confidential Messages". In: *2006 IEEE International Symposium on Information Theory*. July 2006, pp. 957–961. DOI: 10.1109/ISIT.2006.261801. URL: https://ieeexplore.ieee.org/document/4036106/?arnumber=4036106 (visited on 03/27/2025).

[296] Yingbin Liang et al. "Capacity of Cognitive Interference Channels With and Without Secrecy". In: *IEEE Transactions on Information Theory* 55.2 (Feb. 2009), pp. 604–619. ISSN: 1557-9654. DOI: 10.1109/TIT.2008.2009584. URL: https://ieeexplore.ieee.org/document/4777619/?arnumber=4777619 (visited on 03/27/2025).

[297] O. Ozan Koyluoglu et al. "Interference Alignment for Secrecy". In: *IEEE Transactions on Information Theory* 57.6 (June 2011), pp. 3323–3332. ISSN: 1557-9654. DOI: 10.1109/TIT.2011.2132430. URL: https://ieeexplore.ieee.org/document/5773067/?arnumber=5773067 (visited on 03/27/2025).

[298] Yasutada Oohama. "Capacity Theorems for Relay Channels with Confidential Messages". In: *2007 IEEE International Symposium on Information Theory*. June 2007, pp. 926–930. DOI: 10.1109/ISIT.2007.4557113. URL: https://ieeexplore.ieee.org/document/4557113/?arnumber=4557113 (visited on 03/27/2025).

[299] Lifeng Lai and Hesham El Gamal. "The Relay–Eavesdropper Channel: Cooperation for Secrecy". In: *IEEE Transactions on Information Theory* 54.9 (Sept. 2008), pp. 4005–4019. ISSN: 1557-9654. DOI: 10.1109/TIT.2008.928272. URL: https://ieeexplore.ieee.org/document/4608977/?arnumber=4608977 (visited on 03/27/2025).

[300] Megha. S. Kumar, R. Ramanathan, and M. Jayakumar. "Key Less Physical Layer Security for Wireless Networks: A Survey". In: *Engineering Science and Technology, an International Journal* 35 (Nov. 2022), p. 101260. ISSN: 2215-0986. DOI: 10.1016/j.jestch.2022.101260. URL: https://www.sciencedirect.com/science/article/pii/S2215098622001690 (visited on 03/18/2025).

[301] Andrew Thangaraj et al. "Applications of LDPC Codes to the Wiretap Channel". In: *IEEE Transactions on Information Theory* 53.8 (Aug. 2007), pp. 2933–2945. ISSN: 1557-9654. DOI: 10.1109/TIT.2007.901143. URL: https://ieeexplore.ieee.org/document/4276938/?arnumber=4276938 (visited on 03/27/2025).

[302] Ruoheng Liu et al. "Nested Codes for Secure Transmission". In: *2008 IEEE 19th International Symposium on Personal, Indoor and Mobile Radio Communications*. Sept. 2008, pp. 1–5. DOI: 10.1109/PIMRC.2008.4699910. URL: https://ieeexplore.ieee.org/document/4699910/?arnumber=4699910 (visited on 03/27/2025).

[303] Hessam Mahdavifar and Alexander Vardy. "Achieving the Secrecy Capacity of Wiretap Channels Using Polar Codes". In: *IEEE Transactions on Information Theory* 57.10 (Oct. 2011), pp. 6428–6443. ISSN: 1557-9654. DOI: 10.1109/TIT.2011.2162275. URL: https://ieeexplore.ieee.org/document/6034749/?arnumber=6034749 (visited on 03/27/2025).

[304] I.J. Cox et al. "Secure Spread Spectrum Watermarking for Multimedia". In: *IEEE Transactions on Image Processing* 6.12 (Dec. 1997), pp. 1673–1687. ISSN: 1941-0042. DOI: 10.1109/83.650120. URL: https://ieeexplore.ieee.org/document/650120 (visited on 08/08/2024).

[305] Xiang Li et al. "Physical Layer Watermarking of Direct Sequence Spread Spectrum Signals". In: *MILCOM 2013 - 2013 IEEE Military Communications Conference*. San Diego, CA, USA: IEEE, Nov. 2013, pp. 476–481. ISBN: 978-0-7695-5124-1. DOI: 10.1109/MILCOM.2013.88. URL: http://ieeexplore.ieee.org/document/6735668/ (visited on 08/08/2024).

[306] Satashu Goel and Rohit Negi. "Guaranteeing Secrecy Using Artificial Noise". In: *IEEE Transactions on Wireless Communications* 7.6 (June 2008), pp. 2180–2189. ISSN: 1558-2248. DOI: 10.1109/TWC.2008.060848. URL: https://ieeexplore.ieee.org/document/4543070 (visited on 03/27/2025).

[307] Biao He, Yechao She, and Vincent K. N. Lau. "Artificial Noise Injection for Securing Single-Antenna Systems". In: *IEEE Transactions on Vehicular Technology* 66.10 (Oct. 2017), pp. 9577–9581. ISSN: 1939-9359. DOI: 10.1109/TVT.2017.2703159. URL: https://ieeexplore.ieee.org/document/7924410 (visited on 03/18/2025).

[308] Shyamnath Gollakota and Dina Katabi. "Physical Layer Wireless Security Made Fast and Channel Independent". In: *2011 Proceedings IEEE INFOCOM*. Apr. 2011, pp. 1125–1133. DOI: 10.1109/INFCOM.2011.5934889. URL: https://ieeexplore.ieee.org/document/5934889 (visited on 08/05/2024).

[309] Simone Soderi et al. "Physical Layer Security Based on Spread-Spectrum Watermarking and Jamming Receiver". In: *Transactions on Emerging Telecommunications Technologies* 28.7 (2017), e3142. ISSN: 2161-3915. DOI: 10.1002/ett.3142. URL: https://onlinelibrary.wiley.com/doi/abs/10.1002/ett.3142 (visited on 04/18/2024).

[310] L. Xiao et al. "A Physical-Layer Technique to Enhance Authentication for Mobile Terminals". In: *2008 IEEE International Conference on Communications*. May 2008, pp. 1520–1524. DOI: 10.1109/ICC.2008.294. URL: https://ieeexplore.ieee.org/document/4533330/?arnumber=4533330 (visited on 03/28/2025).

[311] Kai Zeng, Kannan Govindan, and Prasant Mohapatra. "Non-Cryptographic Authentication and Identification in Wireless Networks [Security and Privacy in Emerging Wireless Networks]". In: *IEEE Wireless Communications* 17.5 (Oct. 2010), pp. 56–62. ISSN: 1558-0687. DOI: 10.1109/MWC.2010.5601959. URL: https://ieeexplore.ieee.org/abstract/document/5601959 (visited on 03/18/2025).

[312] Neal Patwari and Sneha K. Kasera. "Robust Location Distinction Using Temporal Link Signatures". In: *Proceedings of the 13th Annual ACM International Conference on Mobile Computing and Networking*. Montréal Québec Canada: ACM, Sept. 2007, pp. 111–122. ISBN: 978-1-59593-681-3. DOI: 10.1145/1287853.1287867. URL: https://dl.acm.org/doi/10.1145/1287853.1287867 (visited on 03/28/2025).

[313] Vladimir Brik et al. "Wireless Device Identification with Radiometric Signatures". In: *Proceedings of the 14th ACM International Conference on Mobile Computing and Networking*. MobiCom '08. New York, NY, USA: Association for Computing Machinery, Sept. 2008, pp. 116–127. ISBN: 978-1-60558-096-8. DOI: 10.1145/1409944.1409959. URL: https://dl.acm.org/doi/10.1145/1409944.1409959 (visited on 03/28/2025).

[314] G. Edward Suh and Srinivas Devadas. "Physical Unclonable Functions for Device Authentication and Secret Key Generation". In: *2007 44th ACM/IEEE Design Automation Conference*. June 2007, pp. 9–14. URL: https://ieeexplore.ieee.org/document/4261134 (visited on 03/28/2025).

[315] Yi-Sheng Shiu et al. "Physical Layer Security in Wireless Networks: A Tutorial". In: *IEEE Wireless Communications* 18.2 (Apr. 2011), pp. 66–74. ISSN: 1558-0687. DOI: 10.1109/MWC.2011.5751298. (Visited on 03/18/2025).

[316] Aristides Mpitziopoulos et al. “Defending Wireless Sensor Networks from Jamming Attacks”. In: *2007 IEEE 18th International Symposium on Personal, Indoor and Mobile Radio Communications*. Sept. 2007, pp. 1–5. DOI: 10.1109/PIMRC.2007.4394775. URL: https://ieeexplore.ieee.org/document/4394775/?arnumber=4394775 (visited on 03/28/2025).

[317] Wali Ullah Khan et al. “Opportunities for Physical Layer Security in UAV Communication Enhanced with Intelligent Reflective Surfaces”. In: *IEEE Wireless Communications* 29.6 (Dec. 2022), pp. 22–28. ISSN: 1558-0687. DOI: 10.1109/MWC.001.2200125. URL: https://ieeexplore.ieee.org/document/10003076/?arnumber=10003076 (visited on 03/24/2025).

[318] Mohamed Amine Arfaoui et al. “Physical Layer Security for Visible Light Communication Systems: A Survey”. In: *IEEE Communications Surveys & Tutorials* 22.3 (2020), pp. 1887–1908. ISSN: 1553-877X. DOI: 10.1109/COMST.2020.2988615. URL: https://ieeexplore.ieee.org/document/9070153 (visited on 03/18/2025).

[319] Yongpeng Wu et al. “Secure Massive MIMO Transmission With an Active Eavesdropper”. In: *IEEE Transactions on Information Theory* 62.7 (July 2016), pp. 3880–3900. ISSN: 1557-9654. DOI: 10.1109/TIT.2016.2569118. URL: https://ieeexplore.ieee.org/document/7470273/ (visited on 05/23/2025).

[320] Santosh Timilsina, Dhanushka Kudathanthirige, and Gayan Amarasuriya. “Physical Layer Security in Cell-Free Massive MIMO”. In: *2018 IEEE Global Communications Conference (GLOBECOM)*. Dec. 2018, pp. 1–7. DOI: 10.1109/GLOCOM.2018.8647876. URL: https://ieeexplore.ieee.org/document/8647876 (visited on 03/31/2025).

[321] Jiahua Qiu, Kui Xu, and Xiaochen Xia. “Secure Transmission Based on Non-Overlapping AOA in Cell-Free Massive MIMO Networks”. In: *2020 IEEE/CIC International Conference on Communications in China (ICCC)*. Aug. 2020, pp. 588–593. DOI: 10.1109/ICCC49849.2020.9238973. URL: https://ieeexplore.ieee.org/document/9238973/?arnumber=9238973 (visited on 03/31/2025).

[322] Jiahua Qiu et al. “Secure Transmission Scheme Based on Fingerprint Positioning in Cell-Free Massive MIMO Systems”. In: *IEEE Transactions on Signal and Information Processing over Networks* 8 (2022), pp. 92–105. ISSN: 2373-776X. DOI: 10.1109/TSIPN.2022.3149112. URL: https://ieeexplore.ieee.org/document/9706316 (visited on 03/31/2025).

[323] Mahmoud Alageli et al. “Optimal Downlink Transmission for Cell-Free SWIPT Massive MIMO Systems With Active Eavesdropping”. In: *IEEE Transactions on Information Forensics and Security* 15 (2020), pp. 1983–1998. ISSN: 1556-6021. DOI: 10.1109/TIFS.2019.2954748. URL: https://ieeexplore.ieee.org/document/8907878/?arnumber=8907878 (visited on 03/31/2025).

[324] Salah Elhoushy, Mohamed Ibrahim, and Walaa Hamouda. “Exploiting RIS for Limiting Information Leakage to Active Eavesdropper in Cell-Free Massive MIMO”. In: *IEEE Wireless Communications Letters* 11.3 (Mar. 2022), pp. 443–447. ISSN: 2162-2345. DOI: 10.1109/LWC.2021.3130169. URL: https://ieeexplore.ieee.org/document/9625002 (visited on 03/31/2025).

[325] Xiang Gao et al. “Secure Optimal Precoding for User-Centric Cell-Free Massive MIMO System”. In: *IEEE Wireless Communications Letters* 12.1 (Jan. 2023), pp. 31–35. ISSN: 2162-2345. DOI: 10.1109/LWC.2022.3216050. URL: https://ieeexplore.ieee.org/document/9925607/ (visited on 05/23/2025).

[326] Xiangjun Ma et al. “Secrecy Performance Evaluation of Scalable Cell-Free Massive MIMO Systems: A Stochastic Geometry Approach”. In: *IEEE Transactions on Information Forensics and Security* 18 (2023), pp. 2826–2841. ISSN: 1556-6021. DOI: 10.1109/TIFS.2023.3268443. URL: https://ieeexplore.ieee.org/document/10105654 (visited on 11/22/2024).

[327] Mian Muaz Razaq et al. “Deep Reinforcement Learning-based Physical Layer Security Framework for Internet of Medical Things”. In: *IEEE Transactions on Consumer Electronics* (2024), pp. 1–1. ISSN: 1558-4127. DOI: 10.1109/TCE.2024.3521386. URL: https://ieeexplore.ieee.org/document/10812001/ (visited on 05/27/2025).

[328] Xianyu Zhang et al. “Secure Communications Over Cell-Free Massive MIMO Networks With Hardware Impairments”. In: *IEEE Systems Journal* 14.2 (June 2020), pp. 1909–1920. ISSN: 1937-9234. DOI: 10.1109/JSYST.2019.2919584. URL: https://ieeexplore.ieee.org/document/8734757/ (visited on 05/23/2025).

[329] Xianyu Zhang et al. “Secure Transmission in Cell-Free Massive MIMO Network with Phase Noise”. In: *2022 International Conference on Communications, Computing, Cybersecurity, and Informatics (CCCI)*. Oct. 2022, pp. 1–6. DOI: 10.1109/CCCI55352.2022.9926562. URL: https://ieeexplore.ieee.org/document/9926562/ (visited on 05/23/2025).

[330] Kun Wu et al. “Relay-Aided Physical Layer Security in Multi-User VLC with Single Light Source Using Cooperative Jamming”. In: *IEEE Transactions on Vehicular Technology* (2025), pp. 1–6. ISSN: 1939-9359. DOI: 10.1109/TVT.2025.3566084. URL: https://ieeexplore.ieee.org/document/10981625/ (visited on 05/28/2025).

[331] S. Soderi and R. De Nicola. “6G Networks Physical Layer Security Using RGB Visible Light Communications”. In: *IEEE Access* 10 (2022), pp. 5482–5496. ISSN: 2169-3536. DOI: 10.1109/ACCESS.2021.3139456. URL: https://ieeexplore.ieee.org/document/9665788 (visited on 08/07/2024).

[332] Simone Soderi et al. “VLC Physical Layer Security through RIS-aided Jamming Receiver for 6G Wireless Networks”. In: *2022 19th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)*. Sept. 2022, pp. 370–378. DOI: 10.1109/SECON55815.2022.9918547. arXiv: 2205.09026 [cs]. URL: http://arxiv.org/abs/2205.09026 (visited on 07/02/2024).

[333] Maaz Haider, Amena Ejaz Aziz, and Rashid Iqbal. “Can IRS Assist PLS for Indoor VLC?” In: *Physical Communication* 71 (Aug. 2025), p. 102703. ISSN: 1874-4907. DOI: 10.1016/j.phycom.2025.102703. URL: https://www.sciencedirect.com/science/article/pii/S1874490725001065 (visited on 05/28/2025).

[334] Omar Maraqa et al. “Max-Min Secrecy Rate and Secrecy Energy Efficiency Optimization for RIS-Aided VLC Systems: RSMA Versus NOMA”. In: *IEEE Open Journal of Vehicular Technology* (2025), pp. 1–14. ISSN: 2644-1330. DOI: 10.1109/OJVT.2025.3568436. URL: https://ieeexplore.ieee.org/document/10994327/ (visited on 05/28/2025).

[335] Nan Yang and Akram Shafie. “Terahertz Communications for Massive Connectivity and Security in 6G and Beyond Era”. In: *IEEE Communications Magazine* 62.2 (Feb. 2024), pp. 72–78. ISSN: 1558-1896. DOI: 10.1109/MCOM.001.2200421. URL: https://ieeexplore.ieee.org/document/9933498 (visited on 03/19/2025).

[336] Weijun Gao et al. “Distance-Adaptive Absorption Peak Modulation (DA-APM) for Terahertz Covert Communications”. In: *IEEE Transactions on Wireless Communications* 20.3 (Mar. 2021), pp. 2064–2077. ISSN: 1558-2248. DOI: 10.1109/TWC.2020.3038902. URL: https://ieeexplore.ieee.org/document/9271892/?arnumber=9271892 (visited on 04/01/2025).

[337] Vitaly Petrov et al. “Exploiting Multipath Terahertz Communications for Physical Layer Security in Beyond 5G Networks”. In: *IEEE INFOCOM 2019 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. Apr. 2019, pp. 865–872. DOI: 10.1109/INFCOMW.2019.8845312. URL: https://ieeexplore.ieee.org/document/8845312/?arnumber=8845312 (visited on 04/01/2025).

[338] Xingbo Lu et al. “Robust and Secure Beamforming for Intelligent Reflecting Surface Aided mmWave MISO Systems”. In: *IEEE Wireless Communications Letters* 9.12 (Dec. 2020), pp. 2068–2072. ISSN: 2162-2345. DOI: 10.1109/LWC.2020.3012664. URL: https://ieeexplore.ieee.org/document/9151964/?arnumber=9151964 (visited on 04/01/2025).

[339] Weijun Gao, Chong Han, and Zhi Chen. “DNN-Powered SIC-Free Receiver Artificial Noise Aided Terahertz Secure Communications With Randomly Distributed Eavesdroppers”. In: *IEEE Transactions on Wireless Communications* 21.1 (Jan. 2022), pp. 563–576. ISSN: 1558-2248. DOI: 10.1109/TWC.2021.3098334. URL: https://ieeexplore.ieee.org/document/9497766/?arnumber=9497766 (visited on 04/01/2025).

[340] Lu Lv et al. “Safeguarding Next-Generation Multiple Access Using Physical Layer Security Techniques: A Tutorial”. In: *Proceedings of the IEEE* 112.9 (Sept. 2024), pp. 1421–1466. ISSN: 1558-2256. DOI: 10.1109/JPROC.2024.3420127. URL: https://ieeexplore.ieee.org/document/10605790/?arnumber=10605790 (visited on 03/24/2025).

[341] Hui Han et al. “IRS-Aided Secure NOMA Networks Against Internal and External Eavesdropping”. In: *IEEE Transactions on Communications* 70.11 (Nov. 2022), pp. 7536–7548. ISSN: 1558-0857. DOI: 10.1109/TCOMM.2022.3208341. URL: https://ieeexplore.ieee.org/document/9896889/?arnumber=9896889 (visited on 04/01/2025).

[342] Ning Wang et al. “Physical-Layer Security of 5G Wireless Networks for IoT: Challenges and Opportunities”. In: *IEEE Internet of Things Journal* 6.5 (Oct. 2019), pp. 8169–8181. ISSN: 2327-4662. DOI: 10.1109/JIOT.2019.2927379. URL: https://ieeexplore.ieee.org/document/8758230/?arnumber=8758230 (visited on 04/02/2025).

[343] Li Sun and Qinghe Du. “A Review of Physical Layer Security Techniques for Internet of Things: Challenges and Solutions”. In: *Entropy* 20.10 (Oct. 2018), p. 730. ISSN: 1099-4300. DOI: 10.3390/e20100730. URL: https://www.mdpi.com/1099-4300/20/10/730 (visited on 03/04/2024).

[344] Lun Dong et al. “Improving Wireless Physical Layer Security via Cooperating Relays”. In: *IEEE Transactions on Signal Processing* 58.3 (Mar. 2010), pp. 1875–1888. ISSN: 1941-0476. DOI: 10.1109/TSP.2009.2038412. URL: https://ieeexplore.ieee.org/document/5352243/ (visited on 05/28/2025).

[345] Ioannis Krikidis, John S. Thompson, and Steve Mclaughlin. “Relay Selection for Secure Cooperative Networks with Jamming”. In: *IEEE Transactions on Wireless Communications* 8.10 (Oct. 2009), pp. 5003–5011. ISSN: 1558-2248. DOI: 10.1109/TWC.2009.090323. URL: https://ieeexplore.ieee.org/document/5288936/ (visited on 05/28/2025).

[346] Shunliang Zhang, Dali Zhu, and Yinlong Liu. “Artificial Intelligence Empowered Physical Layer Security for 6G: State-of-the-art, Challenges, and Opportunities”. In: *Computer Networks* 242 (Apr. 2024), p. 110255. ISSN: 1389-1286. DOI: 10.1016/j.comnet.2024.110255. URL: https://www.sciencedirect.com/science/article/pii/S1389128624000872 (visited on 03/24/2025).

[347] Israt Ara and Brian Kelley. “6G Physical Layer Security”. In: *Artificial Intelligence*. Ed. by Manuel Domínguez-Morales et al. Vol. 26. IntechOpen, May 2024. ISBN: 978-1-83768-322-2 978-1-83768-323-9. DOI: 10.5772/intechopen.112989. URL: https://www.intechopen.com/chapters/88429 (visited on 02/13/2025).

[348] Arsenia Chorti et al. "Context-Aware Security for 6G Wireless: The Role of Physical Layer Security". In: *IEEE Communications Standards Magazine* 6.1 (Mar. 2022), pp. 102–108. ISSN: 2471-2833. DOI: 10.1109/MCOMSTD.0001.2000082. URL: https://ieeexplore.ieee.org/document/9762838 (visited on 03/18/2025).

[349] Abbas Acar et al. "A survey on homomorphic encryption schemes: Theory and implementation". In: *ACM Computing Surveys (Csur)* 51.4 (2018), pp. 1–35.

[350] Xun Yi et al. *Homomorphic encryption*. Springer, 2014.

[351] Payman Mohassel and Yupeng Zhang. "SecureML: A System for Scalable Privacy-Preserving Machine Learning". In: *2017 IEEE Symposium on Security and Privacy (SP)*. 2017, pp. 19–38. DOI: 10.1109/SP.2017.12.

[352] Mohammad Al-Rubaie and J. Morris Chang. "Privacy-Preserving Machine Learning: Threats and Solutions". In: *IEEE Security & Privacy* 17.2 (2019), pp. 49–58. DOI: 10.1109/MSEC.2018.2888775.

[353] Lumin Liu et al. "Communication-Efficient Federated Distillation with Active Data Sampling". In: *ICC 2022 - IEEE International Conference on Communications*. 2022, pp. 201–206. DOI: 10.1109/ICC45855.2022.9839214.

[354] Chuhan Wu et al. "Communication-efficient federated learning via knowledge distillation". In: *Nature communications* 13.1 (2022), p. 2032.

[355] Gad Gad and Zubair Fadlullah. "Federated Learning via Augmented Knowledge Distillation for Heterogenous Deep Human Activity Recognition Systems". In: *Sensors* 23.1 (2023). ISSN: 1424-8220. DOI: 10.3390/s23010006. URL: https://www.mdpi.com/1424-8220/23/1/6.

[356] Yu Chen et al. "A training-integrity privacy-preserving federated learning scheme with trusted execution environment". In: *Information Sciences* 522 (2020), pp. 69–79. ISSN: 0020-0255. DOI: https://doi.org/10.1016/j.ins.2020.02.037. URL: https://www.sciencedirect.com/science/article/pii/S0020025520301201.

[357] Fan Mo et al. "PPFL: privacy-preserving federated learning with trusted execution environments". In: MobiSys '21. Virtual Event, Wisconsin: Association for Computing Machinery, 2021, pp. 94–108. ISBN: 9781450384438. DOI: 10.1145/3458864.3466628. URL: https://doi.org/10.1145/3458864.3466628.

[358] Xingyu Li et al. "LoMar: A Local Defense Against Poisoning Attack on Federated Learning". In: *IEEE Transactions on Dependable and Secure Computing* 20.1 (2023), pp. 437–450. DOI: 10.1109/TDSC.2021.3135422.

[359] Chen Zhao et al. "FederatedReverse: A Detection and Defense Method Against Backdoor Attacks in Federated Learning". In: *Proceedings of the 2021 ACM Workshop on Information Hiding and Multimedia Security*. IH&MMSec '21. Virtual Event, Belgium: Association for Computing Machinery, 2021, pp. 51–62. ISBN: 9781450382953. DOI: 10.1145/3437880.3460403. URL: https://doi.org/10.1145/3437880.3460403.

[360] Nuria Rodríguez-Barroso et al. "Dynamic defense against byzantine poisoning attacks in federated learning". In: *Future Generation Computer Systems* 133 (2022), pp. 1–9. ISSN: 0167-739X. DOI: https://doi.org/10.1016/j.future.2022.03.003. URL: https://www.sciencedirect.com/science/article/pii/S0167739X22000784.

[361] Peva Blanchard et al. "Machine Learning with Adversaries: Byzantine Tolerant Gradient Descent". In: *Advances in Neural Information Processing Systems*. Vol. 30. Curran Associates, Inc., 2017. URL: https://proceedings.neurips.cc/paper_files/paper/2017/file/f4b9ec30ad9f68f89b29639786cb62ef-Paper.pdf.

[362] Tsuyoshi Idé. "Collaborative Anomaly Detection on Blockchain from Noisy Sensor Data". In: *2018 IEEE International Conference on Data Mining Workshops (ICDMW)*. 2018, pp. 120–127. DOI: 10.1109/ICDMW.2018.00024.

[363] Zhixiong Chen et al. "Adaptive Model Pruning for Communication and Computation Efficient Wireless Federated Learning". In: *IEEE Transactions on Wireless Communications* 23.7 (2024), pp. 7582–7598. DOI: 10.1109/TWC.2023.3342626.

[364] Saeed Vahidian, Mahdi Morafah, and Bill Lin. "Personalized Federated Learning by Structured and Unstructured Pruning under Data Heterogeneity". In: *2021 IEEE 41st International Conference on Distributed Computing Systems Workshops (ICDCSW)*. 2021, pp. 27–34. DOI: 10.1109/ICDCSW53096.2021.00012.

[365] Yuang Jiang et al. "Model Pruning Enables Efficient Federated Learning on Edge Devices". In: *IEEE Transactions on Neural Networks and Learning Systems* 34.12 (2023), pp. 10374–10386. DOI: 10.1109/TNNLS.2022.3166101.

[366] Liping Yi et al. "FedPE: Adaptive Model Pruning-Expanding for Federated Learning on Mobile Devices". In: *IEEE Transactions on Mobile Computing* 23.11 (2024), pp. 10475–10493. DOI: 10.1109/TMC.2024.3374706.

[367] Xuefeng Jiang et al. "Towards Federated Learning against Noisy Labels via Local Self-Regularization". In: *Proceedings of the 31st ACM International Conference on Information & Knowledge Management*. CIKM '22. Atlanta, GA, USA: Association for Computing Machinery, 2022, pp. 862–873. ISBN: 9781450392365. DOI: 10.1145/3511808.3557475. URL: https://doi.org/10.1145/3511808.3557475.

[368] Zifan Chen et al. "Contractible Regularization for Federated Learning on Non-IID Data". In: *2022 IEEE International Conference on Data Mining (ICDM)*. 2022, pp. 61–70. DOI: 10.1109/ICDM54844.2022.00016.

[369] Yang Liu et al. “Towards secure and efficient integration of blockchain and 6G networks”. In: *Plos one* 19.4 (2024), e0302052.

[370] Sakshi Singh, Avdhesh Gupta, and Anu Chaudhary. “Enhancing Blockchain Security through quantum key distribution and evaluating QKD network in QKDNetSim environment”. In: *2024 3rd International conference on Power Electronics and IoT Applications in Renewable Energy and its Control (PARC)*. 2024, pp. 86–93.

[371] Paulo Martins, Leonel Sousa, and Artur Mariano. “A Survey on Fully Homomorphic Encryption: An Engineering Perspective”. In: 50.6 (Dec. 2017). ISSN: 0360-0300. DOI: 10.1145/3124441. URL: https://doi.org/10.1145/3124441.

[372] Junfeng Fan and Frederik Vercauteren. *Somewhat Practical Fully Homomorphic Encryption*. Cryptology ePrint Archive, Paper 2012/144. 2012. URL: https://eprint.iacr.org/2012/144.

[373] Ivan Damgård et al. “Multiparty computation from somewhat homomorphic encryption”. In: *Annual Cryptology Conference*. Springer. 2012, pp. 643–662.

[374] Mengmeng Yang et al. “Local differential privacy and its applications: A comprehensive survey”. In: *Computer Standards & Interfaces* 89 (2024), p. 103827. ISSN: 0920-5489. DOI: https://doi.org/10.1016/j.csi.2023.103827. URL: https://www.sciencedirect.com/science/article/pii/S0920548923001083.