Artificial Intelligence Enabled Physical Layer Security Framework in 6G Wireless Networks: Challenges, Opportunities and Future Directions

L. A. Olawoyin[1], M. O. Oloyede[2], A. A. Oloyede[1], Y. O. Imam-Fulani[1], A. Mahmoud-Jimoh[1]

[1]Department of Telecommunication Science, University of Ilorin, Nigeria.
[2]Department of Information Technology, University of Ilorin, Nigeria.

ABSTRACT: Sixth-generation (6G) wireless networks are envisioned to deliver integrated space–air–ground–sea connectivity, extreme data rates, ultra-low latency, and native intelligence to support emerging services such as holographic communications, digital twins, autonomous systems, and massive Internet of Things (IoT). While these capabilities enable unprecedented functionality, they also significantly expand the attack surface at the physical layer, where threats such as eavesdropping, jamming, spoofing, and channel manipulation are increasingly difficult to mitigate using conventional cryptography alone. Physical layer security (PLS), grounded in information-theoretic principles and intrinsic channel and hardware characteristics, has therefore re-emerged as a vital complement to upper-layer security mechanisms. However, classical PLS techniques rely heavily on accurate channel state information and static analytical models, limiting their effectiveness in the highly dynamic, heterogeneous, and intelligence-native environments envisioned for 6G. Motivated by recent advances in artificial intelligence (AI) and machine learning (ML), this paper presents a comprehensive and critical review of AI-enabled physical layer security for 6G wireless networks. The review first outlines the 6G vision, security requirements, and threat landscape, highlighting the limitations of conventional PLS approaches. It then systematically examines how supervised, unsupervised, reinforcement, and federated learning paradigms can enhance PLS functionalities, including attack detection, anti-jamming, secure beamforming, physical-layer authentication, and secret key generation. Furthermore, the paper analyses the role of AI-driven PLS across key 6G-enabling technologies such as reconfigurable intelligent surfaces, terahertz communications, cell-free massive MIMO, visible light communications, ambient backscatter, and molecular communications. Finally, open research challenges related to scalability, robustness, trustworthiness, and privacy are identified, and future research directions are outlined toward the realization of intelligent, resilient, and deployable PLS architectures for 6G systems. This review aims to provide a structured reference for researchers and practitioners while highlighting critical research gaps and opportunities at the intersection of AI and physical layer security.

KEYWORDS: 6G, Physical Layer Security, Artificial Intelligence, Machine Learning, Wireless Communications, Terahertz, Edge Intelligence.

[Received Dec. 8, 2024; Revised July 7, 2025; Accepted July 18, 2025] Print ISSN: 0189-9546 | Online ISSN: 2437-2110

I. INTRODUCTION

The evolution toward sixth-generation (6G) wireless networks marks a fundamental shift from connectivity-centric communication to intelligence-native, service-oriented systems (Saad et al., 2020; Alhammadi et al., 2024). Beyond supporting extreme data rates and ultra-low latency, 6G is envisioned to natively integrate communication, sensing, computing, and control across space–air–ground–sea infrastructures (Jiang et al., 2021; Dang et al., 2020; Saad et al., 2020). This convergence is expected to enable transformative applications such as holographic communications, digital twins, autonomous systems, tactile Internet, and massive Internet of Things (IoT). However, the same features that empower these applications significantly expand the attack surface of future wireless networks, particularly at the physical layer (Mahyoub et al., 2024; Siriwardhana et al., 2021; Mahmoud et al., 2024).

Unlike previous generations, 6G networks will be characterized by ultra-dense deployments, heterogeneous radio technologies, distributed edge intelligence, and pervasive reliance on artificial intelligence and machine

*Corresponding author: Olawoyin.la@unilorin.edu.ng

doi: http://doi.org/10.63746/njtd.v23i1.4355

learning (AI/ML) for network control and optimization (Chataut et al., 2024; Alhammadi et al., 2024; Letaief et al., 2019). Due to the nature of transmission of signal in wireless system which is open in nature combined with dynamic topologies and autonomous decision-making, renders 6G and the subsequent generations systems highly vulnerable to physical-layer attacks such as eavesdropping, jamming, pilot spoofing, channel manipulation, and device impersonation (Lo Cigno et al., 2025; Mahmoud et al., 2024; Kazmi et al., 2023). This is as a result of their decentralized, AI-native architecture, widespread use of open radio access networks (O-RAN), and extensive IoT integration.

The reliance on high-frequency terahertz (THz) communication, intelligent surfaces (RIS), and AI-driven channel estimation creates new attack vectors that allow malicious entities to spoof legitimate devices or alter transmission paths. While cryptographic mechanisms remain indispensable, they are often insufficient or impractical for resource-constrained IoT devices, ultra-reliable low-latency communications, and highly dynamic environments where key management, latency, and computational overhead pose significant challenges (Kuchuk & Malokhvii, 2024; Kazmi et al., 2023). Physical Layer Security (PLS) has therefore re-emerged as a critical complementary security paradigm. By exploiting inherent properties of the wireless channel, such as randomness, and noise, PLS enables confidentiality, authentication, and integrity directly at the waveform level (Mitev et al., 2023; Sanenga et al., 2020; Zhang et al., 2021). Despite extensive research, classical PLS techniques are largely model-driven and rely heavily on accurate and timely channel state information (CSI) (Mitev et al., 2023; Aladi, 2023). These assumptions become increasingly unrealistic in large-scale, fast-varying, and heterogeneous 6G environments, limiting the robustness and scalability of traditional PLS approaches (Kazmi et al., 2023; Aladi, 2023).

Recent advances in AI and ML offer a promising pathway to overcome these limitations by transforming PLS from a static, analytical framework into an adaptive, data-driven, and autonomous security mechanism (Mahmoud et al., 2024; Mahmoud et al., 2024; Lu et al., 2022). Learning-based techniques can infer complex channel behaviours, detect anomalous activities, optimize secure transmission strategies, and generalize to previously unseen environments with reduced dependence on perfect CSI (Hoang et al., 2024; Saeed et al., 2023; Lu et al., 2022). Consequently, AI-enabled PLS has emerged as a key enabler for achieving resilient and intelligent security in future 6G networks.

Motivated by this vision, this paper presents a comprehensive and critical review of AI-driven physical layer security for 6G wireless networks. Unlike existing surveys that primarily provide descriptive summaries of isolated techniques (Mitev et al., 2023; Zhang et al., 2021), this review adopts an integrative and analytical perspective. Specifically, it examines how different learning paradigms, such as supervised learning, unsupervised learning, reinforcement learning, and federated learning, can enhance core PLS functionalities, including attack detection, anti-jamming, secure beamforming, physical-layer authentication, and secret key generation. Furthermore, the paper systematically analyzes AI-enabled PLS across key 6G-enabling technologies, including reconfigurable intelligent surfaces, terahertz communications, cell-free massive MIMO, visible light communications, ambient backscatter, and molecular communications.

In addition to surveying state-of-the-art solutions, this review identifies fundamental challenges related to scalability, robustness, trustworthiness, privacy, and adversarial resilience, and outlines promising future research directions toward deployable and intelligent PLS architectures for 6G systems. By synthesizing fragmented research efforts and highlighting open problems, this paper aims to serve as a structured reference for researchers and practitioners working at the intersection of artificial intelligence and physical layer security in next-generation wireless networks.

The remainder of this paper is organized as follows. Section 2 reviews related work on PLS and AI-enabled security in wireless networks. Section 3 discusses security considerations and threat models for AI-driven PLS in 6G. Section 4 surveys learning-based PLS techniques across key 6G technologies. Section 5 and 6 identify open challenges and future research directions. Finally, Section 7 concludes the paper.

II. THEORETICAL AND CONCEPTUAL FRAMEWORK

By automating security through machine learning (ML), facilitating intelligent resource management, and utilizing wireless channel features to thwart eavesdropping, AI-driven Physical Layer Security (PLS) in 6G makes significant advances. Real-time threat detection, adaptive beamforming, secure user-centric access management, and reliable, low-latency authentication for Internet of Things devices are some of the major achievements.

A) Intelligent Anomaly Detection & Threat Identification

AI/ML algorithms monitor network performance, quickly identifying anomalies and intrusions by analyzing massive data volumes from wireless channels.

B) Adaptive Resource Management and Optimization

AI optimizes spectrum efficiency and resource allocation in real-time to enhance secrecy capacity, ensuring secure communication even under changing network conditions.
Intelligent Beamforming and Interference Management: AI is used for intelligent, dynamic, and secure beamforming, which enhances signals for legitimate users while minimizing leakage to potential eavesdroppers.

C) Authentication and Privacy Protection

AI supports lightweight, low-complexity authentication mechanisms, which are critical for power-limited IoT devices in 6G.

D) Cross-Domain Security Enhancement

AI-enabled systems offer complete security across open wireless settings through cross-domain data fusion for improved security in space-air-ground-sea integrated scenarios.

E) Addressing Post-Quantum Security

AI assists in developing and optimizing post-quantum cryptographic algorithms to secure 6G against future quantum computing attacks

III. 6G SECURITY LANDSCAPE AND REQUIREMENTS

The security landscape of sixth-generation (6G) wireless networks is fundamentally shaped by their intelligence-native architecture, heterogeneous deployment, and pervasive integration of emerging technologies (Mao et al., 2023; Chataut et al., 2024; Saad et al., 2020). Unlike previous generations, 6G systems are expected to operate across space–air–ground–sea domains, support massive device connectivity, and rely heavily on artificial intelligence for autonomous control and optimization (Jiang et al., 2021; Alhammadi et al., 2024; Letaief et al., 2019).

These characteristics introduce new threat vectors and amplify existing vulnerabilities, particularly at the physical layer, where the openness of the wireless medium and dynamic propagation environments expose communications to sophisticated attacks (Lo Cigno et al., 2025; Mahmoud et al., 2024; Kazmi et al., 2023). As shown in figure 1 (Porambage et al., 2021), this section provides an overview of the evolving 6G security landscape, highlighting key threat models and attack surfaces and outlines the security requirements necessary to ensure confidentiality, integrity, availability, privacy, and trust in future intelligent wireless networks.

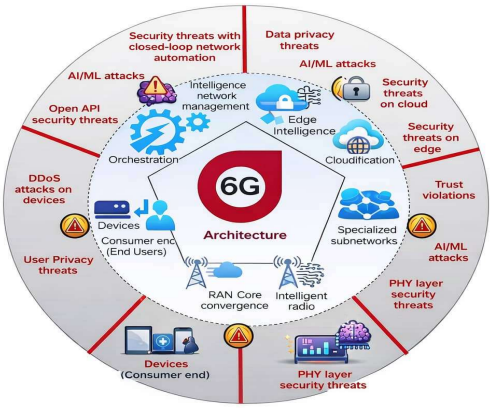

Figure 1 Overview of the Evolving 6G Security Landscape

A. Threat Model in 6G Networks

As shown in figure 2, the threat model of 6G` wireless networks is significantly more complex than that of previous generations due to the convergence of heterogeneous communication technologies, pervasive intelligence, and highly dynamic network architectures (Mao et al., 2023; Chataut et al., 2024; Siriwardhana et al., 2021). In addition to classical wireless threats, 6G introduces new attack vectors arising from the extensive use of artificial intelligence and machine learning (AI/ML) for network control, optimization, and security enforcement. As a result, network attacks in 6G environments may exploit both the physical properties of the wireless medium and the vulnerabilities of learning-driven systems (Mahmoud et al., 2024; Rifa-Pous et al., 2024).

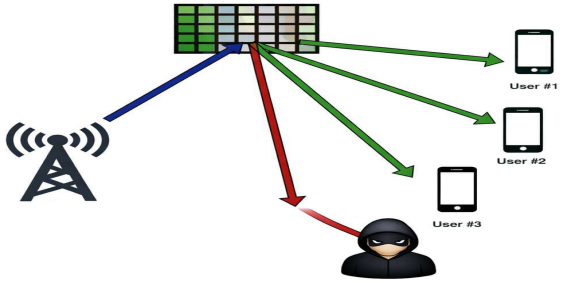

Figure 2 Attack on a Mobile Network

From a traditional physical-layer perspective, 6G networks remain inherently vulnerable to well-known wireless attacks such as passive eavesdropping, active jamming, pilot contamination, spoofing, and channel manipulation (Lo Cigno et al., 2025; Mahmoud et al., 2024; Kazmi et al., 2023). The use of ultra-high-frequency bands, including millimetre-wave and terahertz communications, further worsens these risks due to high directionality, sensitivity to blockage, and rapid channel variations (Rappaport et al., 2013; Rappaport et al., 2019). Moreover, emerging technologies such as reconfigurable intelligent surfaces, cell-free massive MIMO, and non-terrestrial networks introduce new degrees of freedom that can be exploited by attackers to disrupt beam alignment, manipulate propagation environments, or impersonate legitimate devices (Aldirmaz-Colak et al., 2025; Wang et al., 2025).

Beyond these classical threats, the intelligence-native nature of 6G networks gives rise to a new class of AI-driven attacks that directly target learning-based components (Siriwardhana et al., 2021; Rifa-Pous et al., 2024). One prominent threat is data poisoning, where attackers maliciously manipulate training datasets or online learning processes to degrade the performance of AI models used for physical-layer security tasks such as attack detection, beamforming, or authentication (Rifa-Pous et al., 2024; Hoang et al., 2024). In distributed and federated learning settings commonly envisioned for 6G edge intelligence, poisoned local updates can propagate across the network, leading to systemic security failures (Rifa-Pous et al., 2024; Nguyen et al., 2021). Another critical threat is the generation of adversarial samples, in which carefully created signals or perturbations are injected into the wireless environment to mislead machine learning models (Siriwardhana et al., 2021; Rifa-Pous et al., 2024). Such attacks can cause misclassification of legitimate users, failure to detect jamming or spoofing attempts, or incorrect estimation of channel characteristics (Mahmoud et al., 2024; Hoang et al., 2024).

At the physical layer, adversarial examples may manifest as subtle waveform manipulations that are difficult to distinguish from noise, making them particularly challenging to detect using conventional signal processing techniques (Lo Cigno et al., 2025; Hoang et al., 2024). Model extraction and inference attacks further threaten the confidentiality and integrity of AI-enabled PLS systems (Siriwardhana et al., 2021; Rifa-Pous et al., 2024). By repeatedly querying

deployed models and observing their outputs, attackers may infer model parameters, replicate model behaviour, or extract sensitive information about training data and network conditions (Rifa-Pous et al., 2024; Hoang et al., 2024). These attacks are especially concerning in open 6G environments where learning models may be exposed through edge or cloud-based interfaces (Mao et al., 2023; Kuchuk & Malokhvii, 2024).

In addition to external attackers, 6G threat models must also account for insider threats and cross-domain attacks enabled by virtualization, network slicing, and multi-tenant cloud infrastructures (Mao et al., 2023; Kukliński et al., 2021). Compromised edge nodes, malicious users, or untrusted learning participants can exploit shared resources to launch coordinated attacks that simultaneously affect multiple network functions and services (Siriwardhana et al., 2021; Rifa-Pous et al., 2024). The integration of sensing, communication, and computing further blurs trust boundaries, increasing the potential impact of such attacks (Qu et al., 2024; Aldirmaz-Colak et al., 2025).

Collectively, these evolving threats necessitate a comprehensive and multi-dimensional threat model for 6G networks, one that jointly considers traditional wireless attacks (Lo Cigno et al., 2025), AI-specific vulnerabilities (Siriwardhana et al., 2021; Rifa-Pous et al., 2024), and cross-layer interactions (Mao et al., 2023; Mahmoud et al., 2024). This complexity shows the need for adaptive, intelligent, and robust physical-layer security mechanisms capable of learning from the environment, anticipating adversarial behaviour, and responding autonomously to both known and unknown attacks (Mahmoud et al., 2024; Alhammadi et al., 2024). AI-driven PLS is therefore not merely an enhancement but a fundamental requirement for securing future 6G wireless networks. A list of 6G network security threats and potential impact is presented in Table 1.

Table1 6G-network security threat and their Impacts

Category	Example Threats/Issues	Impact
Expanded Attack Surface	Multi-technology integration	Broader exposure
Virtualization & Cloud	Hypervisor or API attacks	Data breach
IoT Insecurity	Botnets, weak authentication	DDoS, data loss
Network Slicing	Slice isolation failure	Unauthorized access
Edge Computing	Local node compromise	Service disruption
Signaling Plane	Spoofing, DoS	Network instability
Privacy	Location tracking	User profiling
Supply Chain	Backdoors, firmware exploits	Compromised trust
AI Integration	Model poisoning	Faulty automation

B. Security Requirements in 6G Networks

The security requirements of 6G wireless networks extend far beyond the classical confidentiality, integrity, and availability (CIA) paradigm due to the intelligence-native, autonomous, and highly heterogeneous nature of future communication systems (Mao et al., 2023; Kazmi et al., 2023). In 6G, security must be continuous, adaptive, and embedded across all layers of the network architecture, particularly at the physical layer where many attacks originate and evolve in real time (Mahmoud et al., 2024; Alhammadi et al., 2024). Consequently, new security objectives emerge that reflect the scale, dynamics, and intelligence of 6G environments. Some of the common security requirement of a 6G network are presented in this subsection.

Authentication: Authentication in 6G networks must evolve from static, session-based mechanisms to continuous and lightweight processes that scale to massive device densities (Sakraoui et al., 2025; Alhoraibi et al., 2023). Traditional cryptographic authentication protocols often incur significant signalling overhead and latency, making them unsuitable for ultra-low-latency and energy-constrained scenarios (Kim et al., 2021). Physical-layer authentication, supported by AI-based feature extraction and learning, enables continuous identity verification based on channel characteristics, radio fingerprints, and device behaviour, providing a scalable solution for massive IoT and autonomous systems (Huang et al., 2021; Abbas et al., 2024; Alhoraibi et al., 2023).

Privacy and Trust: Privacy and trust represent predominant requirements in 6G networks, where data, intelligence, and decision-making are distributed across edge, cloud, and non-terrestrial platforms (Mao et al., 2023; Rifa-Pous et al., 2024). Protecting user privacy while enabling collaborative learning and autonomous operation necessitates decentralized, privacy-preserving, and explainable security mechanisms (Qu et al., 2024; Barnard et al., 2022). Trust models must account for heterogeneous entities, dynamic network slicing, and cross-domain interactions, ensuring that security decisions remain transparent, verifiable, and robust against insider and adversarial learning attacks (Lockey et al., 2021; Habbal et al., 2024). Collectively, these requirements call for a holistic and multi-layered security framework that tightly integrates traditional cryptographic techniques with AI-driven physical layer security. Rather than treating PLS as an isolated enhancement, 6G security must embed intelligent PLS mechanisms as a core component of the network architecture, enabling adaptive, resilient, and trustworthy protection against both classical and AI-driven threats. Common security goals and focus of the 6G network are listed in Table 2.

Table 2 6G Security Requirement

Requirement	Purpose	6G Relevance
Confidentiality	Protect data	High-speed secure communication
Integrity	Prevent tampering	Reliable AI decisions
Availability	Ensure access	Critical services
Authentication	Verify identity	Massive IoT

Privacy Trust	Protect users Ensure reliability	Data-driven systems Distributed networks
Resilience PLS	Attack recovery Signal-level security	Dynamic networks THz, beamforming

IV. LIMITATIONS OF CLASSICAL PHYSICAL LAYER SECURITY

Classical physical layer security (PLS) techniques have been extensively studied as a means of complementing cryptographic security by exploiting the inherent properties of wireless channels (Bloch & Barros, 2011; Mitev et al., 2023; Poor & Schaefer, 2017). Approaches such as secrecy beamforming, artificial noise injection, cooperative jamming, and information-theoretic coding strategies provide elegant analytical frameworks and strong theoretical guarantees under idealized assumptions (Hong et al., 2020; Olawoyin et al., 2015; Mitev et al., 2023). However, the practical applicability of these methods becomes increasingly limited in the context of 6G wireless networks, which are characterized by extreme dynamics, large-scale heterogeneity, and intelligence-native operation (Kazmi et al., 2023; Aladi, 2023; Zhang et al., 2021). A fundamental limitation of classical PLS techniques is their strong dependence on accurate and timely channel state information (CSI) (Mitev et al., 2023; Aladi, 2023). Many PLS schemes assume perfect or near-perfect knowledge of the legitimate and eavesdropping channels in order to optimize beamforming vectors, power allocation, or artificial noise generation (Hong et al., 2020; Olawoyin et al., 2015).

In 6G environments, featuring ultra-high mobility, rapidly varying propagation conditions, cell-free architectures, and non-terrestrial links, acquiring and maintaining such precise CSI is often infeasible (Kazmi et al., 2023; Aladi, 2023). Channel estimation errors, feedback delays, and pilot contamination can severely degrade the effectiveness of classical PLS mechanisms and even expose additional vulnerabilities (Aladi, 2023; Zhang et al., 2021). Scalability represents another major challenge for classical PLS in 6G networks. Ultra-dense deployments, massive IoT connectivity, and distributed antenna systems significantly increase the dimensionality of the optimization problems underlying traditional PLS designs (Kazmi et al., 2023). As the number of users, antennas, and network entities grows, classical analytical solutions become computationally expensive and difficult to implement in real time (Shen et al., 2021). This lack of scalability limits their suitability for large-scale, decentralized, and latency-sensitive 6G scenarios (Kazmi et al., 2023; Aladi, 2023). Classical PLS techniques also exhibit limited robustness against intelligent and adaptive adversaries (Mahmoud et al., 2024; Mitev et al., 2023). Most traditional schemes are designed under fixed threat models and assume passive or static attackers with limited capabilities (Mitev et al., 2023).

In contrast, adversaries in 6G networks may leverage AI and learning-based strategies to adapt their behaviour, infer transmission patterns, and exploit weaknesses in predefined security mechanisms (Siriwardhana et al., 2021; Mahmoud et al., 2024). Static PLS designs are therefore vulnerable to being overcome by adversaries that can learn, predict, and react to defensive strategies (Mahmoud et al., 2024; Hoang et al., 2024). Furthermore, many classical PLS approaches lack intrinsic attack detection and situational awareness capabilities. While they focus on preventing information leakage or degrading an eavesdropper's channel, they typically do not provide mechanisms for detecting ongoing attacks such as jamming, spoofing, or pilot contamination in real time (Aladi, 2023; Sanenga et al., 2020).

As a result, classical PLS often relies on external monitoring or higher-layer security mechanisms, limiting its ability to respond autonomously and promptly to emerging threats (Mahmoud et al., 2024; Alhammadi et al., 2024). Collectively, these limitations highlight a fundamental mismatch between classical PLS assumptions and the operational realities of 6G wireless networks (Kazmi et al., 2023; Aladi, 2023). The reliance on static models, perfect CSI, and predefined threat behaviours constrains the adaptability and resilience of traditional PLS techniques (Mitev et al., 2023; Zhang et al., 2021). These shortcomings strongly motivate the integration of artificial intelligence and machine learning into PLS design, enabling data-driven, adaptive, and autonomous security mechanisms capable of learning from the environment and countering both classical and intelligent adversaries in future 6G systems (Mahmoud et al., 2024; Mahmoud et al., 2024; Lu et al., 2022).

V. AI AND MACHINE LEARNING MODELS FOR PHYSICAL LAYER SECURITY

The increasing complexity, heterogeneity, and dynamism of 6G wireless networks have necessitated a shift from static, model-driven PLS designs toward data-driven and adaptive security mechanisms (Mahmoud et al., 2024; Alhammadi et al., 2024; Lu et al., 2022). AI and ML provide powerful tools for enabling such adaptability by allowing PLS systems to learn from the wireless environment, infer hidden patterns, and respond autonomously to evolving threats (Mahmoud et al., 2024; Hoang et al., 2024; Lu et al., 2022). Rather than categorizing AI-enabled PLS solutions based on specific security functions, this section organizes existing approaches according to their underlying learning models, highlighting how different ML models address distinct security challenges at the physical layer. In figure 2, an architecture of AI-Enhanced IoT in 6G technology is shown.

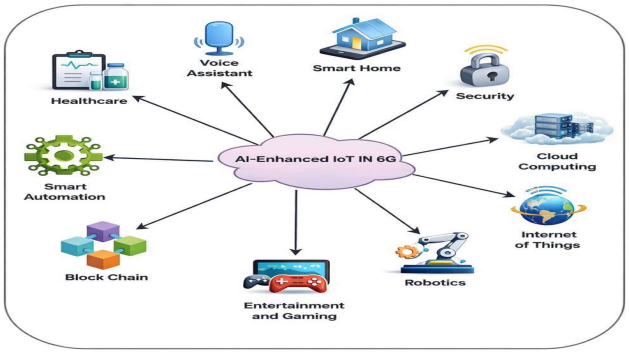

Figure 3 Architecture of AI-Enhanced IoT in 6G Technology

A. Supervised and Unsupervised Learning

Supervised learning techniques play a crucial role in AI-driven PLS by enabling accurate detection of known attacks, device authentication, and transmitter identification through features extracted from the physical layer (Huang et al., 2021; Abbas et al., 2024; Alhoraibi et al., 2023). By leveraging labelled datasets, supervised models can learn discriminative patterns associated with legitimate and malicious behaviours, such as radio frequency (RF) fingerprints, modulation characteristics, or channel statistics (Huang et al., 2021; Alhoraibi et al., 2023). These methods are particularly effective in scenarios where attack signatures are well understood and sufficient training data are available, allowing for high detection accuracy and reliable classification performance (Hoang et al., 2024; Alhoraibi et al., 2023). In contrast, unsupervised learning methods are designed to operate without labelled data, making them well suited for anomaly detection and the discovery of previously unseen threats (Paolini et al., 2023; Saeed et al., 2023).

In 6G environments, where attack strategies may evolve rapidly and labelled datasets may be scarce or outdated, unsupervised approaches provide an essential layer of resilience (Paolini et al., 2023; Saeed et al., 2023). Techniques such as clustering, density estimation, and dimensionality reduction can identify deviations from normal communication patterns, signalling potential security breaches (Paolini et al., 2023). This capability is especially valuable for detecting novel or stealthy attacks that do not conform to known signatures, thereby enhancing the robustness of PLS frameworks against emerging threats (Saeed et al., 2023).

Table 3 The difference between supervised and unsupervised method

Feature	Supervised Learning	Unsupervised Learning
Data Requirement	Labeled dataset	Unlabeled dataset
Learning Objective	Prediction / Classification	Pattern discovery / Clustering
Knowledge of Attacks	Requires known attack patterns	Detects unknown/novel attacks
Accuracy	High (for known threats)	Moderate
Adaptability	Low to moderate	High
Training Complexity	High	Lower (no labeling)
Interpretability	Easier to evaluate	Harder to interpret
Real-time Capability	Limited	Better for anomaly detection
Suitability for 6G	Good for predefined threats	Essential for dynamic threats

B. Reinforcement Learning for Adaptive Defense

Reinforcement learning (RL) introduces a fundamentally different paradigm for PLS by framing security as a sequential decision-making problem under uncertainty (Lu et al., 2022). In this context, an agent learns optimal security strategies, such as power allocation, beamforming, frequency hopping, or jamming mitigation through continuous interaction with the wireless environment (Shen et al., 2021; Lu et al., 2022). By observing environmental states and receiving feedback in the form of rewards, RL-based PLS systems can adapt their behaviour in real time to dynamic channel conditions and adversarial actions (Shen et al., 2021; Hoang et al., 2024). This adaptive capability makes reinforcement learning particularly suitable for proactive defence in 6G networks, where channel characteristics and threat behaviours can change rapidly (Mahmoud et al., 2024; Shen et al., 2021).

RL-based approaches enable PLS mechanisms to anticipate and counteract jamming, eavesdropping, and spoofing attacks without relying on predefined models or complete CSI (Mahmoud et al., 2024; Lu et al., 2022). Furthermore, multi-agent reinforcement learning extends these benefits to distributed and cooperative network settings, allowing multiple nodes to coordinate their security actions (Basharat et al., 2022). Such collaborative learning enhances global network resilience and aligns well with the decentralized and cell-free architectures envisioned for future 6G systems (Basharat et al., 2022; Mahmoud et al., 2024).

Table 4 The table below shows the difference between Reinforced and Adaptive Learning method

Feature	Reinforcement Learning	Adaptive Learning
Learning Style	Trial-and-error with rewards	Continuous adjustment
Data Requirement	Interaction-based	Streaming new data
Goal	Maximize reward	Improve performance over time
Decision Making	Explicit (action-based)	Implicit
Use in 6G	Control and optimization	Real-time adaptation
Complexity	High	Moderate

C. Federated and Distributed Learning

Federated and distributed learning models address critical privacy, scalability, and communication overhead challenges associated with centralized AI-based PLS solutions (Qu et al., 2024; Nguyen et al., 2021). Federated learning enables multiple 6G nodes or edge devices to collaboratively train shared PLS models while keeping raw data localized (El-Hajj, 2025; Nguyen et al., 2021). This approach is particularly attractive for privacy-sensitive applications and IoT-heavy deployments, where transmitting physical-layer data to a central server may be impractical or undesirable (Qu et al.,

2024). By aggregating model updates rather than data, federated learning preserves confidentiality while still benefiting from collective intelligence across the network (El-Hajj, 2025; Nguyen et al., 2021).

Distributed learning further enhances PLS adaptability by empowering edge devices to develop localized security models tailored to their specific propagation environments and threat profiles. Such decentralization reduces latency, improves scalability, and increases robustness against single points of failure (Kuchuk & Malokhvii, 2024). Together, federated and distributed learning models enable privacy-preserving, scalable, and context-aware PLS solutions, making them well aligned with the edge-intelligent and autonomous operation requirements of 6G networks (Qu et al., 2024; El-Hajj, 2025; Nguyen et al., 2021).

Table 5 The difference between Federated and Distributed Learning method

Feature	Federated Learning	Distributed Learning
Data Location	Data stays local	Data may be shared or split
Privacy	High	Low to moderate
Communication	Model updates only	Data and gradients shared
Control	Central server coordinates	Centralized or decentralized
Use Case	Edge devices, IoT	Data centers, cloud computing
Security	Privacy-preserving	Less privacy-focused
6G Suitability	Very high	High

VI. AI-DRIVEN PHYSICAL LAYER SECURITY IN KEY 6G-ENABLING TECHNOLOGIES

The realization of 6G networks relies heavily on a set of disruptive enabling technologies that fundamentally reshape wireless propagation, spectrum usage, and network architecture (Jiang et al., 2021; Dang et al., 2020; Aldirmaz-Colak et al., 2025). While these technologies offer unprecedented gains in capacity, coverage, and flexibility, they also introduce new security vulnerabilities at the physical layer (Aldirmaz-Colak et al., 2025; Wang et al., 2025; Zhang et al., 2021). AI-driven PLS has emerged as a unifying framework capable of harnessing the unique characteristics of these technologies while mitigating their associated risks (Mahmoud et al., 2024; Alhammadi et al., 2024; Lu et al., 2022). This section examines how AI-enhanced PLS mechanisms can be integrated into key 6G-enabling technologies, highlighting their security benefits, challenges, and emerging research directions.

A. Reconfigurable Intelligent Surfaces

Reconfigurable intelligent surfaces (RIS) represent a paradigm shift in wireless communication by enabling programmable control of the propagation environment (Wang et al., 2025). By intelligently adjusting the phase shifts and amplitudes of reflected signals, RIS can enhance signal quality for legitimate users while suppressing information leakage toward potential eavesdroppers (Ge & Fan, 2021; Hong et al., 2020). AI techniques play a pivotal role in optimizing RIS configurations for physical layer security, particularly in complex and dynamic environments where analytical optimization becomes intractable (Ge & Fan, 2021; Wang et al., 2025). Learning-based approaches can adaptively tune RIS parameters to maximize secrecy capacity under varying channel conditions and adversarial behaviours (Ge & Fan, 2021; Hong et al., 2020). For instance, deep reinforcement learning can jointly optimize transmit beamforming and RIS phase control in real time, even with partial or imperfect CSI (Ge & Fan, 2021). However, RIS also introduces new security concerns, including RIS-assisted eavesdropping and malicious reconfiguration attacks (Wang et al., 2025). AI-driven PLS frameworks can address these challenges by enabling anomaly detection and secure control of RIS elements, ensuring that programmable surfaces enhance, rather than undermine, the security of 6G communications (Wang et al., 2025).

B. Terahertz Communications

Terahertz (THz) communication is a cornerstone of 6G networks due to its ability to support ultra-high data rates and extremely low latency (Jornet & Akyildiz, 2014; Rappaport et al., 2019). However, THz links are highly sensitive to blockage, molecular absorption, and rapid channel variations, which complicate the design of reliable and secure transmission schemes (Jornet & Akyildiz, 2014). These characteristics make classical PLS approaches less effective, particularly in mobile and dense deployment scenarios (Aladi, 2023; Zhang et al., 2021). AI-driven techniques offer powerful tools for enhancing PLS in THz systems by enabling accurate beam prediction, channel modelling, and mobility-aware adaptation (Chen et al., 2020). Learning-based beam management can anticipate optimal beam directions and widths, reducing exposure to unintended receivers and minimizing eavesdropping opportunities (Chen et al., 2020). Additionally, deep learning models can capture complex THz channel characteristics, enabling proactive adjustments to transmission parameters that maintain secrecy under dynamic conditions (Chen et al., 2020). By compensating for channel uncertainty and rapid variability, AI-enhanced PLS becomes essential for realizing secure and robust THz communications in 6G networks (Jornet & Akyildiz, 2014; Chen et al., 2020).

C. 5.3 Cell-Free Massive MIMO

Cell-free massive multiple-input multiple-output (MIMO) architectures eliminate traditional cell boundaries by deploying a large number of spatially distributed access points that jointly serve users (Aldirmaz-Colak et al., 2025). While this architecture significantly improves coverage uniformity and spectral efficiency, it also introduces new security challenges related to coordination, scalability, and distributed attack surfaces. Physical layer security in such decentralized systems requires intelligent cooperation among access points to counteract eavesdropping and jamming threats (Aldirmaz-Colak et al., 2025).

AI-driven PLS approaches, particularly graph neural networks and distributed learning techniques, enable coordinated security strategies across cell-free massive MIMO deployments (Basharat et al., 2022). By modelling the network as a graph, learning algorithms can capture spatial correlations and inter-node dependencies, allowing access points to collaboratively optimize beamforming, power allocation, and user association for enhanced secrecy (Basharat et al., 2022). Distributed learning further enables localized decision-making while maintaining global security objectives, reducing reliance on centralized control (El-Hajj, 2025). Leveraging the inherent spatial diversity of cell-free massive MIMO, AI-enhanced PLS frameworks can significantly improve resilience against sophisticated and distributed adversaries in 6G environments (Basharat et al., 2022; Mahmoud et al., 2024).

VII. RESEARCH GAPS AND EMERGING OPPORTUNITIES

Despite the rapid growth of AI-driven physical layer security research for 6G networks, existing studies remain largely fragmented, scenario-dependent, and often tailored to specific technologies or threat models (Oukebdane et al., 2025; Zhang et al., 2021). Most proposed solutions focus on isolated aspects of security, such as anti-jamming or secure beamforming, without addressing broader system-level requirements including scalability, robustness, trust, and deployability (Mahmoud et al., 2024; Rifa-Pous et al., 2024). Moreover, many learning-based PLS schemes assume idealized training conditions and simple learning environments, which may not hold in real-world 6G deployments (Siriwardhana et al., 2021; Rifa-Pous et al., 2024). These limitations highlight the need for unified and holistic PLS frameworks capable of operating reliably across heterogeneous technologies and dynamic threat landscapes (Mahmoud et al., 2024; Kazmi et al., 2023). Some critical open challenges are discussed in this section.

Robustness of Learning Models: AI algorithms used for PLS are themselves vulnerable to manipulation through adversarial examples, data poisoning, and model inversion attacks (Siriwardhana et al., 2021; Rifa-Pous et al., 2024). Ensuring robust learning under adversarial conditions requires the development of defense-aware training strategies, robust optimization techniques, and hybrid schemes that combine model-driven and data-driven approaches (Mahmoud et al., 2024; Hoang et al., 2024). Without such safeguards, AI-enabled PLS mechanisms risk becoming new attack surfaces rather than effective security enablers (Siriwardhana et al., 2021; Rifa-Pous et al., 2024).

Explainability and Trustworthiness of AI-driven Security Decisions: As 6G networks move toward autonomous operation, security mechanisms must be interpretable and auditable to foster trust among network operators, regulators, and end users (Barnard et al., 2022; Visave, 2025). Black-box decision-making in critical security functions raises concerns regarding accountability, fairness, and compliance (Barnard et al., 2022). Explainable AI techniques tailored to physical-layer contexts can provide insights into why specific security actions are taken, enabling human oversight and facilitating safer deployment of intelligent PLS solutions (Barnard et al., 2022; Visave, 2025).

Energy Efficiency and On-device Intelligence: these also present significant challenges, particularly for massive IoT and edge-centric 6G deployments (Shen et al., 2021; Ray, 2025). Many AI-based PLS schemes rely on computationally intensive models that are unsuitable for power- and hardware-constrained devices. Future research must focus on lightweight learning architectures, model compression, and adaptive inference mechanisms that balance security performance with energy consumption. Such approaches are essential for enabling pervasive and sustainable PLS in large-scale 6G networks (Shen et al., 2021; Ray, 2025).

Integration of AI-driven PLS with quantum-resistant cryptographic mechanisms: this also represents a promising yet underexplored opportunity. While PLS offers information-theoretic security guarantees at the physical layer, it cannot fully replace cryptographic protections at higher layers (Bloch & Barros, 2011; Mitev et al., 2023). The advent of quantum computing further complicates this landscape by threatening classical cryptographic primitives (Kaur et al., 2023). Hybrid security architectures that combine AI-enhanced PLS with post-quantum cryptography can provide multi-layered and future-proof protection, leveraging the complementary strengths of both approaches.

Addressing these research gaps will be pivotal for transitioning AI-driven PLS from conceptual and simulation-based studies to practical, scalable, and trustworthy security solutions. By advancing robust, explainable, and energy-efficient learning frameworks and fostering cross-layer integration, future research can unlock the full potential of intelligent physical layer security in realizing secure and resilient 6G networks.

VIII. CONCLUSION

AI-driven physical layer security has emerged as a fundamental enabler for secure, resilient, and intelligent 6G wireless networks. By transforming PLS from static, model-based techniques into adaptive, data-driven paradigms, AI and machine learning could address many of the limitations inherent in classical approaches, particularly in dynamic and heterogeneous environments. This paper has presented a comprehensive review of AI-enabled PLS, examining learning paradigms, key 6G-enabling technologies, threat models, and security requirements, while identifying critical research gaps and opportunities. Despite the promising advances, realizing the full potential of AI-driven PLS requires coordinated research efforts that address adversarial robustness, explainability, scalability, energy efficiency, and deployment feasibility. As wireless systems continue to evolve toward autonomous and intelligence-native operation, the integration of AI into physical layer security will play a pivotal role in safeguarding future networks against both classical and emerging threats. By bridging theory, learning, and practical system design, AI-enhanced PLS stands promising to become a cornerstone of secure 6G communication infrastructures.

REFERENCES

Abbas, S., Abu Talib, M., Nasir, Q., Idhis, S., Alaboudi, M., & Mohamed, A. (2024). Radio frequency fingerprinting techniques for device identification: a survey. International Journal of Information Security, 23(2), 1389-1427.

Aladi, A. A. (2023). Communication Security through Physical-Layer Techniques (Doctoral dissertation, The University of Manchester (United Kingdom)).

A**ldirmaz-Colak, S., Namdar, M., Basgumus, A., Özyurt, S., Kulac, S., Calik, N., ... & Durak-Ata, L. (2025).** A comprehensive review on ISAC for 6G: Enabling technologies, security, and AI/ML perspectives. IEEE Access.

Alhammadi, A., Shayea, I., El-Saleh, A. A., Azmi, M. H., Ismail, Z. H., Kouhalvandi, L., & Saad, S. A. (2024). Artificial intelligence in 6G wireless networks: Opportunities, applications, and challenges. International Journal of Intelligent Systems, (1), 8845070.

Alhoraibi, L., Alghazzawi, D., Alhebshi, R., & Rabie, O. B. J. (2023). Physical layer authentication in wireless networks-based machine learning approaches. Sensors, 23(4), 1814.

Barnard, P., Marchetti, N., & DaSilva, L. A. (2022). Robust network intrusion detection through explainable artificial intelligence (XAI). IEEE Networking Letters, 4(4), 167-171.

Basharat, S., Hassan, S. A., Pervaiz, H., Mahmood, A., Ding, Z., & Gidlund, M. (2022). Intelligent decision making framework for 6G network. China Communications, 19(3), 16-35.

Betzelos, C., Uzunidis, D., Karkazis, P., & Leligou, H. C. (2024, October). Enhancing Reliability in 6G Networks Based on User-Driven AI. In 2020 IEEE 29th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD) (pp. 1-6). IEEE.

Bloch, M., & Barros, J. (2011). Physical-Layer Security: From Information Theory to Security Engineering. Cambridge University Press.

Chataut, R., Nankya, M., & Akl, R. (2024). 6G networks and the AI revolution—Exploring technologies, applications, and emerging challenges. Sensors, 24(6), 1888.

Chen, S., Liang, Y.-C., Sun, S., Kang, X., & Li, Y. (2020). Machine learning for wireless sensing, localization, and communications. IEEE Communications Magazine, 58(6), 80-86.

Dang, S., Amin, O., Shihada, B., & Alouini, M. S. (2020). What should 6G be?. Nature Electronics, 3(1), 20-29.

El-Hajj, M. (2025). Secure and trustworthy open radio access network (O-RAN) optimization: A zero-trust and federated learning framework for 6G networks. Future Internet, 17(6), 233.

Ge, Y., & Fan, J. (2021). Robust secure beamforming for intelligent reflecting surface assisted full-duplex MISO systems. IEEE Transactions on Information Forensics and Security, 17, 253-264.

Habbal, A., Ali, M. K., & Abuzaraida, M. A. (2024). Artificial Intelligence Trust, risk and security management (AI trism): Frameworks, applications, challenges and future research directions. Expert Systems with Applications, 240, 122442.

Hoang, T. M., Vahid, A., Tuan, H. D., & Hanzo, L. (2024). Physical layer authentication and security design in the machine learning era. IEEE Communications Surveys & Tutorials, 26(3), 1830-1860.

Hong, S., Pan, C., Ren, H., Wang, K., & Nallanathan, A. (2020). Artificial-noise-aided secure MIMO wireless communications via intelligent reflecting surface. *IEEE Transactions on Communications*, 68(12), 7851-7866.

Hoque, S., Aydeger, A., Zeydan, E., & Liyanage, M. (2025). A survey on distributed denial of service attack mitigation for 5G and beyond. IEEE Open Journal of the Communications Society.

Huang, D., Al-Hourani, A., Sithamparanathan, K., Rowe, W. S., Bulot, L., & Thompson, A. (2021). Deep learning methods for device authentication using RF fingerprinting. In 2021 15th International Conference on Signal Processing and Communication Systems (ICSPCS) (pp. 1-7). IEEE.

Jiang, W., Han, B., Habibi, M. A., & Schotten, H. D. (2021). The road towards 6G: A comprehensive survey. IEEE Open Journal of the Communications Society, 2, 334-366.

Jornet, J. M., & Akyildiz, I. F. (2014). Graphene-based plasmonic nano-antenna for terahertz band communication in nanonetworks. IEEE Journal on Selected Areas in Communications, 31(12), 685-694.

Kaur, M., Alzubi, A. A., Walia, T. S., Yadav, V., Kumar, N., Singh, D., & Lee, H. N. (2023). EGCrypto: A low-complexity elliptic galois cryptography model for secure data transmission in IoT. IEEE Access, 11, 90739-90748.

Kazmi, S. H. A., Hassan, R., Qamar, F., Nisar, K., & Ibrahim, A. A. A. (2023). Security concepts in emerging 6G communication: Threats, countermeasures, authentication techniques and research directions. Symmetry, 15(6), 1147.

Kim, T. H., Kumar, G., Saha, R., Buchanan, W. J., Devgun, T., & Thomas, R. (2021). LiSP-XK: extended light-weight signcryption for IoT in resource-constrained environments. IEEE Access, 9, 100972-100980.

Kuchuk, H., & Malokhvii, E. (2024). Integration of IoT with cloud, fog, and edge computing: a review. Advanced Information Systems, 8(2), 65-78.

Kukliński, S., Tomaszewski, L., Kołakowski, R., & Chemouil, P. (2021). 6G-LEGO: A framework for 6G network slices. Journal of Communications and Networks, 23(6), 442-453.

Letaief, K. B., Chen, W., Shi, Y., Zhang, J., & Zhang, Y.-J. A. (2019). The roadmap to 6G: AI empowered wireless networks. IEEE Communications Magazine, 57(8), 84-90.

Lo Cigno, R., Gringoli, F., Bartoletti, S., Cominelli, M., Ghiro, L., & Zanini, S. (2025). Communication and sensing: Wireless PHY-layer threats to security and privacy for IoT systems and possible countermeasures. Information, 16(1), 1-18.

Lockey, S., Gillespie, N., Holm, D., & Someh, I. A. (2021). A review of trust in artificial intelligence: Challenges, vulnerabilities and future directions.

Lu, Y., Shi, Y., & Zhang, J. (2022). Learning-based physical layer security: Challenges and opportunities. IEEE Wireless Communications, 29(2), 62-69.

Mahmoud, H., Ismail, T., Baiyekusi, T., & Idrissi, M. (2024). Advanced security framework for 6G networks: Integrating deep learning and physical layer security. Network, 4(4), 453-467.

Mahmoud, H., Ismail, T., Baiyekusi, T., & Idrissi, M. (2024). Advanced security framework for 6G networks: Integrating deep learning and physical layer security. Network, 4(4), 453-467.

Mahyoub, M., AbdulGhaffar, A., Alalade, E., Ndubisi, E., & Matrawy, A. (2024). Security analysis of critical 5G interfaces. IEEE Communications Surveys & Tutorials, 26(4), 2382-2410.

Mao, B., Liu, J., Wu, Y., & Kato, N. (2023). Security and privacy on 6G network edge: A survey. IEEE Communications Surveys & Tutorials, 25(2), 1095-1127.

Mitev, M., Pham, T. M., Chorti, A., Barreto, A. N., & Fettweis, G. (2023). Physical layer security—from theory to practice. IEEE BITS the Information Theory Magazine, 3(2), 67-79.

Nguyen, D. C., Pham, Q.-V., Pathirana, P. N., Ding, M., Seneviratne, A., Li, J., & Poor, H. V. (2021). Federated learning for smart healthcare: A survey. ACM Computing Surveys, 55(3), 1-37.

Olawoyin, L. A., Wu, Y., Yang, H., Salihu, B. A., & Abana, M. A. (2015). Secrecy enhancing in wireless communication with a full-duplexing at the receiver. In 2015 IEEE Global Communications Conference (GLOBECOM) (pp. 1-5). IEEE.

Oukebdane, M. A., Shah, A. S., Azad, A. K., Ekoru, J., & Madahana, M. (2025). Unraveling the nexus of ML and 6G: Challenges, Opportunities, and Future Directions. IEEE Access.

Paolini, E., Valcarenghi, L., Maggiani, L., & Andriolli, N. (2023). Real-time clustering based on deep embeddings for threat detection in 6G networks. IEEE Access, 11, 115827-115835.

Park, J., Samarakoon, S., Shiri, H., Abdel-Aziz, H., Nishio, T. K., Elgabli, A., & Bennis, M. (2020). Extreme urllc: Vision, challenges, and key enablers. arXiv preprint arXiv:2001.09683.

Poor, H. V., & Schaefer, R. F. (2017). Wireless physical layer security. Proceedings of the National Academy of Sciences, 114(1), 19-26.

Porambage, P., Gür, G., Osorio, D. P. M., Liyanage, M., Gurtov, A., & Ylianttila, M. (2021). The roadmap to 6G security and privacy. IEEE Open Journal of the Communications Society, 2, 1094-1122.

Qu, K., Ye, J., Li, X., & Guo, S. (2024). Privacy and security in ubiquitous integrated sensing and communication: Threats, challenges and future directions. IEEE Internet of Things Magazine, 7, 52-58.

Rappaport, T. S., Sun, S., Mayzus, R., Zhao, H., Azar, Y., Wang, K., Wong, G. N., Schulz, J. K., Samimi, M., & Gutierrez, F. (2013). Millimeter wave mobile communications for 5G cellular: It will work! IEEE Access, 1, 335-349.

Rappaport, T. S., Xing, Y., MacCartney, G. R., Molisch, A. F., Mellios, E., & Zhang, J. (2019). Overview of millimeter wave communications for fifth-generation (5G) wireless networks—With a focus on propagation models. IEEE Transactions on Antennas and Propagation, 65(12), 6213-6230.

Ray, P. P. (2025). A review on LLMs for IoT ecosystem: State-of-the-art, lightweight models, use cases, key challenges, future directions. Authorea Preprints.

Rifa-Pous, H., Garcia-Font, V., Nunez-Gomez, C., & Salas, J. (2024). Security, trust and privacy challenges in AI-driven 6G networks. arXiv preprint arXiv:2409.10337.

Saad, W., Bennis, M., & Chen, M. (2020). A vision of 6G wireless systems: Applications, trends, technologies, and open research problems. IEEE Network, 34(3), 134-142.

Saeed, M. M., Saeed, R. A., Abdelhaq, M., Alsaqour, R., Hasan, M. K., & Mokhtar, R. A. (2023). Anomaly detection in 6G networks using machine learning methods. Electronics, 12(15), 3300.

Sakraoui, S., Derdour, M., Ahmim, A., Almukhlifi, R., Ahmim, M., & Ullah, I. (2025). TL2AB: Trusted lightweight authentication using AI and blockchain for 6G networks. Internet of Things, *101661*.

Sanenga, A., Mapunda, G. A., Jacob, T. M. L., Marata, L., Basutli, B., & Chuma, J. M. (2020). An overview of key technologies in physical layer security. Entropy, 22(11), 1261.

Shen, S., Yu, C., Zhang, K., Ni, J., & Ci, S. (2021). Adaptive and dynamic security in AI-empowered 6G: From an energy efficiency perspective. IEEE Communications Standards Magazine, 5(3), 80-88.

Siriwardhana, Y., Porambage, P., Liyanage, M., & Ylianttila, M. (2021). AI and 6G security: Opportunities and challenges. In *2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)* (pp. 616-621). IEEE.

Visave, J. (2025). Transparency in AI for emergency management: Building trust and accountability. AI and Ethics, 1-14.

Wang, H., Lv, T., Cao, Y., Li, W., Zeng, J., Huang, P., & Khan, M. K. (2025). Navigating the dual-use nature and security implications of reconfigurable intelligent surfaces in next-generation wireless systems. arXiv preprint.

Zhang, J., Letaief, K. B., Sun, S., & Cheng, J. (2021). Physical layer security for 6G: A survey. IEEE Communications Surveys & Tutorials, 23(4), 2454-2482.