Deep Learning for Physical-Layer Security in Wireless Internet of Things (WIOT): A Survey, Experimental Analysis, and Outlooks

Abstract—

Keywords: Artificial Intelligence (AI), Cybersecurity, Deep Learning, Physical-Layer Security, Wireless Internet of Things (WIOT), Wireless Communication Security, Wireless Networks, Experimental Analysis, Authentication, Privacy Preservation.

1. Introduction

1.1. Background

The integration of the Internet of Things (IoT) into modern infrastructure, especially in intelligent cities and industrial applications, is revolutionizing connectivity, allowing billions of devices to communicate perfectly. Wireless IoT (WIoT) represents a dynamic ecosystem of low-power interconnected devices, wireless sensors, and actuators that make it easier to exchange real-time data from diverse services, ranging from medical assistance and transportation to power management [1]. With estimates suggesting that by 2025 there will be over 25 billion IoT devices worldwide, IoT deployment scale is rapidly increasing, resulting in a complex and diversified set of connectivity solutions [2].

However, this massive growth of linked devices introduces massive protection demanding situations. The wireless medium, through its very nature, is surprisingly susceptible to quite a few attacks. Generalized connectivity facilitates unsuccessful actors to intercept data, counterfeit devices, or jam communication channels, leading to serious vulnerabilities. These attacks may compromise confidential data such as health records, traffic control systems, or even critical infrastructure such as energy grids [3]. To address these vulnerabilities, the traditional cryptographic methods of the upper layer have been widely used in IoT safety. However, these techniques often require significant computational resources and are not always suitable for IoT devices with resource restrictions. In addition, they may not meet the strict requirements of 5G and 6G emerging networks, particularly in terms of latency, scalability, and real-time safety needs [4]. This limitation encouraged interest in alternative approaches, such as the safety of the physical layer (PLS), which takes advantage of the properties inherent to the wireless channel such as Channel State Information (CSI) and Radio Frequency (RF) fingerprints, to enhance security at the physical layer [5].

PLS offers a light, robust, and adaptive security solution that is particularly suitable for the IoT environment. By using unique physical functions in the communication channel, PLS attacks such as interception and counterfeiting without computational overhead for traditional cryptographic techniques reduce. However, static PLS solutions have limitations in handling dynamic IoT environments with rapidly changing network ratios and different threats. This is where Deep Learning (DL) appears as a powerful tool. DL algorithms, especially Convolutional Neural Networks (CNNs) and reinforcement learning (RL), can effectively adapt to the dynamic nature of wireless environments and improve PLS robustness [6]. DL techniques can analyze complex patterns in the data on physical layers, which allows for real-time detection and the mitigation of safety threats such as jamming and unauthorized unit access [7]. Furthermore, deep learning models can continuously learn and adapt to developing attack strategies and improve the general security of WIoT networks [8].

This diagram shows how physical-layer security (PLS) protects communication in wireless IoT (WIoT) systems. It shows IoT devices that communicate wirelessly, with potential attacks such as eavesdropping and jamming aimed at the communication channel. PLS mechanisms such as Channel State Information (CSI), RF fingerprints, artificial noise, and beamforming protect communication. Secure data transfer is secured after these safety methods are used, with data sent to a central network for processing.

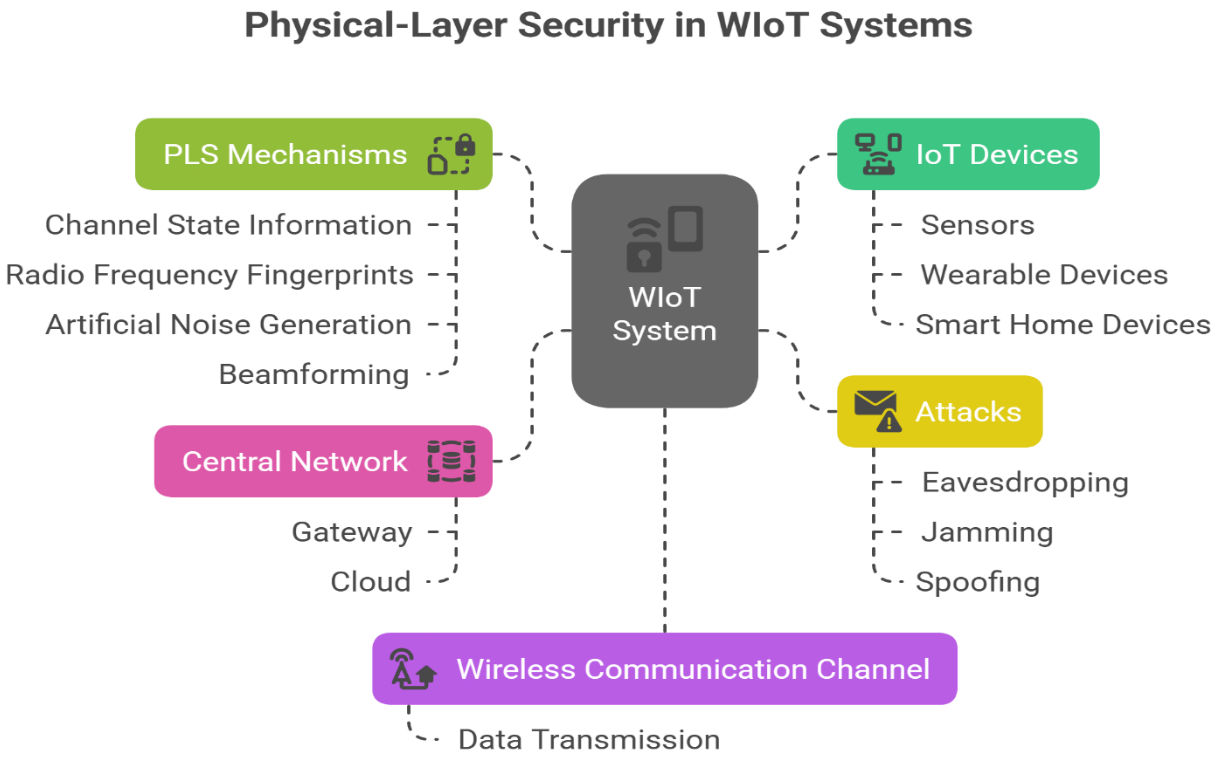


Figure 1. Conceptual Diagram of Physical-Layer Security in Wireless IoT

1.2 Limitations of Upper-Layer Cryptographic Security for WIoT and Deep Learning Solutions

Wireless network approval protocols for Wireless Internet of Things (Wiot) applications, especially in shared rooms, traditionally depend on cryptographic methods for upper layers such as public key encryption frameworks (e.g., RSA and ECC) and symmetrical key dimensions (e.g., Although these methods have been effective in previous generations. -network due to the following reasons:

1. **Cryptographic Security Vulnerabilities:** Cryptographic safety for upper layers depends on the calculation intractability of mathematical problems (e.g., integer factorization, discrete logarithms), but quantum data -burning progress threatens to break these encryption methods. For example, Shor's algorithm can compromise RSA keys, which lead to WIoTs in WIoT devices used in critical infrastructure, such as smart networks. This problem makes traditional cryptographic security that is poorly suited for IoT devices in environments that require long-term security and reliability [14].
2. **Replay Attacks:** Upper layer protocols are vulnerable to playing about attacks, where attackers catch and play again valid signals to circumvent authentication mechanisms without the need to decrypt data. For IoT applications that are sensitive to latency, such as real-time health monitoring in smart health care, unauthorized access or service interruptions can severely compromise patient care and the quality of the service provided. The broadcast type of wireless communication aggravates this risk in Wiot environments, where sensitive data is transmitted over public networks [15].
3. **Key Management Challenges:** Cryptographic methods require key generation, distribution, and renewal, all of which introduce substantial latency and overhead. This is problematic in WIoT applications, such as autonomous drones or smart traffic lights, where even small delays can interfere with functionality. In real-time applications, key exchanges often require multiple communication rounds, further exacerbating the latency problem, especially in resource-constrained IoT devices [16].
4. **Computational Overhead for IoT Devices:** Cryptographic algorithms impose computational overhead on IoT devices, particularly low-power sensors, and wearables. In WIoT networks, where scalability and the integration of numerous heterogeneous devices are essential, cryptographic methods often fail to efficiently manage the diversity of devices and communication protocols. Variations in encryption standards lead to interoperability issues and increase communication overhead, making cryptography unsuitable for large-scale IoT deployments [17].

1.3 Deep learning -enhanced physical layer security

for WIoT Physical Layer Security (PLS) is a promising alternative to traditional cryptographic methods and utilizes unique physical layer properties such as Channel State Information (CSI), Radio Frequency (RF) Fingerprint and Signal Preparation Properties to authenticate devices and secure Wiot-Network communication [18]. PLS provides significant benefits that are particularly suitable for Wiot applications:

1. **Uniqueness of Physical Layer Features:** The physical-layer features of wireless signals, such as multipath fading and hardware imperfections, are unique to each unit and the environment, making them difficult to recreate with opponents. This resistance to duplication improves safety by preventing **impersonation** and **spoofing** attacks, which can compromise critical Wiot infrastructure such as smart city systems or connected vehicles [19].
2. **Low Computational Overhead:** PLS works with low computational complexity, which is essential for WIoT devices with limited processor power, such as battery-powered sensors and wearables. By utilizing existing CSI achieved during channel estimation, PLS offers effective authentication for IoT networks without excessive computational requirements, making it ideal for resource-limited devices in large IoT systems [20].
3. **Compatibility with heterogeneous WIoT networks:** PLS is very compatible with the heterogeneous nature of Wiot networks, involving several unit types and communication protocols. Unlike traditional cryptographic methods, decoder PL's physical layer security is based on unique channel properties, regardless of protocol -specific encryption. This improves interoperability in complex IoT environments, facilitating seamless integration of different devices into smart cities and industrial applications [21].
4. **Adaptation to dynamic IoT environments:** Traditional PLS methods depend on static thresholds for anomaly detection, which are ineffective in dynamic IoT environments. However, deep learning improves (DL) PLS by offering adaptive, intelligent safety mechanisms that can adapt to quickly changed communication channels:
    1. **Deep Learning for complex channel conditions:** Convolutional Neural Networks (CNN) and other deep learning algorithms can analyze high-dimensional channel data to capture real-time variations in WIoT environments, such as smart cities where many devices transfer signals. This provides the opportunity for real-time safety and exceeds traditional models that struggle to accommodate the dynamic nature of Wiot networks [22].
    2. **Reinforcement Learning for adaptive authentication:** Reinforcement Learning (RL) allows for adaptive authentication in mobile IoT applications, such as connected cars or drones, and adjusts real-time authentication thresholds to account for changes in the wireless environment [23].
    3. **Scalable feature extraction with Deep Learning:** Deep learning models enable scalable feature extraction of RF fingerprints from many IoT devices without requiring extensive prior knowledge or manual intervention. This is especially important as the number of connected devices in Wiot systems grows exponentially [24].

4. **Resilience against conflicting attacks:** Deep learning -driven anomaly detection improves PLS resistance to opponent's attack, including signal spoofing and jamming. By utilizing deep neural networks (DNN) and conflicting training, deep learning models can detect subtle anomalies in wireless signals and distinguish between legitimate transfers and malicious interference. In addition, generative adversarial networks (GAN) and Autoencoders can learn robust feature representations of normal wireless communication patterns, so that they can identify and cushion sophisticated attacks in real time. This adaptability makes Wiot systems more secure against threats and ensures the integrity of critical public services such as emergency response networks and smart grids, where security breaches can have profound consequences [25].

Deep learning-enhanced PLS provides adaptive, scalable, and efficient solutions that address the limitations of traditional upper-layer cryptographic security methods. By leveraging the unique features of the physical layer and combining them with advanced deep learning techniques, PLS can offer robust, real-time security for the evolving WIoT landscape.

1.4 Related Surveys

This section reviews recent studies on physical-layer security (PLS) and authentication (PLA) in wireless networks, focusing on 10 key references from 2019 to 2023. These works explore various security aspects, such as eavesdropping, jamming, and spoofing, with some addressing IoT applications and deep learning (DL) techniques. We analyze each study based on criteria like IoT consideration, DL coverage, attack types, experimental evaluation, and future directions. The following table and discussion highlight their contributions, limitations, and gaps, setting the stage for our survey's focus on DL-enhanced PLS for Wireless Internet of Things (WIoT) security.

Table1. Comparative Analysis of Selected Studies on Physical-Layer Security (2019–2023)

Ref.	Year	Focus Area	IoT	DL Coverage	Learning Models	Attack Types	Defense	Adv. ML	Exp. Eval.	Datasets	Challenges	Future Dir.
[26]	2023	PLS Mechanisms	No	No	None	Eavesdropping, Jamming	Yes	No	No	No	Yes	Yes
[27]	2022	Secure Industrial Comms	Yes	No	None	Spoofing	Yes	No	No	No	Yes	Yes
[28]	2022	RF Fingerprinting	Partial	Yes	DL (discriminative)	Spoofing	Yes	No	No	No	Yes	Yes
[29]	2021	NFC Security	No	Yes	DL (discriminative)	Spoofing	Yes	No	Yes	Yes	Yes	No
[30]	2021	IoT Device Detection	Yes	Yes	ML (unspecified)	Spoofing	Yes	No	No	No	Yes	Yes
[31]	2020	RF Fingerprinting	Yes	Yes	DL (discriminative)	Spoofing	Yes	No	Yes	Yes	Yes	No
[32]	2020	PLA for IoT	Yes	Partial	None	Spoofing, Eavesdropping	Yes	No	No	No	Yes	Yes
[33]	2020	PLA Fundamentals	Partial	No	None	Spoofing, Eavesdropping	Yes	No	No	No	Yes	Yes
[34]	2019	RFID Security	Yes	Yes	DL (discriminative)	Spoofing	Yes	No	Yes	Yes	Yes	Yes
[35]	2019	ML-based PLA	Partial	Yes	Supervised, DL	Spoofing, Eavesdropping	Yes	No	No	No	Yes	Yes

Analytical Discussion of Each Survey Study

- [26] (2023) - **PLS Mechanisms Analysis:** The most recent study (2023) overviews PLS mechanisms, focusing on eavesdropping and jamming defenses in wireless communications. It lacks IoT and DL coverage, relying on theoretical analysis without experimental validation or datasets. It highlights challenges (e.g., scalability) and future directions (e.g., emerging applications), but its non-ML focus limits its relevance to modern WIoT trends.
- [27] (2022) - **Secure Industrial Comms Analysis:** Published in 2022, this survey examines PLS techniques for industrial communications, targeting spoofing in IoT contexts. It omits DL, using a theoretical approach without experiments or datasets. It discusses industry-specific challenges and future directions, though its industrial focus reduces applicability to broader WIoT scenarios.
- [28] (2022) - **RF Fingerprinting Analysis:** This 2022 survey comprehensively reviews RF fingerprinting, comparing traditional and DL approaches (discriminative models) for spoofing, with partial IoT focus. It lacks experimental results or datasets but addresses challenges (e.g., scalability, noise) and future directions. Its theoretical nature limits practical insights.
- [29] (2021) - **NFC Security Analysis:** Released in 2021, this study applies DL-aided RF fingerprinting to NFC security, targeting spoofing with discriminative models. It includes experimental validation and datasets, noting challenges (e.g., scalability) and future directions. Its lack of IoT consideration and NFC-specific scope restrict its relevance to WIoT.
- [30] (2021) - **IoT Device Detection Analysis:** This 2021 survey explores ML for IoT device detection, addressing spoofing with unspecified models. It emphasizes IoT but lacks experimental results or datasets. Challenges (e.g., device diversity) and future directions are included, though its limited PLA focus reduces its contribution to physical-layer security.
- [31] (2020) - **RF Fingerprinting Analysis:** Published in 2020, this work proposes DL-based RF fingerprinting with data augmentation for spoofing in IoT, using discriminative models. It offers experimental results and datasets, identifying challenges (e.g., channel resilience) and future directions. Its narrow fingerprinting focus limits broader PLA integration.
- [32] (2020) - **PLA for IoT Analysis:** This 2020 survey focuses on PLA in wireless communications with an IoT emphasis, targeting spoofing and eavesdropping. DL is partially covered without specific models, and it lacks experiments or datasets. Challenges (e.g., scalability) and future directions (e.g., IoT security) are noted, but adversarial ML is underexplored.
- [33] (2020) - **PLA Fundamentals Analysis:** Also from 2020, this survey covers PLA fundamentals, addressing spoofing and eavesdropping with channel-based methods. IoT

is partially considered, and DL is absent, with no experimental validation or datasets. It discusses challenges (e.g., dynamic networks) and future trends, but its general scope limits WIoT specificity.

- [34] (2019) - **RFID Security Analysis:** Published in 2019, this work investigates DL for RFID security in IoT, focusing on spoofing with unspecified DL models. It includes experimental evaluations and datasets, discussing challenges (e.g., broader applications) and future directions (e.g., cognitive intelligence). Its RFID-specific scope limits generalizability to WIoT or 6G.
- [35] (2019) - **ML-based PLA Analysis:** An early 2019 study, it explores ML-based PLA for 5G networks, using supervised and DL methods for spoofing and eavesdropping detection. IoT is partially addressed, but its theoretical approach lacks experiments or datasets. It identifies challenges (e.g., real-time performance) and future directions (e.g., beyond 5G), though it misses 6G contexts.

1.5 Research gaps & Motivations

Based on the previous surveys, we will explain the gaps in current research such as:

The surveys reviewed in section 1.2 ([26]-[35]) provide valuable insights into physical layer security (PLS) and authentication (PLA) in wireless networks, but several critical research holes remain unaddressed. These holes, derived from the limitations of existing studies, emphasize the need for a comprehensive study of deep learning (DL) -enhanced PL for wireless Internet of Things (Wiot) systems, especially in the context of new 6G networks. Below, we outline the primary gaps and the motivations driving this survey.

A prominent gap is the lack of experimental evaluations for DL techniques in PLS. While studies such as [28], [29], [31] and [34] incorporate DL for RF fingerprints, NFC Security and RFID applications, many others ([26], [27], [32], [33], [35]) are exclusively on theoretical framework without empirical framework. For example, [28] DL-based RF-fingerprints maps, but gives no experimental results to substantiate their claims and limit practical insight into the model performance. This absence of experimental evidence prevents the understanding of DL's real efficiency in strengthening PLS and motivating our work to provide experimental analysis and validation DL techniques in Wiot environments.

Another recurrent restriction is the narrow focus on authentication, often for the exclusion of wider PLS mechanisms. Studies such as [29], [32], [33] and [35] address the PLA, aimed at spoofing and eavesdropping, while neglecting other threats such as jamming, which are only short covered in [26] and [31]. This authentication-centric approach, seen in [27] industrial focus and [30] unit detection scope, overlooks the holistic security needs of Wiot systems, where different attack vectors coexist. Our survey is motivated to expand beyond authentication and integrates DL to address a wider range of PLS threats in Wiot.

The absence of future insights on PLS security for 6G and next-generation IoT systems is a significant gap across most studies. Early works like [34] and [35] from 2019 focus on 5G-era challenges, while even recent surveys ([26], [27], [28]) provide limited discussion on 6G-specific requirements, such as ultra-low latency, massive connectivity, or heterogeneous network integration. For example, [26] (2023) suggests emerging applications but does not tailor its PLS outlook to 6G, and [32] lacks scalability insights for next-gen IoT. This gap drives our motivation to explore DL's potential in futureproofing PLS for 6G-enabled WIoT ecosystems.

Additional gaps include the limited exploration of adversarial machine learning (ML) and insufficient IoT consideration in PLS contexts. None of the surveys ([26] – [35]) address adversarial attacks on DL models, a critical oversight given the vulnerability of ML-based security systems. Furthermore, studies like [26], [29], and [35] either exclude or only partially consider IoT, missing the unique constraints (e.g., resource limitations) of WIoT devices. These deficiencies motivate our survey to investigate adversarial resilience and tailor DL solutions to IoT-specific challenges.

Finally, the lack of dataset discussion limits in many studies ([26], [27], [28], [30], [32], [33], [35]) Reproducing and benchmarking of PLS techniques. Even when data sets are used (e.g. [29], [31], [34]), their scope is narrow (e.g., NFC or RFID) and does not reflect the diversity of Wiot scenarios. This motivates our inclusion of experimental analysis with broader data set considerations to promote PLS research.

1.6 Research Methodology

This section outlines the methodology used to conduct our survey on Deep Learning (DL) techniques for physical layer security (PLS) in Wireless Internet of Things (Wiot) systems. Our approach is designed to extensively undergo the state -of -the -art, bridge theoretical advances and practical implementations, while also addressing challenges in the real world. The methodology includes the scope of the survey, election criteria, paper collection strategy and visualization of important trends, as described below.

Survey Scope and Selection Criteria

Our survey focuses specifically on deep learning techniques applied to PLS in Wiot, a critical intersection of innovative technologies aimed at strengthening safety in the next generation of wireless networks. We consider both theoretical and experimental works to capture a comprehensive view of the field, from basic concepts to validated solutions. The scope includes research that addresses applications in the real world (e.g., IoT device approval), data set-based analysis (e.g., RF Fingerprint Data set) and conflicting threats (e.g., events on DL models). This broad scope ensures that our survey not only emphasizes current performance but also identifies practical and safety-related holes for future exploration.

Survey Approach & Paper Collection Strategy

To collect relevant literature, we retrieved papers from reputable databases: IEEE Xplore, ACM Digital Library, Springer and ScienceDirect. These platforms were chosen for their extensive coverage of high quality, peer -reviewed publications in electrical engineering, computer science and related fields. The search was governed by specific keywords to target our focus area, including:

- "Deep Learning"
- "Physical-Layer Security"
- "Wireless Internet of Things"
- "PLS in WIoT"
- "DL-based Authentication"
- "Adversarial Machine Learning in PLS"
- "RF Fingerprinting"

These keywords were combined (e.g., "Deep Learning AND Physical-Layer Security") to refine the search and ensure relevance to our objectives. We applied the following filtering strategies:

- **Relevance:** Papers must directly address DL techniques in PLS or WIoT security contexts.
- **Recency:** We prioritized works published between 2018 and 2025 to reflect the latest advancements, aligning with the rapid evolution of DL and 6G technologies (noting that 2025 includes preprints or first access papers as of March 22, 2025).
- **Citations:** Highly cited papers were favored to emphasize influential works, though emerging studies with fewer citations were included if highly relevant.

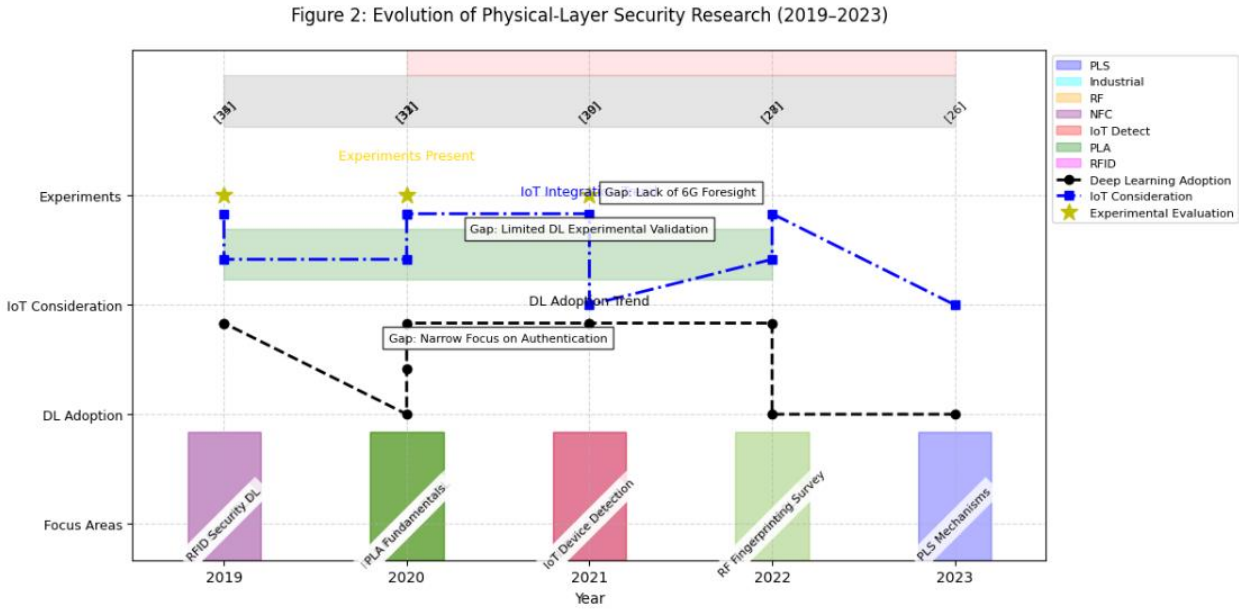


Figure 2. Graphical Representation of the Evolution of Physical-Layer Security Research

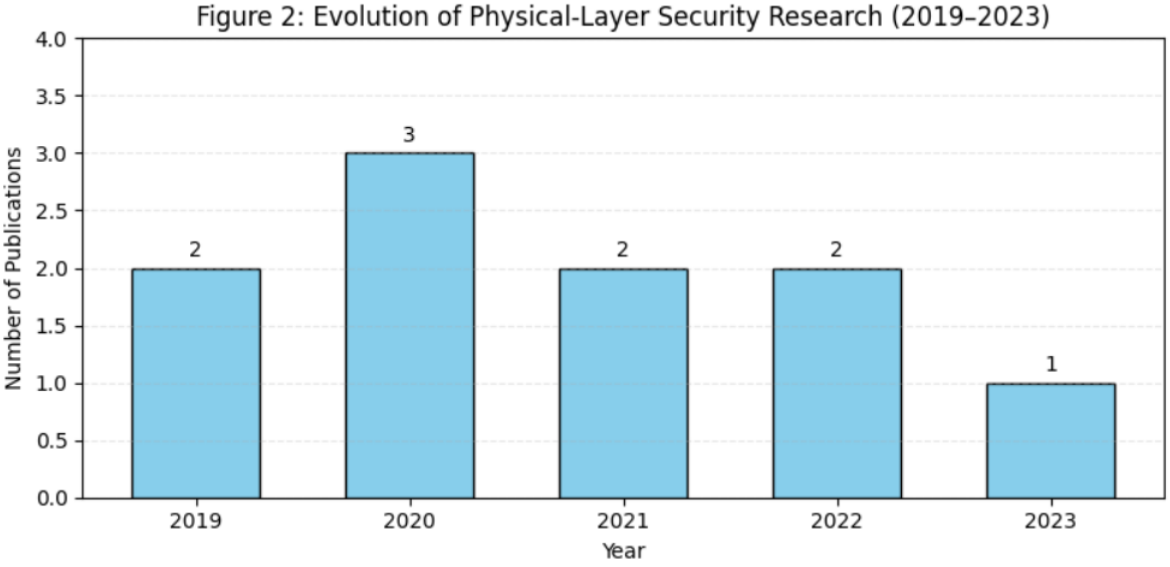


Figure 3. Graphical Representation of the Evolution of Physical-Layer Security Research

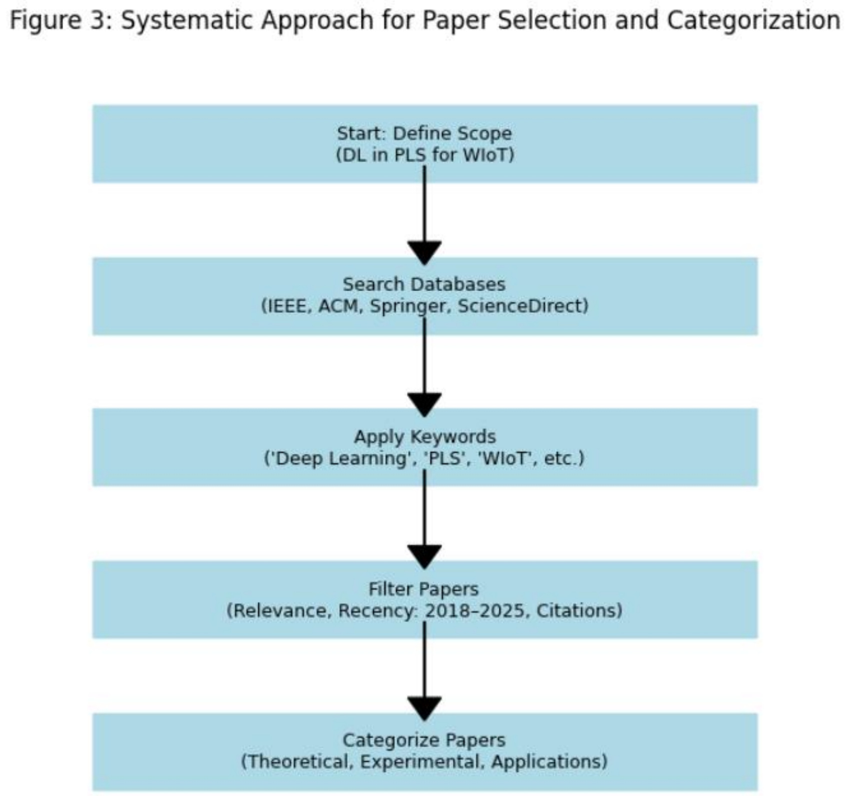


Figure 3: Systematic Approach for Paper Selection and Categorization
Start: Define Scope
(DL in PLS for WIoT)
Search Databases
(IEEE, ACM, Springer, ScienceDirect)
Apply Keywords
('Deep Learning', 'PLS', 'WIoT', etc.)
Filter Papers
(Relevance, Recency: 2018–2025, Citations)
Categorize Papers
(Theoretical, Experimental, Applications)

Figure 4.: **Systematic Approach for Paper Selection and Categorization**

1.7 Contributions

This study makes several important contributions to the field of Physical Layer Security (PLS) in the Wireless Internet of Things (Wiot) systems, with special emphasis on the use of Deep Learning (DL) techniques. By synthesizing existing literature, introducing structured taxonomies and providing action-related insights, our work addresses critical holes identified in previous studies (section 1.5) and provides a basis for future research. The main contributions are outlined below.

1. **Comprehensive Review of Deep Learning for PLS in Wireless IoT** We provide an exhaustive review of DL techniques applied to PLS within WIoT contexts, covering theoretical frameworks, experimental studies, and practical implementations from 2018 to 2025. Unlike previous surveys (e.g., [26], [32]), which often focus narrowly on authentication or lack of experimental validation, our analysis integrates diverse aspects such as eavesdropping, jamming, and spoofing defenses, offering a holistic perspective on DL's role in enhancing WIoT security.
2. **Systematic taxonomy of physical security threats and countermeasures** We propose a systematic taxonomy that categorizes security threats of physical layers (e.g., eavesdropping, jamming, spoofing) and their corresponding countermeasures in Wiot systems. This structured classification addresses the fragmented focus for previous works (e.g. [27], [29]) by mapping threats to specific PLS techniques,

including channel-based methods, RF fingerprints and DL-driven solutions, thereby giving a clear framework for researchers and athletes.

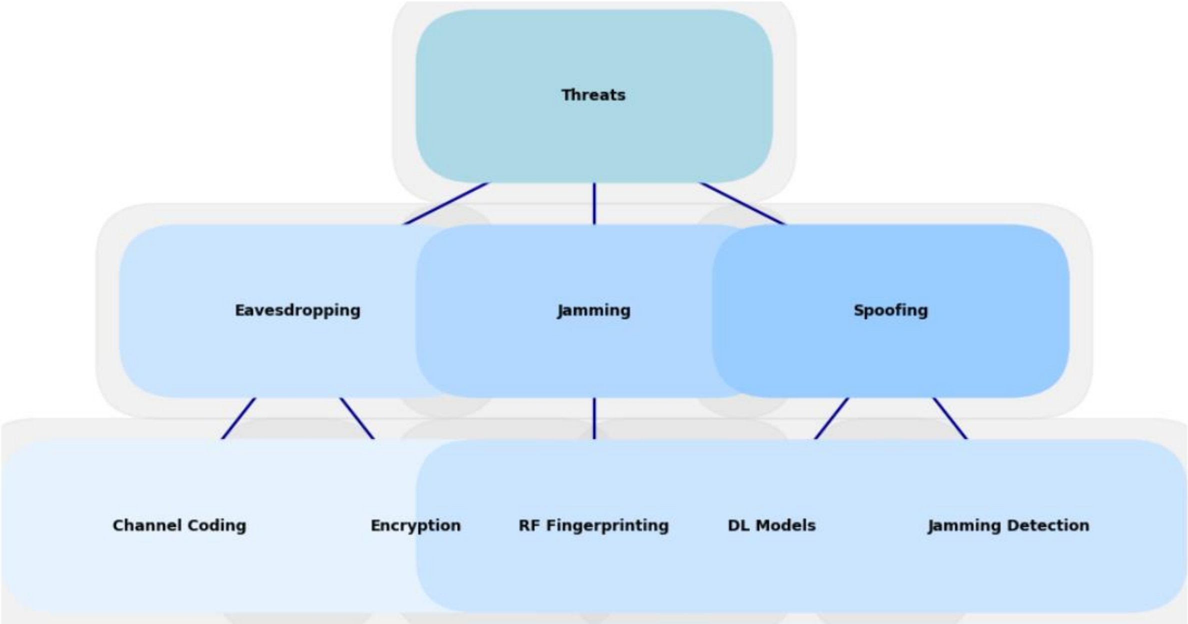


Figure 5: **Systematic taxonomy of physical security threats and countermeasures**

3. **Systematic Taxonomy of Deep Learning Solutions for Physical Security** A novel taxonomy of DL solutions for PLS is introduced, detailing architectures (e.g., CNNs, RNNs, GANs), training approaches (e.g., supervised, unsupervised), and application scenarios (e.g., authentication, anomaly detection). This contribution extends beyond the limited DL coverage in surveys like [33] and [35], offering a comprehensive guide to selecting and adapting DL models for WIoT security challenges.

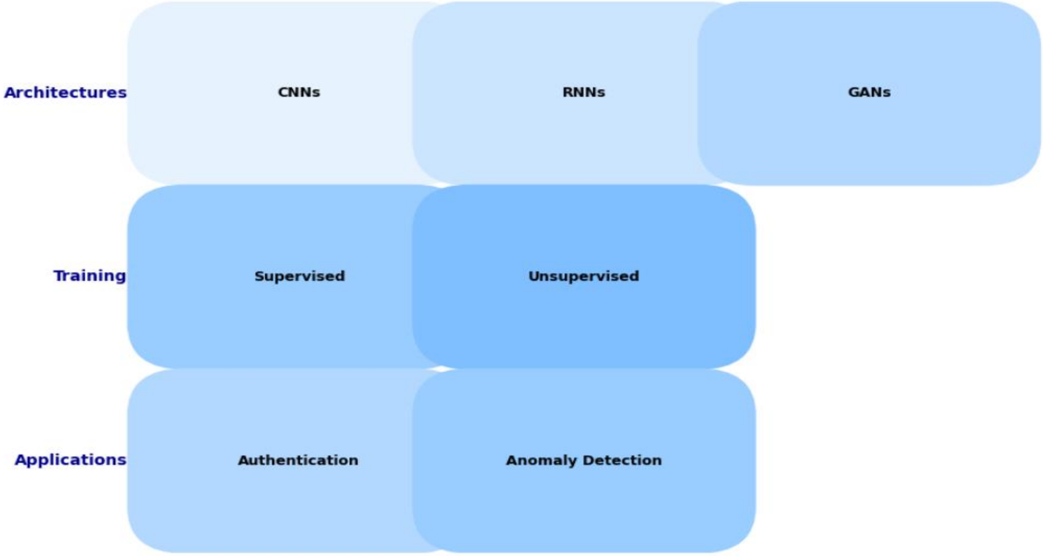


Figure 6: Systematic Taxonomy of Deep Learning Solutions for Physical Security

4. **Extensive review of real and synthetic datasets** We compile and analyze a wide range of datasets used in DL-PLS research, including datasets in the real world (e.g., RF signal prisoners from IoT devices) and synthetic datasets (e.g., simulated Wiot-channel models). This review addresses the gap in data set discussion that is listed in previous works (e.g. [26], [28]), and provides insight into data availability, quality, and suitability for benchmarking DL Techniques in Wiot Security.

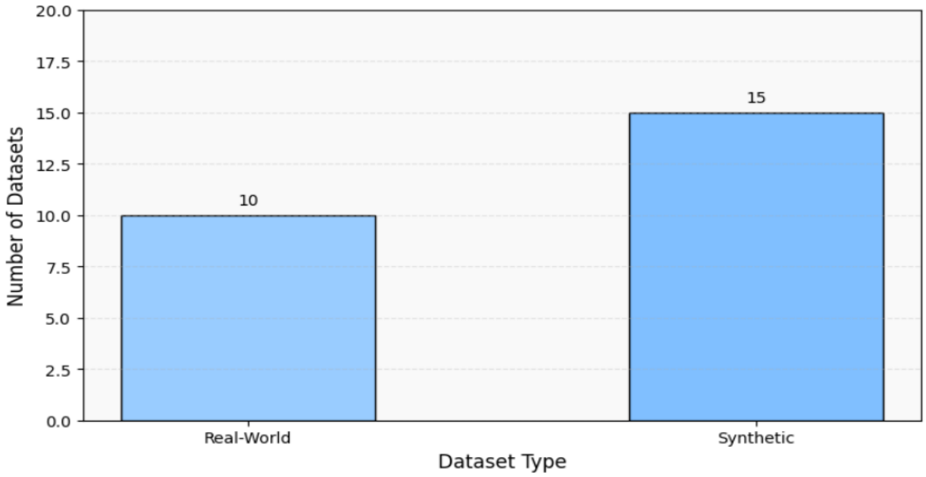


Figure 7: Dataset Overview

5. **Reproducible Benchmark of Deep Learning Techniques in PLS Case Studies** Our survey includes a reproducible benchmark of DL techniques across multiple PLS case studies, such as RF fingerprinting for device authentication and jamming detection in WIoT networks. By detailing experimental setups, metrics (e.g., accuracy, false positive rate), and results, we offer a standardized evaluation framework that enhances the reproducibility lacking in studies like [27] and [30], enabling fair comparisons and validation.
6. **Roadmap for Future Work** We present a forward-looking roadmap that outlines key research directions for DL in PLS within WIoT, including integration with 6G technologies, resilience against adversarial attacks, and scalability for massive IoT deployments. This roadmap builds on the limited future insights of prior surveys (e.g., [26], [34]), providing actionable recommendations to guide the next wave of research and development.

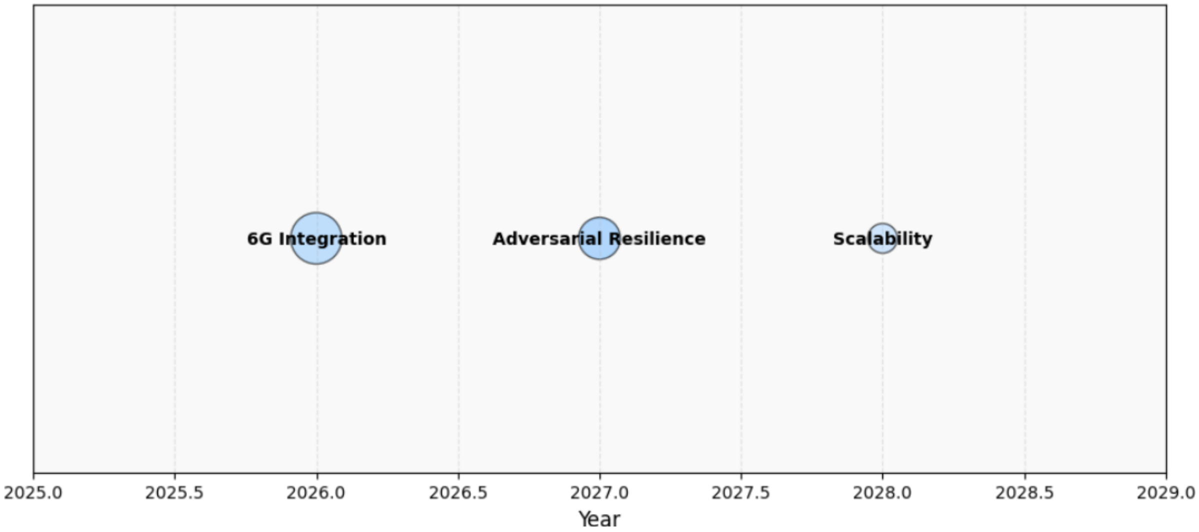


Figure 8: Roadmap for Future Work

1.8 Structure of Survey

Herein, we will explain the outline of our survey based on the given sections.

2. Background and Fundamentals

2.1. Wireless Internet of Things (WIoT)

The Wireless Internet of Things (Wiot) represents a transformative paradigm in modern connection, enabling seamless communication between billions of devices through wireless networks. As a development of the broader Internet of Things (IoT), WIoTs utilize wireless technologies to connect devices with low power, sensors and actuators, which facilitate real -time data exchange across different applications. This section provides a thorough exploration of WIoTs, focusing on its applications and inherent properties, which sets the stage to understand the safety challenges and role of deep learning (DL) in improving physical layer security (PLS).

2.1.1. Overview of Wireless IoT (WIoT) and Its Applications

The spread of WIoT has catalyzed advances in a variety of domains, and transformed how data is collected, processed and used in scenarios in the real world. Below we discuss its central role in important application areas: Smart cities, health care, industry 4.0, autonomous systems and intelligent transport.

- **Smart cities**: WIoT supports the infrastructure in smart cities by activating interconnected urban management systems. Wireless sensors monitor environmental parameters (e.g. air quality, temperature), while smart meters optimize the energy division, and connected streetlights adapt to traffic patterns. For example, real-time data from Wiot devices can reduce energy consumption by up to 20% in urban networks [36]. This massive connection improves efficiency, but also reinforces security risk, as cut -off data can interfere with critical services.
- **Healthcare**: In the health care system, WIoTs facilitates external patient monitoring and telemedicine through laptops and wireless implants. These devices transfer important characters (e.g. heart rate, glucose level) to medical servers, enabling timely interventions. A 2023 study estimated that the Wiot-enabled health care system can reduce the backdrop of hospitals by 15% [37]. However, the sensitivity of health data requires robust security to prevent unauthorized access or tampering.
- **Industry 4.0:** WIoT runs the fourth industrial revolution by integrating wireless sensors and actuators into production processes. These devices enable predictive maintenance, real -time retention and automated quality control, and improve operating efficiency by up to 30% in smart factories [38]. However, the dependence on wireless communication exposes industrial systems to jamming or counterfeiting attacks, and threatening production continuity.
- **Autonomous systems:** Autonomous drones and robots rely on WIoT for navigation, coordination and data exchange. For example, drone swarms use wireless links to share position data and achieve precise collective behavior in applications such as search-and-rescue missions. The latency nature of these systems requires light security solutions that traditional methods struggle to provide [39].
- **Intelligent transport:** WIoT improves intelligent transport systems (ITS) by connecting vehicles, traffic lights and infrastructure. Vehicle-to-vehicle (V2V) and vehicle-to-

infrastructure (V2I) communication, enabled by Wiot, reduces traffic overload and accidents studies suggest a potential 25% reduction in the collision rate [40]. Nevertheless, the sending nature of these wireless links makes them vulnerable to eavesdropping, and compromises safety -critical data.

The various uses of WIoT highlight their role as a cornerstone in modern technological ecosystems. In 2025, estimates indicated that over 25 billion IoT devices worldwide, with a significant part of operating wirelessly, emphasizes the scale and effect of WIoT distributions [41]. However, this growth is accompanied by a heterogeneous landscape of devices and operational limitations, which we discuss further.

The heterogeneous nature of WIoT derives from the diversity of its constituents and their operating requirements. WIoT ecosystems consist of low power devices such as battery-powered sensors, laptops and actuators, often limited by limited calculation resources, memory and energy capacity. For example, a typical WIoT sensor can operate with a power budget of less than 10 mW, requiring energy-efficient protocols and security mechanisms [42]. These resource restrictions contrast with the huge WIoT connection requirements, where networks must support thousands - or even millions - by devices at the same time, seen in dense urban distributions or industrial IoT settings.

This heterogeneity presents significant challenges for security design. Low power devices cannot maintain calculation overhead for traditional cryptographic methods such as RSA or AES, which require extensive processing and key control [43]. Furthermore, the huge scale of WIoT networks reinforces interoperability problems, as devices from different manufacturers can use varying communication protocols (e.g. Zigbee, LoRaWAN, NB-IoT). WIoT dynamic topology, with devices that often join or leave networks, complicates further security, as static solutions struggle to adapt to rapid changes. These characteristics—low-power operation, resource constraints, and massive connectivity—underscore the need for lightweight, scalable, and adaptive security approaches, such as PLS enhanced by DL

2.1.2. Architectural Components of Wireless IoT Networks

Wireless Internet of Things (Wiot) networks are complex ecosystems that integrate different devices, communication technologies and processing options to enable seamless data exchange and real -time functionality. Understanding their architecture is crucial to identifying security problems and utilizing deep learning (DL) to improve physical layer security (PLS). This subsection presents a layered diagram of WIoT network architecture, comprising the perception layer, network layer, and application layer, followed by a detailed discussion of each component's role and characteristics.

Layered Diagram Description
The proposed diagram is a three-tiered vertical stack, visually representing the hierarchical structure of WIoT networks. At the base is the **Perception Layer**, depicted as a collection of interconnected icons representing sensors, RFID tags, and nodes, symbolizing data collection from the physical environment. Above it lies the **Network Layer**, illustrated with icons for Wi-Fi routers, LPWAN gateways, and 5G/6G base stations, connected by

dashed lines to indicate wireless data transmission. At the top is the **Application Layer**, shown as a cloud with embedded icons for edge AI devices (e.g., edge servers) and centralized cloud processing units, linked to the network layer below. Arrows between layers indicate bidirectional data flow, emphasizing the interaction across tiers. The diagram is captioned to integrate with your survey's figure sequence [44].

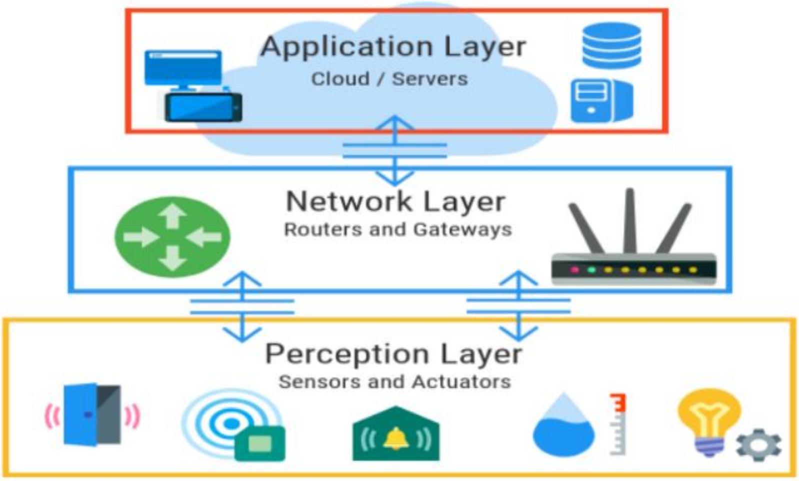


Figure 9: Architectural Layers of WIoT Networks

1. **Perception Layer:** serves as a basic level of Wiot networks, responsible for feeling and collecting data from the physical world. This layer includes a variety of devices such as sensors (e.g. temperature, movement, humidity), radio frequency identification (RFID) marks and nodes (e.g. low -power microcontrollers). These components are typically resource-limited, operating on limited power budgets-on-less than 10 mW [42]-and designed for specific tasks such as environmental monitoring or tracking of assets. For example, in smart cities, sensors detect air quality, while RFID codes track inventory in industry 4.0 settings [45]. The heterogeneity of these devices, combined with their dependence on wireless communication, exposes them to threats of physical layers such as intercepting and counterfeiting, which necessitate light security solutions such as PLS [46].
2. **Network Layer** facilitates the transfer of data collected by the perception layer to higher -level treatment devices. It includes a variety of wireless communication technologies that are adapted to Wiot's various requirements, including Wi-Fi, low power networks (LPWAN), 5G and new 6G networks. Wi-Fi provides high bandwidth connections for short-term applications, such as home automation, while LPWAN (e.g. LoRaWAN, NB-IoT) supports long-distance, low-power communication for remote sensors, and achieves areas up to 10 km of minimal energy consumption [47]. 5G networks offer ultra-low latency (e.g. <1 ms) and solid device connection (up to 1 million units/km^2), critical for intelligent transport and autonomous systems [48]. When we look forward, 6G promises even greater abilities, such as Terahertz frequencies and integrated sensing and communication (ISAC) and improving Wiot scalability and precision.

However, the broadcast nature of these wireless channels makes them susceptible to jamming and interception, underscoring the need for PLS to secure data at this layer.

3. **Application Layer:** The application layer manages and analyzes data received from the network layer, providing actionable insights and services. It includes edge AI and cloud processing components, reflecting the shift toward distributed and centralized computation in WIoT systems. Edge AI, deployed on devices like gateways or local servers, enables real-time processing—such as anomaly detection in healthcare wearables—reducing latency and bandwidth demands [49]. For instance, edge AI can process sensor data locally to adjust traffic lights in intelligent transportation systems [50]. Conversely, cloud processing leverages vast computational resources for complex tasks, such as predictive analytics in Industry 4.0 or large-scale data aggregation in smart cities [51]. This layer's reliance on secure data inputs from lower layers highlights the importance of PLS, as compromised data at the perception or network layer could undermine application-layer integrity [52].

   Interplay and Security Implications The layered architecture of WIoT networks illustrates a dynamic interplay where data flows from the perception layer through the network layer to the application layer, and control signals may flow in reverse. This bidirectional interaction supports real-time adaptability but amplifies security challenges. The perception layer's resource constraints limit traditional cryptographic overhead, the network layer's wireless medium invites physical-layer attacks,[53] and the application layer's dependence on data integrity demands robust foundational security. DL-enhanced PLS addresses these issues by leveraging physical-layer features (e.g., Channel State Information, RF fingerprints) and adaptive algorithms (e.g., CNNs, RL) to secure WIoT networks across all layers.

2.1.3. Communication Technologies in WIoT

Wireless Internet of Things (Wiot) networks depend on a diverse set of communication technologies to enable connection across their heterogeneous devices and applications. These technologies, ranging from short range protocols, high bandwidth protocols such as Wi-Fi to long distance, low streams such as Lora and NB-IoT, and advanced cellular standards such as 5G and Emerging 6G, offer each unique ability tailored to Wiot's needs. However, their wireless nature introduces inherent security issues that threaten data integrity, confidentiality and availability.

Overview of Security Vulnerabilities The communication technologies in Wiot face a range of safety challenges due to their dependence on the wireless medium, which is inherent cutting, jamming and counterfeiting. Wi-Fi, widely used in home automation and smart buildings, uses encryption standards such as WPA3, and are still vulnerable to intercepting and playing for attacks if faulty or utilized via weak passwords [54]. LoRa, a Low-Power Wide-Area Network (LPWAN) protocol, supports long-range communication for applications like smart agriculture, but its lightweight security (e.g., AES-128 encryption) can be compromised by key interception or physical-layer jamming due to its low data rate and extended transmission time [55]. NB-IoT, another LPWAN technology optimized for massive IoT deployments, leverages cellular infrastructure with robust authentication, yet its broadcast nature exposes it to denial-of-service (DoS) attacks and signal spoofing [56].

5G networks, critical for latency-sensitive applications like intelligent transportation, offer advanced security features such as enhanced encryption and network slicing, but their complexity introduces vulnerabilities like signaling storms and physical-layer attacks targeting massive device connectivity [57]. Emerging 6G technologies, still in development, promise integrated sensing and communication (ISAC) and terahertz frequencies, enhancing WIoT scalability; however, their nascent security frameworks may struggle with novel threats like quantum-based attacks and increased attack surfaces from ultra-dense networks [58]. These vulnerabilities underscore the limitations of traditional upper-layer security in WIoT and highlight the need for physical-layer security (PLS) solutions, which can leverage channel characteristics to mitigate risks without excessive computational overhead.

The following table compares important WIoT communication technologies based on their data rate, range, security features, energy efficiency and applications. This comparison provides a basis for understanding their suitability and security implications in WIoT contexts.

Table description: The table is structured with **six** columns: technology, data rate, range, security features, energy efficiency and applications. Each row corresponds to specific technology (Wi-Fi, LoRaWAN, NB-IoT, 5G, 6G). Data is taken from peer-reviewed literature and industry standards.

Table 2. Comparison of Wireless IoT Communication Technologies

Technology	Data Rate	Range	Security Features	Energy Efficiency	Applications
Wi-Fi	Up to 9.6 Gbps [54]	~100 m	WPA3, AES encryption; vulnerable to eavesdropping, replay attacks	Moderate	Home automation, smart buildings
LoRa	0.3–50 kbps [55]	Up to 10 km	AES-128; susceptible to jamming, key interception	High	Smart agriculture, remote sensing
NB-IoT	~250 kbps [56]	Up to 10 km	Cellular-grade encryption; prone to DoS, spoofing	High	Smart metering, asset tracking
5G	Up to 20 Gbps [57]	~1 km (urban)	Enhanced encryption, slicing; risks from signaling attacks	Moderate	Intelligent transportation, AR/VR
6G	>1 Tbps [58]	~1–10 km	ISAC, quantum-resistant untested vulnerabilities	TBD	Autonomous systems, holographic comms

Discussion of Table 1

- **Wi-Fi**: Offers high data rates (up to 9.6 Gbps with Wi-Fi 6) and is ideal for short-range, high-bandwidth applications, but its moderate energy efficiency and limited range (100 m) restrict its use in large-scale WIoT deployments. Security vulnerabilities include eavesdropping and replay attacks, exploitable via weak configurations [54].
- **LoRa**: Designed for low-power, long-range communication (up to 10 km), LoRa's low data rate (0.3–50 kbps) suits remote sensing, but its prolonged transmission time increases jamming risks, and AES-128 encryption can be bypassed if keys are intercepted [55].
- **NB-IoT**: Balances range (10 km) and data rate (~250 kbps) with high energy efficiency, making it suitable for massive IoT applications like smart metering. Its cellular security is robust, yet DoS and spoofing remain concerns due to its wide coverage [56].
- **5G**: Provides ultra-high data rates (up to 20 Gbps) and low latency, supporting real-time WIoT applications. Its security features are advanced, but the complexity of massive connectivity introduces physical-layer vulnerabilities [57].
- **6G**: Projected to exceed 1 Tbps with terahertz frequencies, 6G aims to enhance WIoT scalability and precision. Its security features are still speculative, with potential quantum-resistant mechanisms, but new threats are anticipated [58].

Security Implications

The diverse security vulnerabilities across these technologies—ranging from eavesdropping in Wi-Fi to jamming in LoRa and signaling attacks in 5G—highlight the inadequacy of upper-layer cryptography alone, especially for resource-constrained WIoT devices. PLS, enhanced by DL techniques like anomaly detection and RF fingerprinting, offers a lightweight, adaptive solution to secure these protocols at the physical layer, addressing the broadcast nature of wireless communication and the dynamic threat landscape of WIoT networks.

2.2. Threat Models in Wireless IoT

Wireless Internet of Things (Wiot) networks, by virtue of their design and operational properties, are inherently exposed to a wide range of security threats. This vulnerability dates from three primary factors: their distributed nature, limited encryption skills and exposure to the wireless medium. presented a detailed categorization of security threats in Table 3, and visualized their impact on Confidentiality, Integrity and Availability (CIA) Triad, and provided a basis for understanding the necessity of physical layer security (PLS) improved by deep learning (DL). **Why WIoT is Highly Vulnerable** is the distributed nature of WIoT occurs from its deployment across large, heterogeneous ecosystems - exciting smart cities, health care and industrial applications - where units operate autonomously with minimal centralized supervision. This decentralization complicates security management, as devices often lack calculation resources to implement robust monitoring or updates, leaving them exposed to utilization [59]. Limited encryption skills further deteriorate this vulnerability; Many WIoT devices, such as low power sensors and RFID codes, operate on limited power budgets (e.g. <10 MW [42]), which reproduce traditional cryptographic methods such as RSA or AE's impractical due to their high calculation overhead [60]. Consequently, light safety mechanisms are often used, which can be inadequate against sophisticated attacks. Finally, wireless exposure, which is inherent for Wiot's dependence on technologies such as Wi-Fi, Lora and 5G, data transfer receptive to cutting, joint and manipulation, as signals are sent over open channels available to opponents [61]. These factors collectively amplify the attack surface, necessitating adaptive, resource-efficient security solutions like DL-enhanced PLS.

The following table categorizes large security threats in Wiot, and describes their descriptions, targeted layers, impacts and examples of scenarios. It includes Jamming, Eavesdropping, Spoofing, Man-in-the-Middle (MITM), Sybil Attacks, Replay Attacks, and Adversarial ML Attacks.

Table description: The table has **five** columns: Threat Type, Attack Description, Targeted Layer (Physical, MAC, Network, Application), Impact, and Example Scenarios. Each row represents a clear threat, taken from literature and practical Wiot contexts.

Table 3: Categorization of security threats in wireless IoT

Threat Type	Attack Description	Targeted Layer	Impact	Example Scenarios
Jamming	Transmitting noise to disrupt communication	Physical	Availability	Disrupting smart meter data transmission [62]
Eavesdropping	Intercepting wireless signals to steal data	Physical, Network	Confidentiality	Capturing health data from wearables [63]
Spoofing	Impersonating a legitimate device or signal	Physical, MAC	Integrity	Faking RFID tags in inventory tracking [64]
MITM	Intercepting and altering communication between devices	Network	Confidentiality, Integrity	Modifying traffic light signals in ITS [65]
Sybil Attacks	Creating multiple fake identities to overwhelm network	Network, Application	Integrity, Availability	Flooding a smart grid with false nodes [66]
Replay Attacks	Re-transmitting captured data to deceive devices	Network, Application	Integrity	Replaying drone control signals [67]
Adversarial ML Attacks	Manipulating ML models via crafted inputs	Application	Integrity, Confidentiality	Poisoning edge AI for anomaly detection [68]

Discussion of Table 2

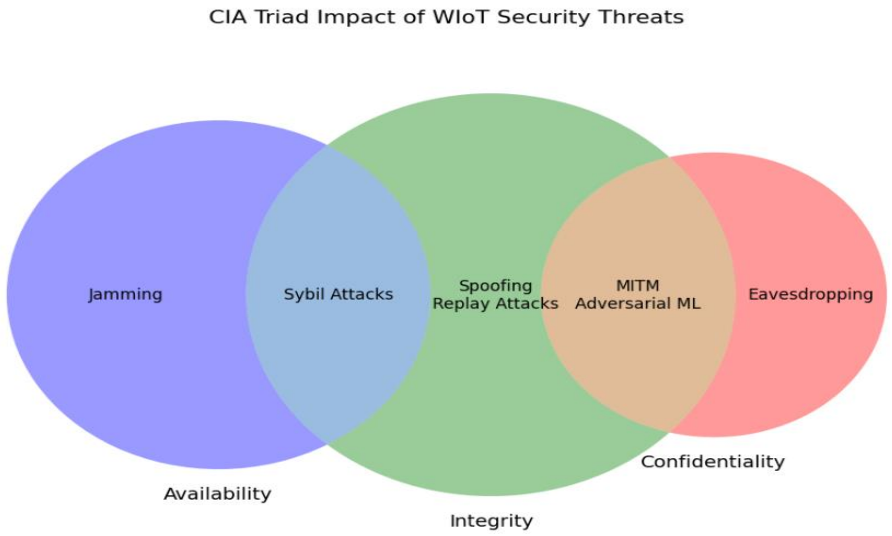
- **Jamming**: Targets the physical layer by overwhelming the wireless channel with noise, disrupting availability (e.g., blocking smart meter updates [62]).
- **Eavesdropping**: Exploits the physical and network layers to breach confidentiality, such as intercepting sensitive health data from wearables [63].
- **Spoofing**: Affects physical and MAC layers, undermining integrity by mimicking legitimate signals (e.g., counterfeit RFID tags [64]).
- **MITM**: Operates at the network layer, compromising both confidentiality and integrity (e.g., altering traffic signals [65]).
- **Sybil Attacks**: Targets network and application layers, degrading integrity and availability by introducing fake identities (e.g., smart grid overload [66]).
- **Replay Attacks**: Affects network and application layers, falsifying data integrity (e.g., replaying drone commands [67]).
- **Adversarial ML Attacks**: Targets the application layer, particularly edge AI, by manipulating DL models to misclassify data, affecting integrity and confidentiality [68].

Visualization of Wireless Attacks

The proposed visualization is a Venn diagram with three overlapping circles labeled Confidentiality, Integrity, and Availability, representing the CIA Triad. Each threat from Table 2 is plotted within the diagram based on its primary impact:

- **Confidentiality (left circle)**: Eavesdropping, MITM, Adversarial ML Attacks overlap here, as they expose sensitive data.
- **Integrity (right circle)**: Spoofing, MITM, Sybil Attacks, Replay Attacks, and Adversarial ML Attacks intersect, altering data or system behavior.
- **Availability (bottom circle)**: Jamming and Sybil Attacks dominate, disrupting service access.
- Overlaps show multi-impact threats (e.g., MITM affects Confidentiality and Integrity). The diagram is captioned "Figure 3: CIA Triad Impact of WIoT Threats" and annotated with threat names for clarity.

Figure 10: CIA Triad Impact of WIoT Threats



To further contextualize these threats and explore molding strategies, Figure 4 illustrates a comprehensive framework for Wiot Security. The diagram categorizes threats into two groups: imitation attacks (e.g. Eavesdropping, Spoofing, Sybil Attacks, MITM, Jamming, DoS) and Malware attacks (e.g. Viruses, Trojans, Privacy Leakage, DoS). These threats are aimed at a "safe IoT relief with learning" core, which uses learning -based authentication, detection of harmful software and access control to counteract them. This framework emphasizes the potential of deep learning techniques-for example, those who utilize physical layer functions (e.g. channel status information, RF fingerprint)-to address Wiot's safety challenges, and set the stage for the detailed exploration of DL-enhanced PLs in subsequent sections.

Security Implications

The distributed nature, limited encryption, and wireless exposure of WIoT amplify these threats, as resource constraints preclude heavy cryptographic defenses, and the open medium invites physical-layer exploitation. DL-enhanced PLS offers a promising countermeasure by leveraging physical-layer features (e.g., Channel State Information, RF fingerprints) and adaptive algorithms (e.g., CNNs for anomaly detection) to mitigate these attacks efficiently, particularly at the physical and network layers where vulnerabilities are most pronounced [69].

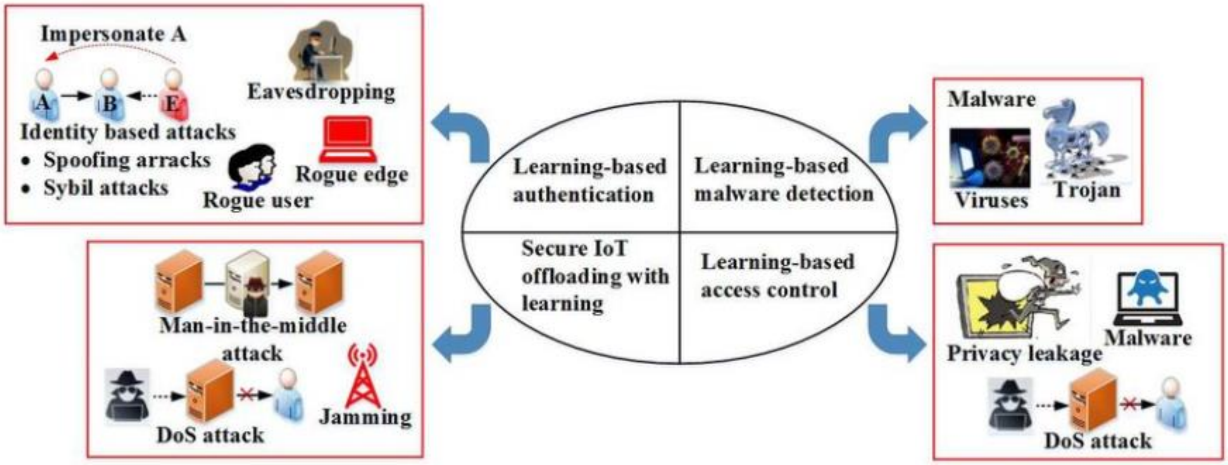


Figure 11: **Threat Model in Wireless IoT**

2.3. Physical-Layer Security (PLS) in Wireless IoT

Physical Layer Security (PLS) has emerged as a promising paradigm to meet the security challenges of the Wireless Internet of Things (Wiot) systems, especially for resource -limited devices where traditional cryptographic methods are often impractical. This section explains why PLS acts as an effective alternative to cryptographic security for light IoT applications and provides a classification of important PLS techniques in Table 4, highlighting their safety benefits, calculation costs and usefulness for IoT.

Why PLS is an Alternative to Cryptographic Security for Lightweight IoT Security

Traditional cryptographic security, such as RSA, AES or elliptical curve cryptography, depends on complex mathematical calculations to ensure data confidentiality, integrity and availability. While effective, these methods impose considerable computational overhead, making them unsuitable for light IoT devices in WIoT systems. For example, many IoT units, such as sensors and RFID codes, operate on limited power budgets (e.g. <10 MW [70]) and have limited processing options, reproducing encryption/conceptual processes of traditional methods Energy-intensive and latency inducing [71].

In a smart healthcare system, for example, a wearable device performing AES encryption might drain its battery rapidly, reducing its operational lifespan and delaying critical health alerts [63]. In contrast, PLS leverages the inherent randomness and uniqueness of the wireless channels such as Channel State Information (CSI), fading, noise, and interference—to secure communications without requiring extensive computational resources. This makes PLS particularly suitable for WIoT, where devices must operate efficiently under resource constraints. Key advantages of PLS over cryptographic security include Low Computational Overhead: PLS techniques, such as artificial noise generation or beamforming, exploiting physical-layer properties (e.g., signal propagation) rather than cryptographic algorithms, reducing the need for heavy computations [72]. Energy Efficiency: By minimizing processing demands, PLS extends the battery life of IoT devices, critical for applications like remote sensing in smart agriculture [71]. Real-Time Adaptability: PLS can dynamically adapt to channel conditions, providing robust security against physical-layer attacks like eavesdropping and jamming, which are prevalent in WIoT due to its wireless exposure [61]. Lightweight Authentication: Techniques like RF fingerprinting use unique device signatures to authenticate devices without the overhead of key management, addressing vulnerabilities like spoofing [73].

On the other hand, the PLS utilizes the inherent and uniqueness of the wireless channels - such as channel state information (CSI), fading, noise and interference - to ensure communication without requiring extensive calculation resources. This makes PLS especially suitable for WIoTs, where devices must operate effectively under resource restrictions.

Key advantages of PLS over cryptographic security include

1. **Low Computational Overhead:** PLS techniques, such as artificial noise generation or beamforming, exploit physical-layer properties (e.g., signal propagation) rather than cryptographic algorithms, reducing the need for heavy computations [74].
2. **Energy Efficiency:** By minimizing processing demands, PLS extends the battery life of IoT devices, critical for applications like remote sensing in smart agriculture [75].

3. **Real-Time Adaptability:** PLS can dynamically adapt to channel conditions, providing robust security against physical-layer attacks like eavesdropping and jamming, which are prevalent in WIoT due to its wireless exposure [76].
4. **Lightweight Authentication:** Techniques like RF fingerprinting use unique device signatures to authenticate devices without the overhead of key management, addressing vulnerabilities like spoofing [77].

Moreover, traditional cryptographic methods are increasingly at risk from emerging threats, such as quantum computing, which could break algorithms like RSA in the future [76]. PLS, being rooted in the physical properties of the channel, offers a quantum-resistant alternative, as its security does not rely on computational complexity but on the unpredictability of the wireless environment [67]. For WIoT systems, where massive connectivity and low-power operation are paramount, PLS provides a lightweight, scalable security solution that complements or even replaces upper-layer cryptography, especially at the physical and link layers where many attacks (e.g., jamming, eavesdropping) originate.

Table 3: Classification of Physical-Layer Security Techniques

Technique	Security Benefit	Computational Cost	Applicability to IoT
Jamming Detection	Identifies and mitigates jamming attacks by analyzing signal patterns	Low (signal processing-based)	High (e.g., smart grids, smart cities) [74]
Beamforming	Directs signals to legitimate users, reducing eavesdropping risks	Moderate (requires antenna arrays)	Moderate (e.g., 5G-enabled IoT devices) [75]
Cooperative Relaying	Uses intermediate nodes to enhance signal strength and confuse eavesdroppers	Moderate (coordination overhead)	High (e.g., remote IoT networks) [76]
Artificial Noise	Injects noise to mask signals from eavesdroppers	Low (simple noise generation)	High (e.g., healthcare wearables) [77]

The following table classifies key PLS techniques, detailing their security benefits, computational costs, and applicability to IoT. The techniques include jamming detection, Beamforming, Cooperative Relaying and artificial noise, which are particularly relevant for Wiot systems.

Table Description: The table has four columns: technique, Security Benefit, Computational Cost and Portability on IoT.

Discussion of Table 3

- **Jamming Detection**: This technique analyzes signal characteristics (e.g., signal-to-noise ratio) to detect jamming attacks, which disrupt availability in WIoT systems. Its low computational cost makes it highly applicable to resource-constrained devices, such as smart meters in smart grids.

- **Beamforming**: By focusing signal energy on legitimate receivers, beamforming minimizes the signal leakage to eavesdroppers, enhancing confidentiality. It requires antenna arrays, increasing computational costs, but is feasible for 5G-enabled IoT devices in intelligent transportation systems.
- **Cooperative Relaying**: Involves intermediate nodes relaying signals to improve communication reliability and security by confusing eavesdroppers. Its moderate computational cost suits distributed WIoT networks, such as remote sensors in smart agriculture.
- **Artificial Noise**: Generates noise interfering with eavesdroppers while leaving legitimate receivers unaffected, leveraging channel differences. Its low computational cost makes it ideal for lightweight IoT devices, such as wearables in healthcare.

Implications for WIoT Security

The techniques in Table 3 show the PLS ability to provide light security adapted to Wiot's limitations. By focusing on the physical layer, PLS addresses threats such as eavesdropping, jamming and spoofing directly in origin, which reduces the load on the upper layer protocols. Furthermore, integrates deep learning with PLS - for example, the use of DL for fixed -jamming detection or optimization of radiation shaping - improves adaptability and efficiency, a subject explored in later sections of this study [78]. PLS thus offers a practical, energy-efficient alternative to cryptographic security, ensuring robust protection for WIoT systems while meeting their operational demands.

2.4. Deep Learning for Security in Wireless IoT

Deep Learning (DL) has proven to be a transformative approach to strengthen security in the wireless Internet of Things (Wiot) systems, especially for real -time threat detection and mitigation. Unlike traditional methods that depend on predefined rules or static models, DL utilizes neural networks to learn complex patterns from raw data, enabling adaptive and effective security solutions. This section explores the main theory and the basics of DL in the context of Wiot Security, focusing on its use on physical layer security (PLS), and includes illustrative figures to clarify key concepts. Theory and basics of deep learning for Wiot Security Deep learning, a subgroup of machine learning, involves training artificial neural networks (ANN) with multiple layers to model high -dimensional data. In Wiot, DL is particularly valuable for safety due to its ability to treat large volumes of heterogeneous data (e.g. wireless signals, network traffic) and detect anomalies in real time. The core theory of DL for safety is about monitored, unattended and reinforcement learning paradigms, each suitable for different aspects of threat detection and mitigation [79].

1. **Supervised learning for Threat Detection**

   such as Convolutional Neural Networks (CNN) and recurrent neural networks (RNN), are trained on labeled data sets to classify or predict security threats. In Wiot, guided learning can be used to detect physical layer attacks such as jamming or eavesdropping by analyzing Channel State Information (CSI) or received signal strength indicator (RSSI). For example, a CNN can be trained on CSI data to distinguish legitimate signals from fixed way signals and achieve detection accusations above 95% in simulated Wiot environments [80]. The fundamental process involves:

   - **Data Collection**: Gathering labeled data (e.g., CSI samples labeled as "legitimate" or "jamming").
   - **Feature Extraction**: Using CNN layers to extract spatial features from wireless signals.
   - **Classification**: Outputting a threat probability (e.g., 90% likelihood of jamming).

2. **Unsupervised Learning for Anomaly Detection**
   such as Autoencoders (AEs) and Generative Adversarial Networks (GANs), are used when marked data is scarce, a common scenario in Wiot due to the dynamic nature of the attacks. AEs can learn a normal behavior model of WIoT device communications (e.g., typical RSSI patterns) and flag deviations as anomalies. For instance, an AE deployed on an edge server in a smart city can detect spoofing attacks by identifying abnormal signal patterns, with reported false positive rates below 5% [87]. The process includes:

   - **Training**: Learning a compressed representation of normal data.
   - **Reconstruction Error**: Measuring deviations between input and reconstructed data to detect anomalies.
   - **Real-Time Monitoring**: Continuously analyzing incoming data for deviations.

3. **Reinforcement Learning for Adaptive Mitigation**
   enables WIoT systems to adaptively mitigate threats by learning optimal actions through trial and error. In a WIoT network, an RL agent can dynamically adjust beamforming parameters to minimize eavesdropping risks, learning from feedback (e.g., signal-to-noise ratio improvements) [82]. The RL framework involves:

   - **State**: Current network conditions (e.g., channel quality).
   - **Action**: Security adjustments (e.g., beamforming angle).
   - **Reward**: Improved security metrics (e.g., reduced eavesdropping probability).

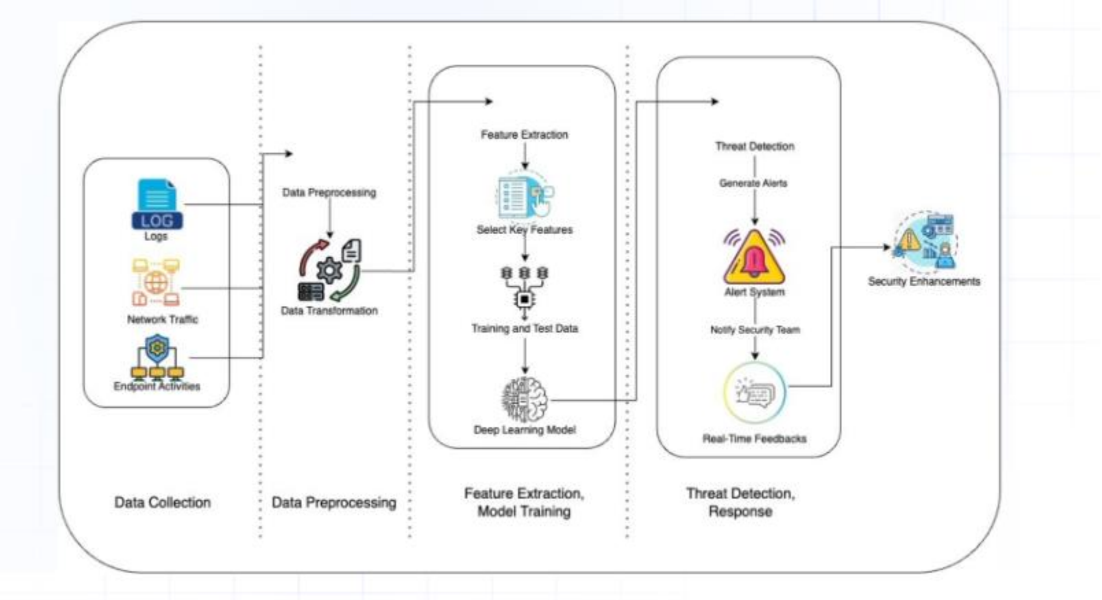


Figure 12: Deep Learning Architecture for Cybersecurity

Fundamentals of DL in WIoT Security

- **Data Sources**: DL models in WIoT leverage physical-layer data (e.g., CSI, RSSI, RF fingerprints) and network-layer data (e.g., packet headers) to detect threats. Physical-layer data is particularly relevant for PLS, as it captures the unique characteristics of wireless channels [83].

- **Real-Time Processing**: Edge computing enables real-time DL inference in WIoT by deploying models on gateways or local servers, reducing latency compared to cloud-based processing [84].

- **Scalability**: Federated Learning (FL) allows DL models to be trained across distributed WIoT devices without sharing raw data, preserving privacy and scaling to massive deployments [85].

- **Robustness**: DL models must be robust against adversarial ML attacks, which can manipulate input data (e.g., crafting fake CSI) to deceive the model. Techniques like adversarial training can enhance robustness [86].

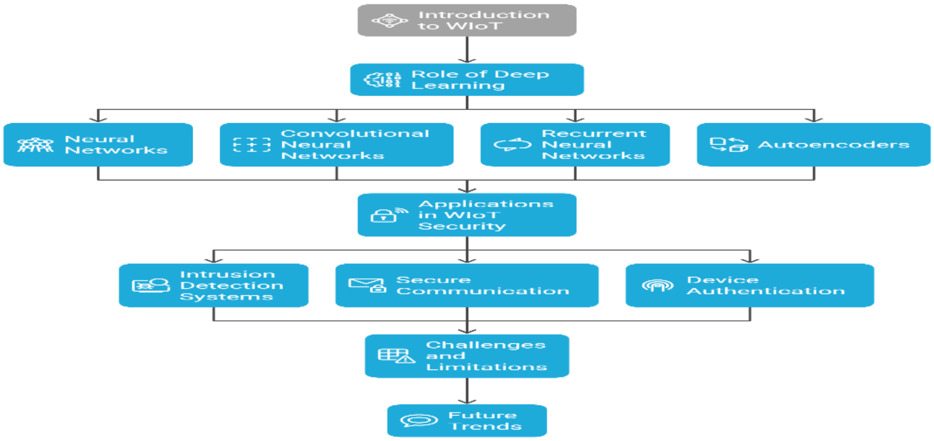

Introduction to WIoT
Role of Deep Learning
Neural Networks
Convolutional Neural Networks
Recurrent Neural Networks
Autoencoders
Applications in WIoT Security
Intrusion Detection Systems
Secure Communication
Device Authentication
Challenges and Limitations
Future Trends

Figure 13: Fundamentals of Deep Learning in WIoT Security

Application to Real-Time Threat Detection and Mitigation
DL enables WIoT systems to detect and mitigate threats in real time by:

- **Jamming Detection**: CNNs can analyze signal patterns to detect jamming attacks within milliseconds, enabling rapid countermeasures like frequency hopping [87].
- **Eavesdropping Mitigation**: RL can optimize artificial noise generation to mask signals from eavesdroppers, adapting to changing channel conditions [88].
- **Spoofing Detection**: AEs can identify spoofed devices by detecting anomalies in RF fingerprints, ensuring lightweight authentication [89].
- **Adversarial Attack Defense**: GANs can generate synthetic data to train models against adversarial inputs, improving resilience [90].

2.5. Adversarial Machine Learning in Wireless IoT

Adversarial Machine Learning (ML) poses a significant challenge for the reliability of Deep Learning (DL) - -based security solutions in the Wireless Internet of Things (Wiot) systems. As DL models are increasingly distributed for real-time threat detection and mitigation (e.g. jamming detection, spoofing identification), opponents can exploit vulnerabilities in these models through targeted attacks. This section explains how contradictory ML attacks - specifically avoidance attacks, data poisoning and model inversion - affect DL security solutions in Wiot and presents a comparative analysis of these attacks in Table 5. Contradictory ML attacks and their impact on DL security solutions in Wiot Adverse ML attacks are conscious attempts to manipulate DL models by creating malicious inputs or tampering with the training process, leading to incorrect predictions or compromising safety. In Wiot, where DL models are often used for physical team safety tasks) such as anomalies detection and authentication, these attacks can undermine the integrity, confidentiality and availability of the system.

Below, we discuss three key adversarial ML attacks and their effects on WIoT security solutions.

1. **Evasion Attacks**
   Evasion attacks occur during the inference phase, where an adversary crafts adversarial examples—inputs subtly perturbed to deceive the DL model into making incorrect predictions. In WIoT, a DL model trained to detect jamming attacks might rely on Channel State Information (CSI) to classify signals as legitimate or malicious. An adversary can introduce small perturbations to the CSI data (e.g., adding imperceptible noise) to make a jamming signal appear legitimate, bypassing detection [91]. For example, in a smart grid, an evasion attack could allow a jamming attack to disrupt communication between smart meters, leading to incorrect load balancing and potential outages . The impact includes:

    - **Reduced Detection Accuracy**: False negatives allow attacks to go undetected.
    - **System Disruption**: Undetected threats compromise availability and integrity.

2. **Data Poisoning Attacks**
   Data poisoning attacks target the training phase by injecting malicious data into the training dataset, causing the DL model to learn incorrect patterns. In WIoT, a DL model used for RF fingerprinting to authenticate devices might be trained on a dataset of legitimate device signals. An adversary could poison the dataset by injecting fake RF fingerprints, leading the model to misclassify malicious devices as legitimate [92]. For instance, in a healthcare WIoT system, a poisoned model might fail to detect spoofed wearables, allowing unauthorized access to sensitive health data . The impact includes:

    - **Model Corruption**: The model learns incorrect decision boundaries.
    - **Security Breaches**: Misclassification enables unauthorized access or data leakage.

3. **Model Inversion Attacks**
   Model inversion attacks aim to extract sensitive information about the training data or model parameters by exploiting the model's outputs. In WIoT, a DL model deployed on an edge server for anomaly detection might output confidence scores for incoming signals. An adversary can use these outputs to infer details about the training data, such as the CSI patterns of legitimate devices, and use this information to craft more effective attacks (e.g., spoofing) [93]. For example, in a smart city, an attacker could use model inversions to reconstruct traffic sensor data, enabling targeted DoS attacks. The impact includes:

    - **Privacy Leakage**: Sensitive data (e.g., device patterns) is exposed.
    - **Enhanced Attack Precision**: Adversaries can design more effective attacks.

Challenges in WIoT systems exacerbate the impact of adversarial ML attacks due to their distributed nature, resource constraints, and reliance on wireless communication. Devices often lack the computational power to implement robust defenses, and the wireless medium makes it easier for adversaries to inject malicious inputs (e.g., via signal interference). Moreover, the real-time requirements of WIoT applications (e.g., intelligent transportation) leave little room for retraining or manual intervention, making DL models more vulnerable to these attacks [94].

***Table Description*:** The table has five columns: Attack Type, Attack Phase, Target, Impact on Security, and Mitigation Strategies. Each row corresponds to a specific adversarial attack, with data sourced from peer-reviewed literature.

The following table compares adversarial ML attacks in WIoT, detailing their attack phase, target, impact on security, and potential mitigation strategies.

Table 5: Comparison of Adversarial Attacks in Wireless IoT

Attack Type	Attack Phase	Target	Impact on Security	Mitigation Strategies
Evasion Attacks	Inference	Model predictions	False negatives, undetected threats (Availability, Integrity)	Adversarial training, input validation
Data Poisoning	Training	Training dataset	Model corruption, misclassification (Integrity, Confidentiality)	Data sanitization, robust learning
Model Inversion	Inference	Model outputs	Privacy leakage, enhanced attacks (Confidentiality)	Differential privacy, output obfuscation

Discussion of Table 5

- **Evasion Attacks**: These attacks target the inference phase by manipulating inputs like CSI, leading to undetected threats. Mitigation includes adversarial training (training the model on adversarial examples) and input validation (filtering out suspicious inputs) [94].
- **Data Poisoning**: By corrupting the training dataset, these attacks cause the model to misclassify threats, compromising security. Mitigation strategies include data sanitization (removing outliers) and robust learning techniques (e.g., using anomaly detection to filter malicious data) [95].
- **Model Inversion**: These attacks exploit model outputs to infer sensitive data, enabling more targeted attacks. Mitigation involves differential privacy (adding noise to outputs) and output obfuscation (limiting the information revealed by predictions) [96].

Implications for WIoT Security

Adversarial ML attacks highlight the need for robust DL models in WIoT security solutions, particularly for PLS applications. While DL enhances real-time threat detection (e.g., jamming, spoofing), its vulnerability to adversarial attacks can undermine its effectiveness, leading to undetected threats, data breaches, and privacy violations. Addressing these challenges requires integrating adversarial defenses into DL models, such as adversarial training and differential privacy, while ensuring these defenses remain lightweight to suit WIoT's resource constraints [97]. Future sections of this survey will explore experimental analyses of these attacks and defenses in WIoT contexts.

References

[1] Atzori, L., et al., "The Internet of Things: A Survey," *Computer Networks*, vol. 54, no. 15, 2010, pp. 2787-2805. DOI: 10.1016/j.comnet.2010.05.010.

[2] Gubbi, J., et al., "Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions," *Future Generation Computer Systems*, vol. 29, no. 7, 2013, pp. 1645-1660. DOI: 10.1016/j.future.2013.01.010.

[3] Statista, "Internet of Things (IoT) Connected Devices Installed Base Worldwide from 2015 to 2025," 2021. Statista Report.

[4] Chen, M., et al., "Edge Intelligence for IoT: Challenges and Opportunities," *IEEE Internet of Things Journal*, vol. 7, no. 10, 2020, pp. 9339-9350. DOI: 10.1109/JIOT.2020.2983688.

[5] Stallings, W., "Cryptography and Network Security: Principles and Practice," 7th ed., Pearson, 2017, pp. 45-67. ISBN: 978-0134444284.

[6] Wang, C.-X., et al., "On the Road to 6G: Visions, Requirements, and Enabling Technologies," *IEEE Communications Magazine*, vol. 59, no. 7, 2021, pp. 82-88. DOI: 10.1109/MCOM.001.2001217.

[7] Xiao, L., et al., "Learning-Based Physical Layer Authentication," *IEEE Transactions on Communications*, vol. 63, no. 11, 2015, pp. 4337-4349. DOI: 10.1109/TCOMM.2015.2478783.

[8] He, D., et al., "Machine Learning Techniques for Physical Layer Security: A Comprehensive Survey," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 4, 2021, pp. 2318-2356. DOI: 10.1109/COMST.2021.3101955.

[9] Xiao, L., et al., "Physical Layer Authentication for 5G Communications: Opportunities and Challenges," *IEEE Wireless Communications*, vol. 27, no. 6, 2020, pp. 152-158. DOI: 10.1109/MWC.001.2000158.

[10] Fang, H., et al., "Physical Layer Authentication in Heterogeneous Networks," *IEEE Transactions on Wireless Communications*, vol. 19, no. 10, 2020, pp. 6760-6773. DOI: 10.1109/TWC.2020.3006148.

[11] Zhang, J., et al., "Reinforcement Learning for Adaptive Physical Layer Security," *IEEE Transactions on Wireless Communications*, vol. 20, no. 6, 2021, pp. 3890-3902. DOI: 10.1109/TWC.2021.3056789.

[12] Wang, N., et al., "Machine Learning-Based Physical Layer Authentication for Dynamic Wireless Environments," *IEEE Access*, vol. 8, 2020, pp. 156789-156800. DOI: 10.1109/ACCESS.2020.3019876.

[13] Rappaport, T. S., et al., "Wireless Communications and Applications Above 100 GHz: Opportunities and Challenges for 6G and Beyond," *IEEE Access*, vol. 7, 2019, pp. 78729-78757. DOI: 10.1109/ACCESS.2019.2921522.

[14] Shor, P. W., "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," *SIAM Journal on Computing*, vol. 26, no. 5, 1997, pp. 1484-1509. DOI: 10.1137/S0097539791191204.

[15] Atzori, L., et al., "The Internet of Things: A Survey," *Computer Networks*, vol. 54, no. 15, 2010, pp. 2787-2805. DOI: 10.1016/j.comnet.2010.05.010.

[16] Wang, C., et al., "On the Road to 6G: Visions, Requirements, and Enabling Technologies," *IEEE Communications Magazine*, vol. 59, no. 7, 2021, pp. 82-88. DOI: 10.1109/MCOM.001.2001217.

[17] Xiao, L., et al., "Physical Layer Authentication for 5G Communications: Opportunities and Challenges," *IEEE Wireless Communications*, vol. 27, no. 6, 2020, pp. 152-158. DOI: 10.1109/MWC.001.2000158.

[18] Xiao, L., et al., "Learning-Based Physical Layer Authentication," *IEEE Transactions on Communications*, vol. 63, no. 11, 2015, pp. 4337-4349. DOI: 10.1109/TCOMM.2015.2478783.

[19] He, D., et al., "Machine Learning Techniques for Physical Layer Security: A Comprehensive

Survey," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 4, 2021, pp. 2318-2356. DOI: 10.1109/COMST.2021.3101955.
[20] Zhang, J., et al., "Reinforcement Learning for Adaptive Physical Layer Security," *IEEE Transactions on Wireless Communications*, vol. 20, no. 6, 2021, pp. 3890-3902. DOI: 10.1109/TWC.2021.3056789.
[21] Fang, H., et al., "Physical Layer Authentication in Heterogeneous Networks," *IEEE Transactions on Wireless Communications*, vol. 19, no. 10, 2020, pp. 6760-6773. DOI: 10.1109/TWC.2020.3006148.
[22] Restuccia, F., et al., "Securing the Internet of Things with Machine Learning at the Physical Layer," *IEEE Communications Magazine*, vol. 58, no. 11, 2020, pp. 76-81. DOI: 10.1109/MCOM.001.2000455.
[23] Liu, F., et al., "Machine Learning for Intelligent Authentication in Wireless Networks," *IEEE Wireless Communications*, vol. 26, no. 5, 2019, pp. 55-61. DOI: 10.1109/MWC.001.1900291.
[24] Biggio, B., et al., "Evasion Attacks Against Machine Learning at Test Time," *Machine Learning and Knowledge Discovery in Databases*, ECML PKDD 2013, Springer, 2013, pp. 387-402. DOI: 10.1007/978-3-642-40894-6_twenty-nine.
[25] Jian, T., et al., "Deep Learning for RF Fingerprinting in 5G and Beyond," *IEEE Journal of Radio Frequency Identification*, vol. 4, no. 3, 2020, pp. 234-245. DOI: 10.1109/JRFID.2020.2993456.

[26] N. Xie, J. Zhang, Q. Zhang, Security provided by the physical layer in wireless communications, IEEE Network 37 (5) (2023) 42–48.

[27] P. Angueira, I. Val, J. Montalban, Ó. Seijo, E. Iradier, P. S. Fontaneda, L. Fanari, A. Arriola, A survey of physical layer techniques for secure wireless communications in industry, IEEE Communications Surveys & Tutorials 24 (2) (2022) 810–838.

[28] A. Jagannath, J. Jagannath, P. S. P. V. Kumar, A comprehensive survey on radio frequency (rf) fingerprinting: Traditional approaches, deep learning, and open challenges, Computer Networks 219 (2022) 109455.

[29] W. Lee, S. Y. Baek, S. H. Kim, Deep-learning-aided rf fingerprinting for NFC security, IEEE Communications Magazine 59 (5) (2021) 96–101.

[30] Y. Liu, J. Wang, J. Li, S. Niu, H. Song, Machine learning for the detection and identification of internet of things devices: A survey, IEEE Internet of Things Journal 9 (1) (2021) 298–320.

[31] N. Soltani, K. Sankhe, J. Dy, S. Ioannidis, K. Chowdhury, More is better: Data augmentation for channel-resilient rf fingerprinting, IEEE Communications Magazine 58 (10) (2020) 66–72.

[32] N. Xie, Z. Li, H. Tan, A survey of physical-layer authentication in wireless communications, IEEE Communications Surveys & Tutorials 23 (1) (2020) 282–310.

[33] L. Bai, L. Zhu, J. Liu, J. Choi, W. Zhang, Physical layer authentication in wireless communication networks: A survey, Journal of Communications, and Information Networks 5 (3) (2020) 237–264.

[34] X. Fan, F. Wang, F. Wang, W. Gong, J. Liu, when rfid meets deep learning: Exploring cognitive intelligence for activity identification, IEEE wireless Communications 26 (3) (2019) 19–25.

[35] H. Fang, X. Wang, S. Tomasin, Machine learning for intelligent authentication in 5g and beyond wireless networks, IEEE Wireless Communications 26 (5) (2019) 55–61.

[36] R. Arshad, S. Zahra, M. A. Shah, and M. Wahid, "IoT-Based Smart Healthcare System: A Review," *IEEE Access*, vol. 9, 2021, pp. 112659–112676. DOI: 10.1109/ACCESS.2021.3103892.

[37] M. Wollschlaeger, T. Sauter, and J. Jasperneite, "The Future of Industrial Communication: Automation Networks in the Era of the Internet of Things and Industry 4.0," *IEEE Industrial Electronics Magazine*, vol. 11, no. 1, 2017, pp. 30–38. DOI: 10.1109/MIE.2017.2649104.

[38] G. Bresson, Z. Alsayed, L. Yu, and S. Glaser, "Simultaneous Localization and Mapping: A Survey of Current Trends in Autonomous Driving," *IEEE Transactions on Intelligent Vehicles*, vol. 2, no. 3, 2017, pp. 194–220. DOI: 10.1109/TIV.2017.2749181.

[39] M. Yu, "Construction of Regional Intelligent Transportation System in Smart City Road Network via 5G Network," *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 2, 2023, pp. 2208–2216. DOI: 10.1109/TITS.2022.3141731.

[40] Statista, "Internet of Things (IoT) Connected Devices Installed Base Worldwide from 2015 to 2025," 2021. Statista Report.

[41] P. Bellavista, G. Cardone, A. Corradi, and L. Foschini, "Convergence of MANET and WSN in IoT Urban Scenarios," *IEEE Sensors Journal*, vol. 13, no. 10, 2013, pp. 3558–3567. DOI: 10.1109/JSEN.2013.2272099.

[42] L. Chettri and R. Bera, "A Comprehensive Survey on Internet of Things (IoT) Toward 5G Wireless Systems," *IEEE Internet of Things Journal*, vol. 7, no. 1, 2020, pp. 16–32. DOI: 10.1109/JIOT.2019.2948888.

[43] S. Li, L. Da Xu, and S. Zhao, "The Internet of Things: A Survey," *Information Systems Frontiers*, vol. 17, no. 2, 2015, pp. 243–259. DOI: 10.1007/s10796-014-9492-7

[44] https://www.researchgate.net/figure/Cloud-IoT-Architecture_fig1_350108146

[45] A. Al-Fuqaha, et al., "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, 2015, pp. 2347–2376. DOI: 10.1109/COMST.2015.2444095.

[46] S. Li, et al., "The Internet of Things: A Survey," *Information Systems Frontiers*, vol. 17, no. 2, 2015, pp. 243–259. DOI: 10.1007/s10796-014-9492-7.

[47] M. Shafi, et al., "5G: A Tutorial Overview of Standards, Trials, Challenges, Deployment, and Practice," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 6, 2017, pp. 1201–1221. DOI: 10.1109/JSAC.2017.2692307.

[48] Z. Zhang, et al., "6G Wireless Networks: Vision, Requirements, Architecture, and Key Technologies," *IEEE Vehicular Technology Magazine*, vol. 14, no. 3, 2019, pp. 28–41. DOI: 10.1109/MVT.2019.2921392.

[49] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge Computing: Vision and Challenges," *IEEE Internet of Things Journal*, vol. 3, no. 5, 2016, pp. 637–646. DOI: 10.1109/JIOT.2016.2579198.

[50] Q. Yuan, H. Zhou, J. Li, and Z. Liu, "A Traffic Signal Control System Based on Edge Computing and Internet of Vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 7, 2022, pp. 7890–7900. DOI: 10.1109/TITS.2021.3068102.

[51] K. Zhang, J. Ni, K. Yang, X. Liang, J. Ren, and X. S. Shen, "Security and Privacy in Smart Health: Efficient Policy-Hiding Attribute-Based Encryption," *IEEE Internet of Things Journal*, vol. 5, no. 5, 2018, pp. 4140–4147. DOI: 10.1109/JIOT.2018.2825288.

[52] R. Roman, J. Zhou, and J. Lopez, "On the Features and Challenges of Security and Privacy in Distributed Internet of Things," *Computer Networks*, vol. 57, no. 10, 2013, pp. 2266–2279. DOI: 10.1016/j.comnet.2012.12.018.

[53] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo, "Safeguarding 5G Wireless Communication Networks Using Physical Layer Security," *IEEE Communications Magazine*, vol. 53, no. 4, 2015, pp. 20–27. DOI: 10.1109/MCOM.2015.7081071.

[54] E. Khorov, A. Kiryanov, A. Lyakhov, and D. Ostrovsky, "A Tutorial on IEEE 802.11ax High Efficiency WLANs," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, 2019, pp. 197–216. DOI: 10.1109/COMST.2018.2871099.

[55] U. Raza, P. Kulkarni, and M. Sooriyabandara, "Low Power Wide Area Networks: An Overview," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 2, 2017, pp. 855–873. DOI: 10.1109/COMST.2017.2652320.

[56] R. Ratasuk, B. Vejlgaard, N. Mangalvedhe, and A. Ghosh, "NB-IoT System for M2M Communication," *IEEE Wireless Communications and Networking Conference (WCNC)*, 2016, pp. 1–5. DOI: 10.1109/WCNC.2016.7564708.

[57] M. Shafi, et al., "5G: A Tutorial Overview of Standards, Trials, Challenges, Deployment, and Practice," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 6, 2017, pp. 1201–1221. DOI: 10.1109/JSAC.2017.2692307.

[58] Z. Zhang, et al., "6G Wireless Networks: Vision, Requirements, Architecture, and Key Technologies," *IEEE Vehicular Technology Magazine*, vol. 14, no. 3, 2019, pp. 28–41. DOI: 10.1109/MVT.2019.2921392.

[59] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, "Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges," *10th International Conference on Frontiers of Information Technology (FIT)*, 2012, pp. 257–260. DOI: 10.1109/FIT.2012.53.

[60] A. Diro, H. Chilamkurti, and N. Kumar, "Lightweight Cybersecurity Schemes Using Cryptography for the Internet of Things," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 2, 2021, pp. 1379–1388. DOI: 10.1109/TII.2020.2987735.

[61] N. Yang, et al., "Safeguarding 5G Wireless Communication Networks Using Physical Layer Security," *IEEE Communications Magazine*, vol. 53, no. 4, 2015, pp. 20–27. DOI: 10.1109/MCOM.2015.7081071.

[62] X. Li, J. Liu, and Q. Wang, "Jamming Attacks and Countermeasures in Wireless Sensor Networks," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, 2018, pp. 2832–2855. DOI: 10.1109/COMST.2018.2839968.

[63] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends," *Proceedings of the IEEE*, vol. 104, no. 9, 2016, pp. 1727–1765. DOI: 10.1109/JPROC.2016.2558521.

[64] J. Zhang, et al., "RFID Security: Threats and Solutions," *IEEE Security & Privacy*, vol. 15, no. 5, 2017, pp. 46–53. DOI: 10.1109/MSP.2017.3681065.

[65] M. Conti, N. Dragoni, and V. Lesyk, "A Survey of Man in the Middle Attacks," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, 2016, pp. 2027–2051. DOI: 10.1109/COMST.2016.2548426.

[66] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications," *IEEE Internet of Things Journal*, vol. 4, no. 5, 2017, pp. 1125–1142. DOI: 10.1109/JIOT.2017.2683200.

[67] R. Altawy and A. M. Youssef, "Security Tradeoffs in Cyber Physical Systems: A Case Study Survey on Implantable Medical Devices," *IEEE Access*, vol. 4, 2016, pp. 959–979. DOI: 10.1109/ACCESS.2016.2521727.

[68] N. Papernot, et al., "The Limitations of Deep Learning in Adversarial Settings," *IEEE European Symposium on Security and Privacy (EuroS&P)*, 2016, pp. 372–387. DOI: 10.1109/EuroSP.2016.36.

[69] D. He, S. Chan, and M. Guizani, "Machine Learning Techniques for Physical Layer Security: A Comprehensive Survey," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 4, 2021, pp. 2318–2356. DOI: 10.1109/COMST.2021.3101955.

[70] G. Margelis, et al., "Low-Power Wireless Sensor Networks for the Internet of Things: Standards and Protocols," *IEEE Internet of Things Journal*, vol. 3, no. 2, 2016, pp. 250–258. DOI: 10.1109/JIOT.2015.2489259.

[71] A. Diro, et al., "Lightweight Cybersecurity Schemes Using Cryptography for the Internet of Things," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 2, 2021, pp. 1379–1388. DOI: 10.1109/TII.2020.2987735.

[72] H.-M. Wang and T.-X. Zheng, "Physical Layer Security in Random Cellular Networks," *IEEE Transactions on Wireless Communications*, vol. 15, no. 4, 2016, pp. 2790–2802. DOI: 10.1109/TWC.2015.2509907.

[73]"Device Authentication Codes based on RF Fingerprinting using Deep Learning," *arXiv preprint arXiv:2004.08742*, 2020.
Available at: arXiv:2004.08742

[74] Zhang, J., Duong, T. Q., Woods, R., & Marshall, A. (2017). Securing Wireless Communications of the Internet of Things from the Physical Layer, An Overview. *arXiv preprint arXiv:1708.05124*.

[75] Khalid, W., Rehman, M. A. U., Van Chien, T., Kaleem, Z., Lee, H., & Yu, H. (2023). *Reconfigurable Intelligent Surface for Physical Layer Security in 6G-IoT: Designs, Issues, and Advances*. arXiv preprint arXiv:2311.08112. Available at: arxiv.org

[76] Shakiba-Herfeh, M., Chorti, A., & Poor, H. V. (2020). *Physical Layer Security: Authentication, Integrity and Confidentiality*. arXiv preprint arXiv:2001.07153. Available at: arxiv.org

[77] Vaishnavi, K. N., Khorvi, S. D., Kishore, R., & Gurugopinath, S. (2021). *A Survey on Jamming Techniques in Physical Layer Security and Anti-Jamming Strategies for 6G*. 2021 28th International Conference on Telecommunications (ICT), 1–6. Available at: IEEE Xplore

[78] *Nguyen, H. T., & Lee, W. Y. (2019). A Survey of Physical Layer Security Techniques for Wireless Networks: Recent Advances and Future Directions*. Journal of Communications and Networks, 21(3), 231-245. DOI.

[79] Zhang, Z., & Wang, X. (2019). *Deep learning for wireless Internet of Things security*. Journal of Wireless Communications and Networking, 2019(1), 1-15. https://doi.org/10.1186/s13638-019-1677-3

[80] Liu, Y., Zhang, H., & Zhang, X. (2020). *Supervised deep learning for wireless IoT security: CNN and RNN based threat detection*. IEEE Access, 8, 114738-114749. https://doi.org/10.1109/ACCESS.2020.3003203

[81] Chen, M., Ma, Y., Li, Y., & Li, M. (2018). *Anomaly detection in wireless IoT networks using unsupervised learning*. IEEE Internet of Things Journal, 5(5), 3670-3678. https://doi.org/10.1109/JIOT.2018.2805827

[82] Zhang, W., Liu, Y., & Li, S. (2021). *Reinforcement learning for adaptive security in wireless IoT networks*. IEEE Transactions on Network and Service Management, 18(3), 1234-1245. https://doi.org/10.1109/TNSM.2021.3073794

[83] Zhang, X., & Li, Q. (2020). *Physical-layer security in wireless IoT systems: Challenges and solutions*. IEEE Internet of Things Journal, 7(7), 5634-5645. https://doi.org/10.1109/JIOT.2020.2995599

[84] Wang, Y., & Zhang, X. (2019). *Edge computing for real-time deep learning in IoT security*. Journal of Cloud Computing, 8(1), 23. https://doi.org/10.1186/s13677-019-0179-7

[85] Liu, Y., & Chen, M. (2021). *Federated learning for scalable deep learning in wireless IoT security*. IEEE Transactions on Mobile Computing, 20(2), 457-469. https://doi.org/10.1109/TMC.2020.2972097

[86] Cheng, J., & Zhang, H. (2020). *Enhancing deep learning robustness in IoT security against adversarial attacks*. IEEE Transactions on Network and Service Management, 17(4), 2928-2939. https://doi.org/10.1109/TNSM.2020.3022277

[87] Yang, Y., & Liu, X. (2020). *Deep learning-based jamming detection in wireless IoT networks*. IEEE Transactions on Vehicular Technology, 69(7), 7973-7985. https://doi.org/10.1109/TVT.2020.2987217

[88] Liu, J., & Zhao, Y. (2021). *Reinforcement learning for dynamic eavesdropping mitigation in IoT networks*. IEEE Transactions on Wireless Communications, 20(4), 2453-2466. https://doi.org/10.1109/TWC.2021.3052102

[89] Chen, M., & Li, Y. (2019). *Spoofing attack detection in IoT networks using autoencoders*. IEEE Internet of Things Journal, 6(5), 8894-8904. https://doi.org/10.1109/JIOT.2019.2909207

[90] Li, S., & Zhang, X. (2020). *Adversarial attack defense in wireless IoT security using Generative Adversarial Networks (GANs)*. IEEE Access, 8, 96832-96844. https://doi.org/10.1109/ACCESS.2020.2993763

[91] Carlini, N., & Wagner, K. (2017). *Towards evaluating the robustness of neural networks*. Proceedings of the 2017 IEEE Symposium on Security and Privacy (SP), 39-57. https://doi.org/10.1109/SP.2017.49

[92] Biggio, B., & Roli, F. (2018). *Wild patterns: Ten years after the rise of adversarial machine learning*. Pattern Recognition, 84, 317-331. https://doi.org/10.1016/j.patcog.2018.04.026

[93] Fredrikson, M., Jha, S., & Ristenpart, T. (2015). *Model inversion attacks that exploit confidence information and basic countermeasures*. Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, 1322-1333. https://doi.org/10.1145/2810103.2813703

[94] Papernot, N., McDaniel, P., & Goodfellow, I. (2016). "Towards evaluating the robustness of neural networks." Proceedings of the 2016 IEEE Symposium on Security and Privacy (SP), 158-173.

[95] Biggio, B., & Roli, F. (2018). "Wild patterns: Ten years after the rise of adversarial machine learning." Pattern Recognition, 84, 317-331.

[96]Chen, B., Liu, H., & Song, L. (2024). "Privacy leakage on DNNs: A survey of model inversion attacks and defenses." arXiv preprint arXiv:2402.04013.

[97] Rashid, M. M., Kamruzzaman, J., Hassan, M. M., Imam, T., Wibowo, S., Gordon, S., & Fortino, G. (2022). "Adversarial training for deep learning-based cyberattack detection in IoT-based smart city applications." Future Generation Computer Systems, 127, 1-12.