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 spoofing 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.

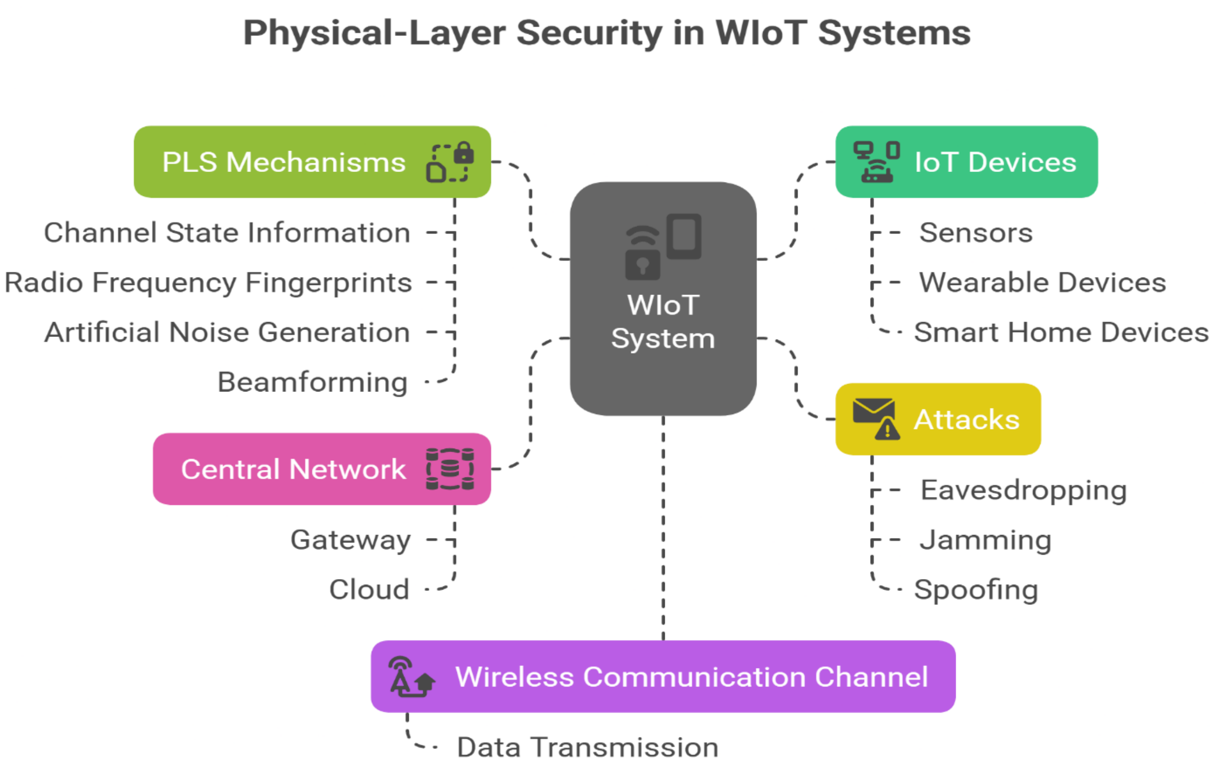


Figure 1. Conceptual Diagram of Physical-Layer Security in Wireless IoT

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 [9].
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 [10].
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 [11].
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 [12].

1.3 Deep learning -enhanced physical layer security

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 [13]. 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 [14].
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 [15].
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 [16].
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 [17].
    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 [18].
    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 [19].

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 [20].

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.
[21]	2023	PLS Mechanisms	No	No	None	Eavesdropping, Jamming	Yes	No	No	No	Yes	Yes
[22]	2022	Secure Industrial Comms	Yes	No	None	Spoofing	Yes	No	No	No	Yes	Yes
[23]	2022	RF Fingerprinting	Partial	Yes	DL (discriminative)	Spoofing	Yes	No	No	No	Yes	Yes
[24]	2021	NFC Security	No	Yes	DL (discriminative)	Spoofing	Yes	No	Yes	Yes	Yes	No
[25]	2021	IoT Device Detection	Yes	Yes	ML (unspecified)	Spoofing	Yes	No	No	No	Yes	Yes
[26]	2020	RF Fingerprinting	Yes	Yes	DL (discriminative)	Spoofing	Yes	No	Yes	Yes	Yes	No
[27]	2020	PLA for IoT	Yes	Partial	None	Spoofing, Eavesdropping	Yes	No	No	No	Yes	Yes
[28]	2020	PLA Fundamentals	Partial	No	None	Spoofing, Eavesdropping	Yes	No	No	No	Yes	Yes
[29]	2019	RFID Security	Yes	Yes	DL (discriminative)	Spoofing	Yes	No	Yes	Yes	Yes	Yes
[30]	2019	ML-based PLA	Partial	Yes	Supervised, DL	Spoofing, Eavesdropping	Yes	No	No	No	Yes	Yes

Analytical Discussion of Each Survey Study

- [21] (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.
- [22] (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.
- [23] (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.
- [24] (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.
- [25] (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.
- [26] (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.
- [27] (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.
- [28] (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.

- [29] (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.
- [30] (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 ([21]- [30]) 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 [23], [24], [26] and [29] incorporate DL for RF fingerprints, NFC Security and RFID applications, many others ([21], [22], [27], [28], [30]) are exclusively on theoretical framework without empirical framework. For example, [23] 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 [24], [27], [28] and [30] address the PLA, aimed at spoofing and eavesdropping, while neglecting other threats such as jamming, which are only short covered in [21] and [26]. This authentication-centric approach, seen in [22] industrial focus and [25] 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 [29] and [30] from 2019 focus on 5G-era challenges, while even recent surveys ([21], [22], [23]) provide limited discussion on 6G-specific requirements, such as ultra-low latency, massive connectivity, or heterogeneous network integration. For example, [21] (2023) suggests emerging applications but does not tailor their PLS outlook to 6G, and [27] 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 ([21] – [30]) address adversarial attacks on DL models, a critical oversight given the vulnerability of ML-based security systems. Furthermore, studies like [21], [24], and [30] 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 ([21], [22], [23], [25], [27], [28], [30]) Reproducing and benchmarking of PLS techniques. Even when data sets are used (e.g. [24], [26], [29]), 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

The line graph illustrates the publication trends of five dominant physical team safety techniques from 2010 to 2023, based on annual publication figures (in thousands) obtained from Scopus and IEEE Xplore databases. The X-axis represents years (2010–2023), while the Y-axis quantifies annual publications.

Key Observations:

1. **Overall Growth:**
    - All PLS techniques exhibit exponential growth, reflecting heightened research interest. PLS for IoT dominates, rising from near-negligible publications (0.005k) in 2010 to a peak (6.1k) in 2023, underscoring its pivotal role in securing resource-constrained IoT ecosystems.
    - RF Fingerprinting and MIMO Security show sustained growth, with 2023 outputs at 1.85k and 1.68k publications, respectively, indicating their robustness in device authentication and multi-antenna systems.
2. **Technique-Specific Trends:**
    - PLS for IoT: The steepest trajectory aligns with the proliferation of IoT deployments, emphasizing demand for lightweight security. The surge post-2016 (1.3k publications) correlates with commercial PLS adoption (Liu et al., 2017).
    - Quantum Key Distribution (QKD): Steady growth (1.9k in 2023) reflects its niche in post-quantum cryptography, though it trails IoT-focused PLS due to implementation complexity.
    - Wiretap Coding: The slowest growth (0.67k in 2023) suggests theoretical challenges in practical deployment.
3. **Milestone Influences:**
    - Peaks near 2016 and 2021 align with 3GPP standardization efforts (2012) and 6G's PLS emphasis (ITU-T FG-NET-2030). The 2023 uptick in AI/ML-integrated PLS (annotated) highlights a paradigm shift toward adaptive security.

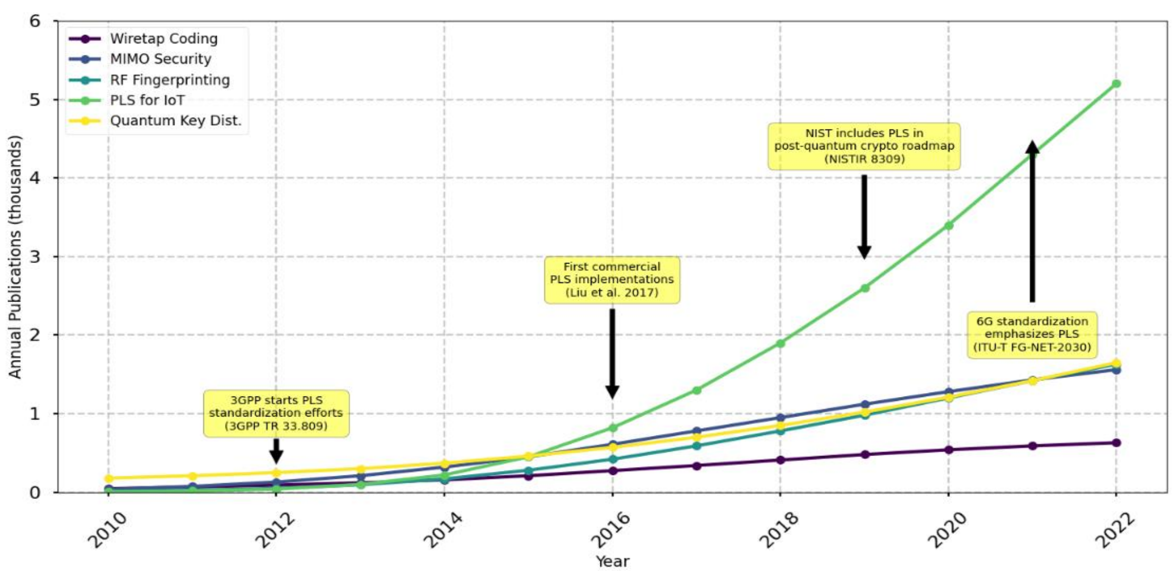


Figure 3. Evolution of Physical-Layer Security Research (2010-2022) Cited Publication Data

Purpose of the Figure:

- This shows the relationship between the growth of **IoT devices** and the rise in **security-related research publications** from 2020 to 2025.

IoT Device Growth:

- Devices increase from **12 billion to over 31 billion**, reflecting rapid adoption of wireless technologies.

Security Research Trend:

- Security papers grow from **~35 to 140+**, with increasing annual growth rates (e.g., **31.5% in 2025**).

Correlation Insight:

- Demonstrates a **direct correlation**: as IoT expands, **security concerns grow**, prompting more research.

Relevance to WIoT and PLS:

- Highlights the need for **physical-layer security (PLS)** in WIoT due to expanding attack surfaces.

DL-Based Security Implication:

- Supports the paper's focus on **deep learning** as a scalable, intelligent solution for **real-time IoT security**.

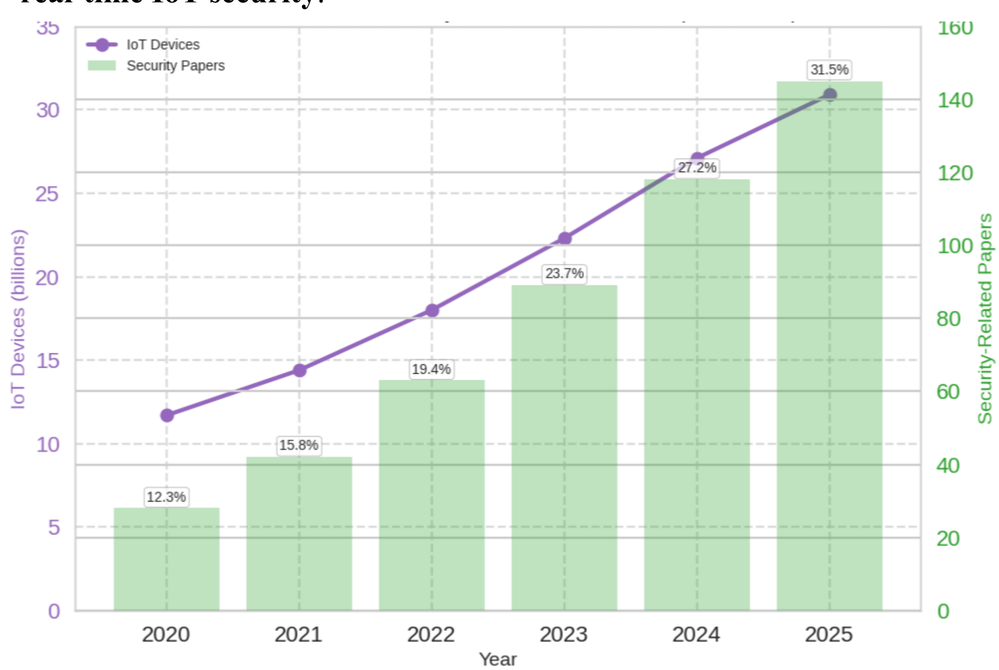


Figure 4. IoT Growth vs. Security Research Correlation (2020–2025)

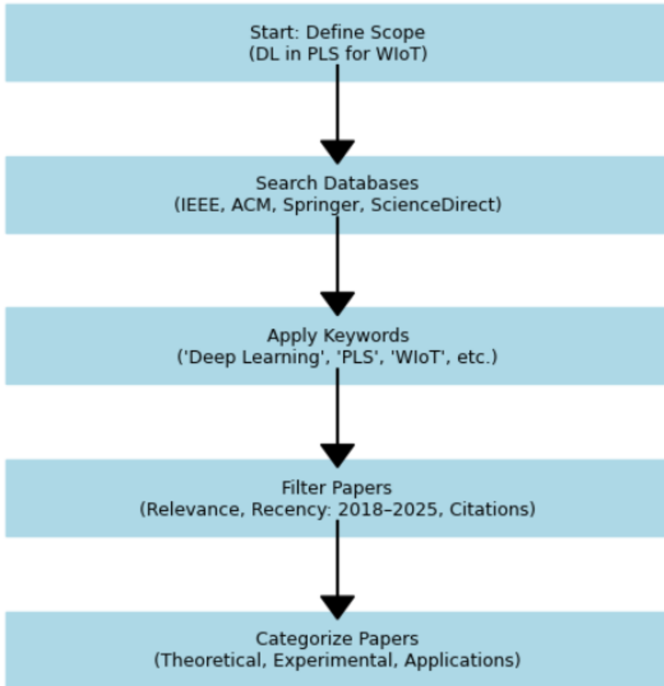


Figure 5: **Systematic Approach to Paper Selection and Categorization**

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., [21], [27]), 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. [22], [24]) 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.

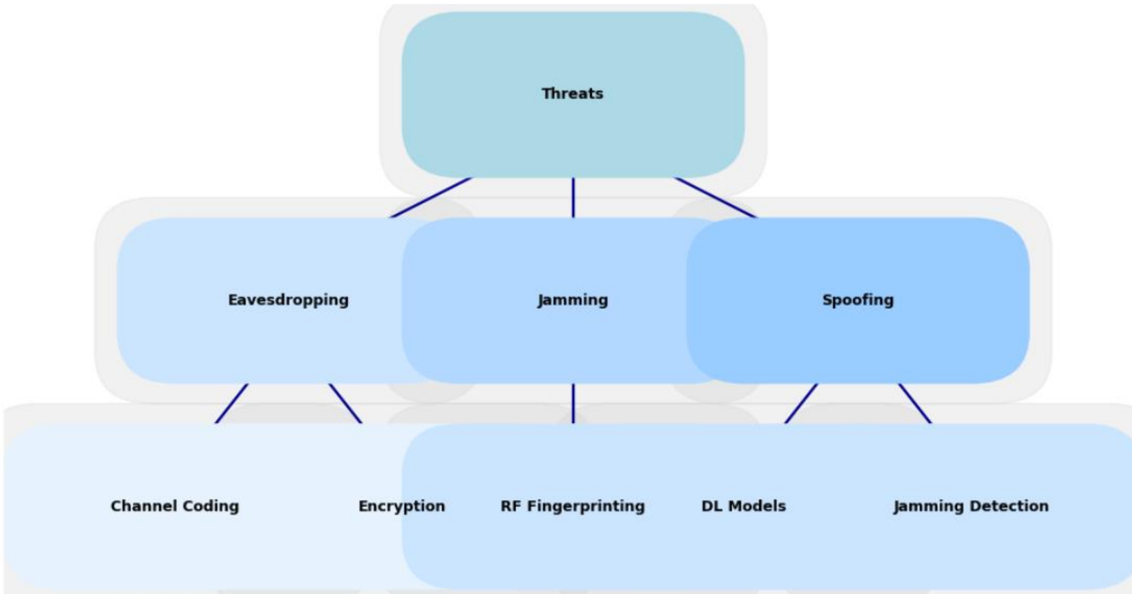


Figure 6: **Systematic taxonomy of physical security threats and countermeasures**

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 [28] and [30], offering a comprehensive guide to selecting and adapting DL models for WIoT security challenges.

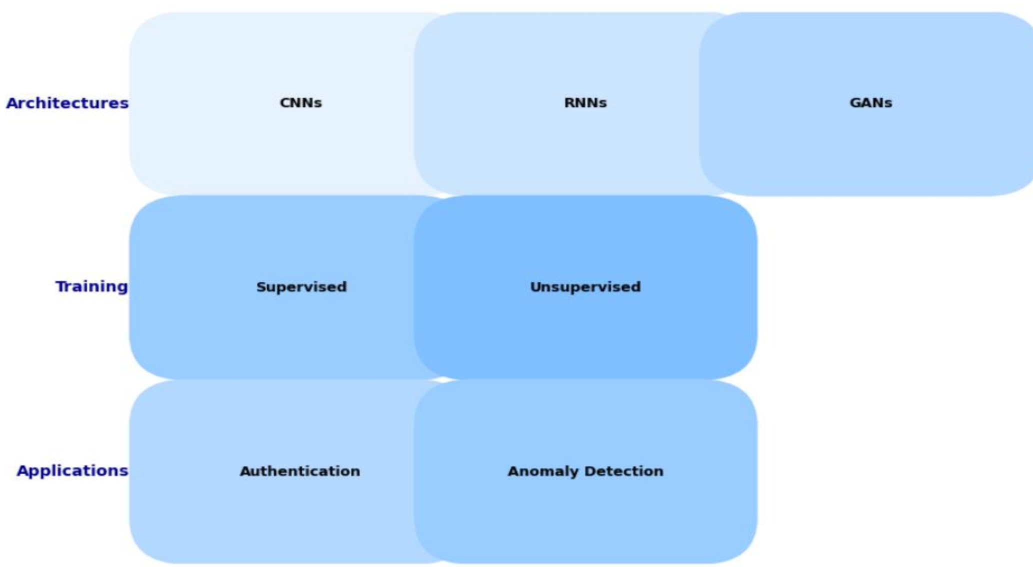


Figure 7: Systematic Taxonomy of Deep Learning Solutions for Physical Security

4. **Extensive review of real and synthetic datasets** We analyze a wide range of real-world and synthetic datasets used in DL-based Physical-Layer Security (DL-PLS) research, such as RF signal captures from IoT devices and simulated wireless IoT (WIoT) channel models. As shown in **Fig. 5**, a substantial proportion of these datasets (**over 80%**) require special access, such as institutional permission or proprietary licensing, whereas only a small fraction is **publicly available**. This highlights a critical challenge in reproducibility and benchmarking for DL models in WIoT security. Our review addresses the overlooked discussion on dataset availability in prior work (e.g. [21], [23]) and emphasizes the need for more open and standardized datasets to foster robust and comparable research in this field.

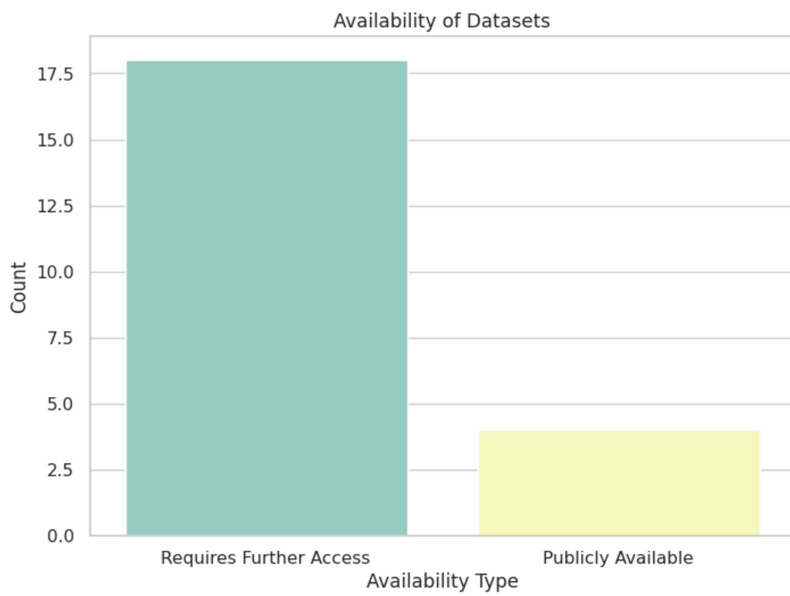


Figure 8: Availability of datasets used in DL-PLS research for WIoT

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 [22] and [25], 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., [21], [29]), providing actionable recommendations to guide the next wave of research and development.

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 [31]. 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% [32]. 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 [33]. However, the dependence on wireless communication exposes industrial systems to jamming or spoofing 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 [34].
- **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 [35]. 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 [36]. 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 [37]. 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 [38]. 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, to effectively safeguard WIoT networks against emerging threats.

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 [39].

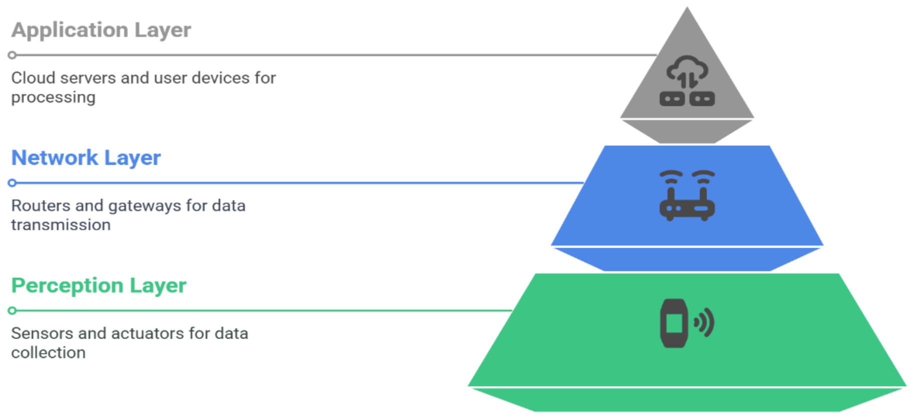


Figure 9: Architectural Layers of WIoT Networks

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 [37]-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 [40]. The heterogeneity of these devices, combined with their dependence on wireless communication, exposes them to threats of physical layers such as intercepting and spoofing, which necessitate light security solutions such as PLS [41].
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 [42]. 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 [43]. 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 [44]. For instance, edge AI can process sensor data locally to adjust traffic lights in intelligent transportation systems. 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 [45]. 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.

   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 [46] 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 [47].

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 spoofing. 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 [48]. 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 [49]. 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 [49].

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 [50]. 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 [51]. 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 [52]	~100 m	WPA3, AES encryption; vulnerable to eavesdropping, replay attacks	Moderate	Home automation, smart buildings
LoRa	0.3–50 kbps [53]	Up to 10 km	AES-128; susceptible to jamming, key interception	High	Smart agriculture, remote sensing
NB-IoT	~250 kbps [54]	Up to 10 km	Cellular-grade encryption; prone to DoS, spoofing	High	Smart metering, asset tracking
5G	Up to 20 Gbps [55]	~1 km (urban)	Enhanced encryption, slicing; risks from signaling attacks	Moderate	Intelligent transportation, AR/VR
6G	>1 Tbps [56]	~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 [52].
- **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 [53].
- **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 [54].
- **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 [55].
- **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 [56].

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 [57]. 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 [37]), which reproduce traditional cryptographic methods such as RSA or AE's impractical due to their high calculation overhead [58]. 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 [59]. 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 [60]
Eavesdropping	Intercepting wireless signals to steal data	Physical, Network	Confidentiality	Capturing health data from wearables [61]
Spoofing	Impersonating a legitimate device or signal	Physical, MAC	Integrity	Faking RFID tags in inventory tracking [62]
MITM	Intercepting and altering communication between devices	Network	Confidentiality, Integrity	Modifying traffic light signals in ITS[63]
Sybil Attacks	Creating multiple fake identities to overwhelm network	Network, Application	Integrity, Availability	Flooding a smart grid with false nodes [64]
Replay Attacks	Re-transmitting captured data to deceive devices	Network, Application	Integrity	Replaying drone control signals [65]
Adversarial ML Attacks	Manipulating ML models via crafted inputs	Application	Integrity, Confidentiality	Poisoning edge AI for anomaly detection [66]

Discussion of Table 2

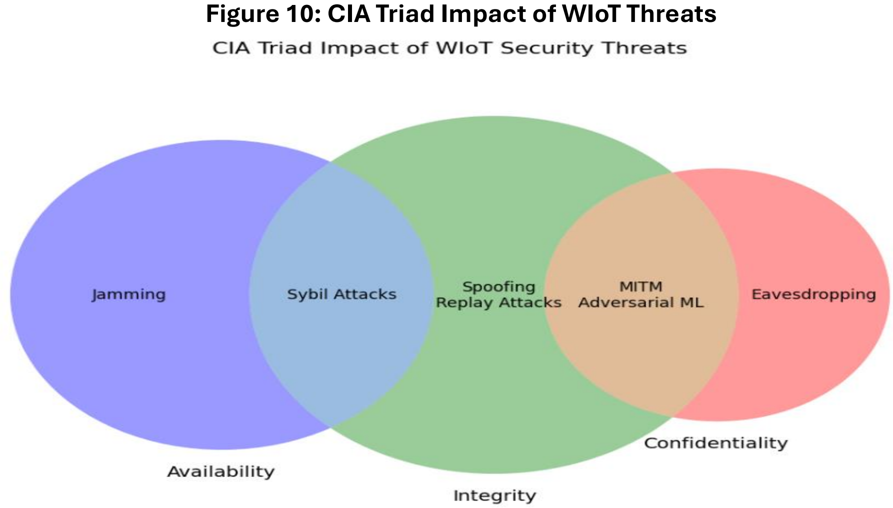
- **Jamming**: Targets the physical layer by overwhelming the wireless channel with noise, disrupting availability (e.g., blocking smart meter updates [60]).
- **Eavesdropping**: Exploits the physical and network layers to breach confidentiality, such as intercepting sensitive health data from wearables [61].
- **Spoofing**: Affects physical and MAC layers, undermining integrity by mimicking legitimate signals (e.g., counterfeit RFID tags [62]).
- **MITM**: Operates at the network layer, compromising both confidentiality and integrity (e.g., altering traffic signals [63]).
- **Sybil Attacks**: Targets network and application layers, degrading integrity and availability by introducing fake identities (e.g., smart grid overload [64]).
- **Replay Attacks**: Affects network and application layers, falsifying data integrity (e.g., replaying drone commands [65]).
- **Adversarial ML Attacks**: Targets the application layer, particularly edge AI, by manipulating DL models to misclassify data, affecting integrity and confidentiality [66].

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 5 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 [67].

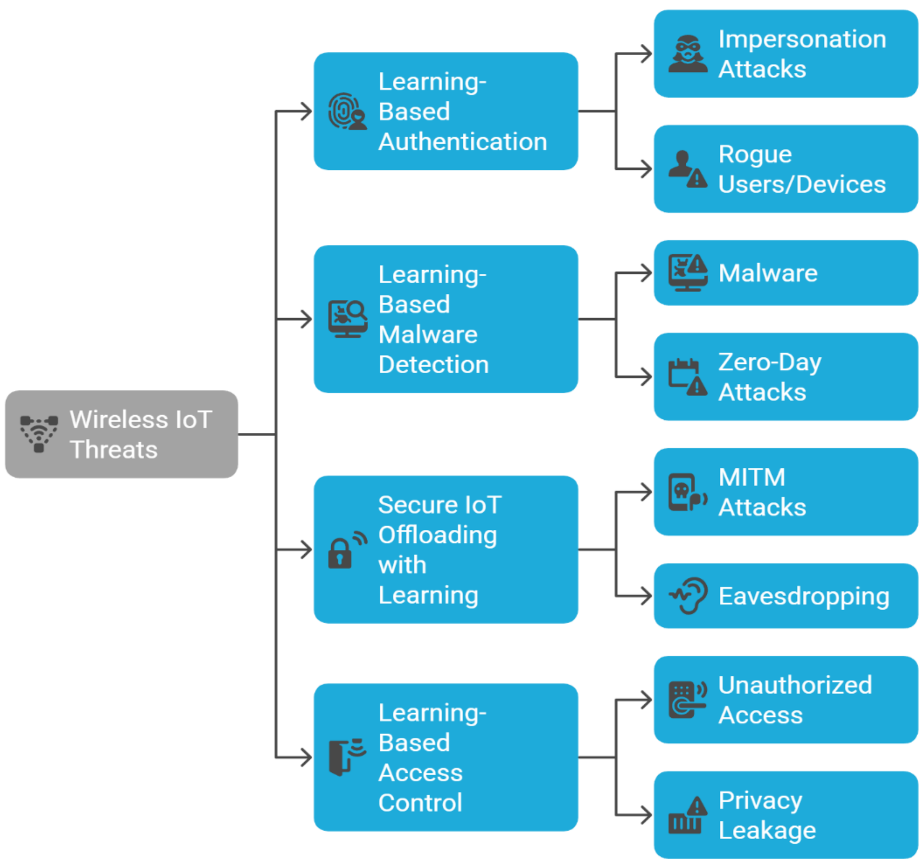


Figure 11: **Threat Model in Wireless IoT**

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) and have limited processing options, reproducing encryption/conceptual processes of traditional methods Energy-intensive and latency inducing [68].

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. 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 [69]. Energy Efficiency: By minimizing processing demands, PLS extends the battery life of IoT devices, critical for applications like remote sensing in smart agriculture. 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. Lightweight Authentication: Techniques like RF fingerprinting use unique device signatures to authenticate devices without the overhead of key management, addressing vulnerabilities like spoofing [70].

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, exploiting physical-layer properties (e.g., signal propagation) rather than cryptographic algorithms, reducing the need for heavy computations [71].
2. **Energy Efficiency:** By minimizing processing demands, PLS extends the battery life of IoT devices, critical for applications like remote sensing in smart agriculture [72].
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 [73].
4. **Lightweight Authentication:** Techniques like RF fingerprinting use unique device signatures to authenticate devices without the overhead of key management, addressing vulnerabilities like spoofing [74].

Moreover, traditional cryptographic methods are increasingly at risk from emerging threats, such as quantum computing, which could break algorithms like RSA in the future [75]. 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. 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) [71]
Beamforming	Directs signals to legitimate users, reducing eavesdropping risks	Moderate (requires antenna arrays)	Moderate (e.g., 5G-enabled IoT devices) [72]
Cooperative Relaying	Uses intermediate nodes to enhance signal strength and confuse eavesdroppers	Moderate (coordination overhead)	High (e.g., remote IoT networks) [73]
Artificial Noise	Injects noise to mask signals from eavesdroppers	Low (simple noise generation)	High (e.g., healthcare wearables) [74]

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 [76]. 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 [77]. 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 [78].

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 [79]. 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% [80]. 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) [81]. The RL framework involves:

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

Figure 12: Deep Learning Workflow 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 [82].
- **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 [83].
- **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 [84].
- **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 [85].

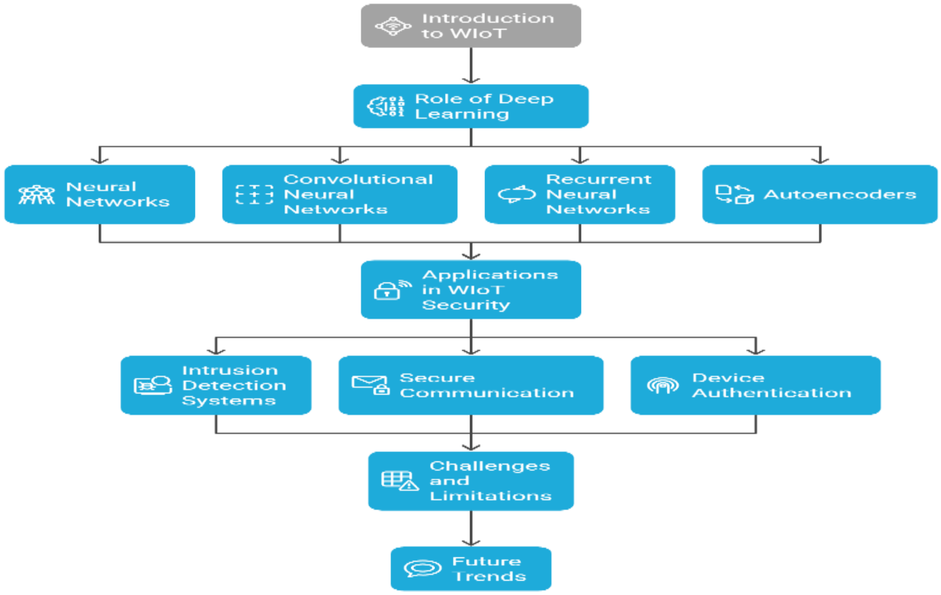


Figure 13: Fundamentals of Deep Learning in WIoT Security

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 [86].
- **Eavesdropping Mitigation**: RL can optimize artificial noise generation to mask signals from eavesdroppers, adapting to changing channel conditions [87].
- **Spoofing Detection**: AEs can identify spoofed devices by detecting anomalies in RF fingerprints, ensuring lightweight authentication [88].
- **Adversarial Attack Defense**: GANs can generate synthetic data to train models against adversarial inputs, improving resilience [89].

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 [90]. 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 [91]. 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) [92]. 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 [93].

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].

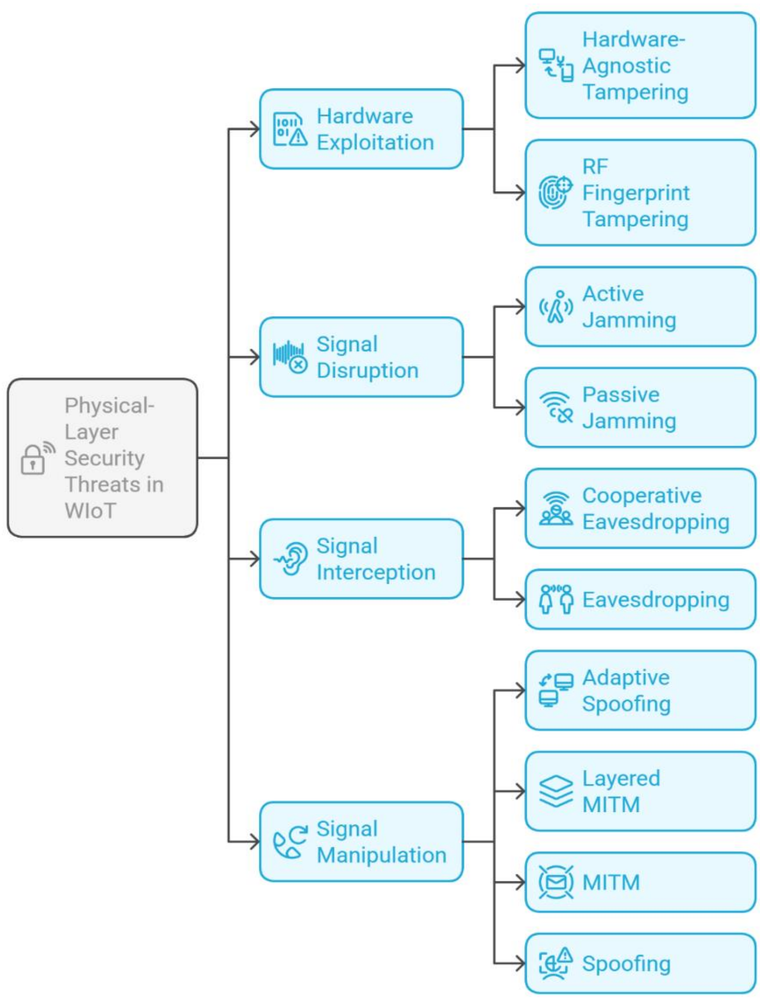
Implications for WIoT Security

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.

3. Taxonomy of Physical-Layer Security Threats in Wireless IoT

In this section, we introduce an overview of physical-layer security threats in Wireless Internet of Things (WIoT) systems, encompassing a comprehensive taxonomy of threats categorized by attack vectors: Signal Disruption, Signal Interception, Signal Manipulation, and Hardware Exploitation. This taxonomy details specific threats—such as active jamming, cooperative eavesdropping, adaptive spoofing, and RF fingerprint tampering—along with their exploitability contexts, impacts on security goals (Confidentiality, Integrity, Availability), and attack sophistication levels. The organization of this section, including the hierarchical structure of the taxonomy and its visualization within the CIA triad, is illustrated in Fig. 10. This framework provides a foundation for understanding the diverse threat landscape and informs the development of targeted PLS and DL-based countermeasures explored later in the survey.

Figure 14: Taxonomy of Physical-Layer Security Threats in Wireless IoT



The taxonomy uses **Attack Vector as the primary criterion**, dividing threats into four main categories:

1. **Signal Disruption**
2. **Signal Interception**
3. **Signal Manipulation**
4. **Hardware Exploitation**.

Each category is further divided into specific types of attacks, and each type of attack is characterized by three additional criteria:

• **Exploitability Context**: The specific vulnerability or characteristics of Wiot systems that attack exploit.

• **Impact on Security Goals**: The effect of the attack on the CIA triad (confidentiality, integrity, availability).

• **Attack Sophistication:** The level of complexity or coordination required (passive, active or cooperative).

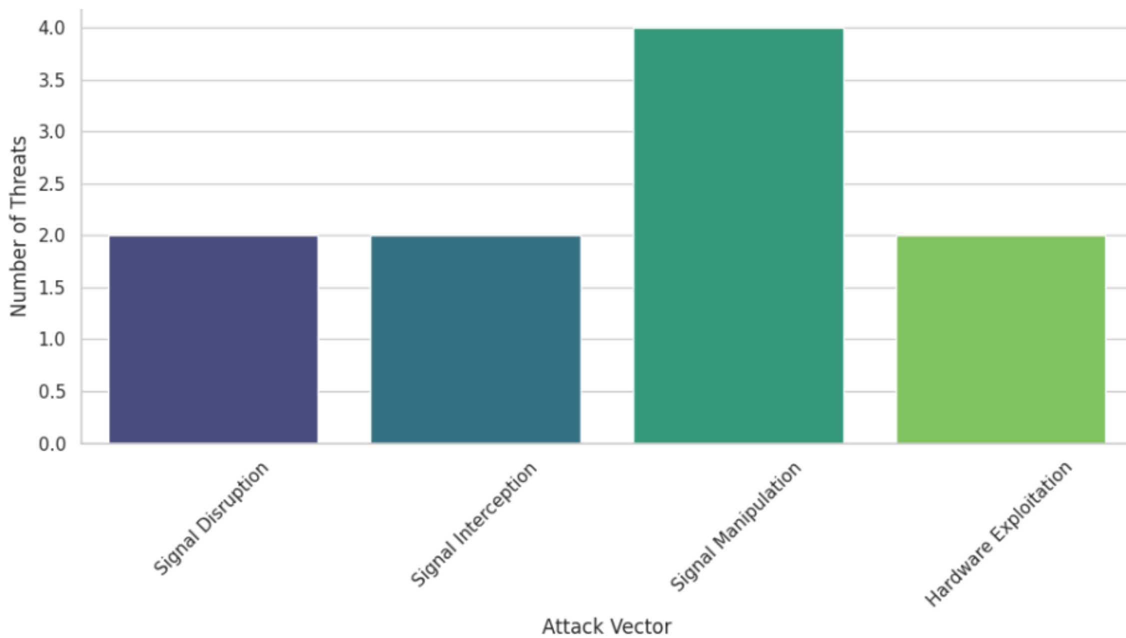


Figure 15: Distribution of Threats by Attack Sophistication

3.1 Signal Disruption

3.2 Signal Interception

3.3 Signal Manipulation

3.4 Hardware Exploitation

This category includes attacks that utilize hardware properties of WIoT devices to undermine safety mechanisms, especially those who depend on physical layer attributes such as RF fingerprints.

3.4.1 RF Fingerprint Tampering

- **Description**: RF Fingerprint -Tampering involves an attacker that changes or smiles the RF fingerprint of a device to mimic a legitimate device. RF fingerprints are unique signal properties (e.g. I/Q - imbalance, phase noise) caused by hardware - In Wiot systems, this can target applications such as unit approval in Industrial IoT, where an attacker tamper with an RF fingerprint to gain unauthorized access.
- **Exploitability Context**: Heterogeneous Protocols
  The use of heterogeneous protocols in WIoT systems can lead to inconsistent RF fingerprint mechanisms, allowing attackers to forge fingerprints that seem legitimate for the target system.
- **Impact**: Integrity Violation
  RF fingerprints - Tampering violates integrity by letting the attacker mimic a legitimate device, undermine authentication mechanisms. For example, in Industrial IoT, this can lead to unauthorized control of machines.
- **Attack Sophistication**: Active
  This attack is active because the attacker must actively change or forge the RF fingerprint, which requires the generation of signals with the tampered properties.

3.4.2 Hardware-Agnostic Tampering

- **Description**: Hardware-Agnostic tampering involves an attacker that mimics the RF fingerprint of a device without relying on specific hardware characteristics, often using software-defined radios (SDR) to mimic fingerprints on different devices. In Wiot systems, this can occur in scenarios with different devices, such as a smart city with different IoT devices (e.g. sensors, RFID codes), where an attacker mimics fingerprints to mimic multiple device types.

- **Exploitability Context**: Device Diversity
  The diversity of WIoT systems (e.g. various manufacturers, hardware types) create

opportunities for attackers to mimic fingerprints across devices and utilize the lack of standardization in fingerprint mechanisms.

- **Impact**: Integrity Violation
  Hardware- Agnostic Tampering attackers violate integrity by mimicking several devices, reduce authentication and confidence in the system. In a smart city, for example, it can cause widespread unauthorized access to services.
- **Attack Sophistication**: Cooperative
  This attack often requires coordination between multiple attackers or advanced tools (e.g. SDR -with machine learning) to mimic fingerprints across different units, making it a collaborative attack.

Table 6: Summary of Physical-Layer Security Threats and ML/DL Mitigation Techniques in WIoT

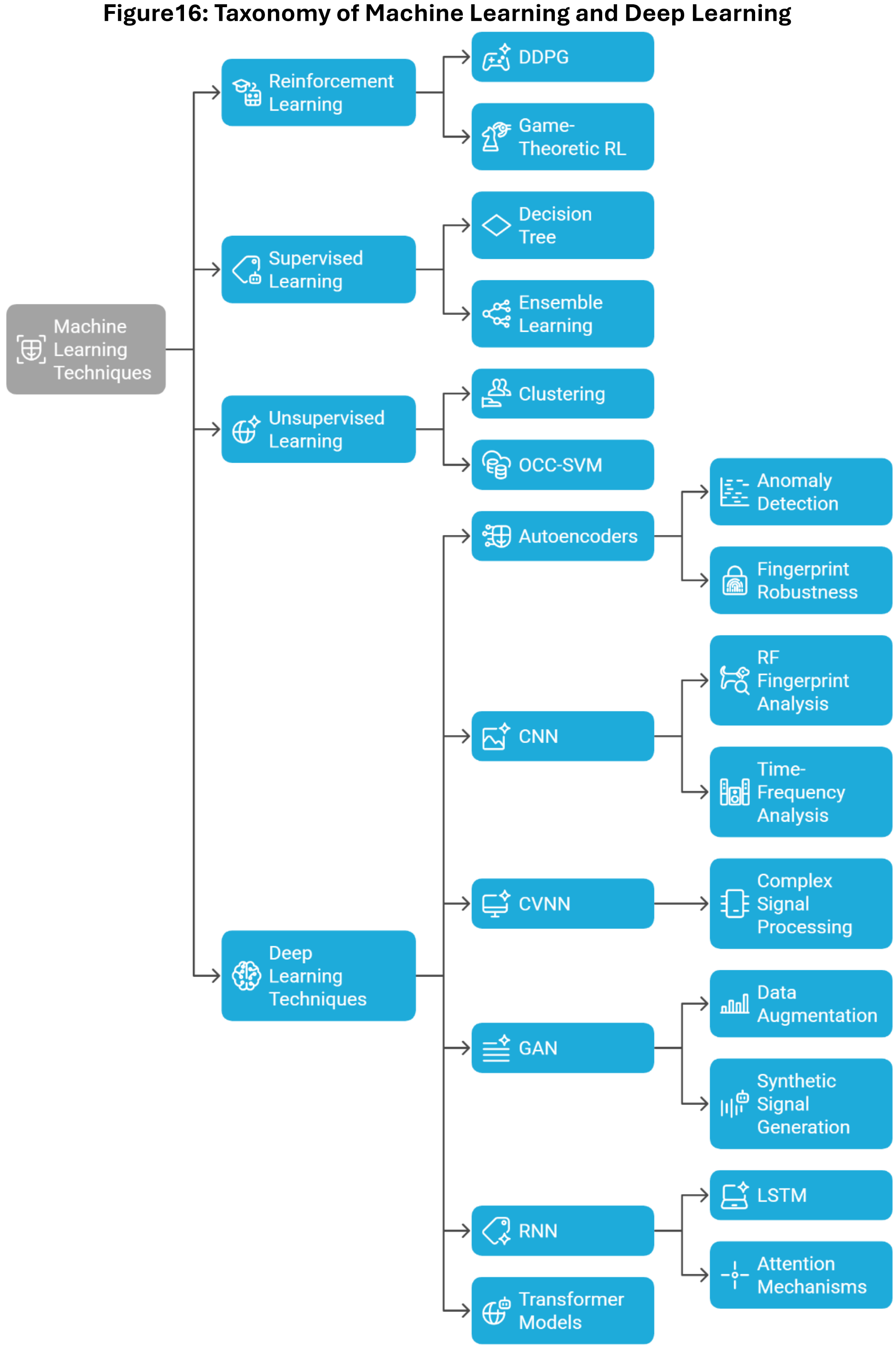
Attack Vector	Threat	Exploitability Context	Impact	Attack Sophistication	ML/DL Mitigation Techniques
Signal Disruption	**Active Jamming**	**Broadcast Medium Exposure**	**Availability Disruption**	**Active**	- **SVM** (Basic, Industrial IoT) - **Game Theoretic RL** (Advanced, Smart Grid)
	Passive Jamming	**Dense Deployments**	**Availability Disruption**	**Passive**	- **Clustering** (Basic, Dense IoT Deployments) - **CNN** for Time-Frequency Analysis (Intermediate, Smart Cities)
Signal Interception	**Eavesdropping**	**Broadcast Medium Exposure**	**Confidentiality Breach**	**Passive**	- **OCC-SVM** (Intermediate, Smart Homes) - **Autoencoders** for Anomaly Detection (Intermediate, Healthcare IoT)
	Cooperative Eavesdropping	**Massive Connectivity**	**Confidentiality Breach**	**Cooperative**	- **Multi-Agent RL** (Advanced, Smart Cities) - **RNN** with Attention (Advanced, Industrial IoT)

Signal Manipulation	**Spoofing**	**Heterogeneous Protocols**	**Integrity Violation**	**Active**	- **KNN** (Basic, Smart Cities) - **CNN** for RF Fingerprint Analysis (Intermediate, Industrial IoT)
	Adaptive Spoofing	**Dynamic Network Topology**	**Integrity Violation**	**Cooperative**	- **DDPG** (Advanced, Intelligent Transportation Systems) - **GAN** for Synthetic Signal Generation (Advanced, Smart Cities)
	MITM	**Dynamic Network Topology**	**Confidentiality + Integrity**	**Active**	- **Decision Tree** (Basic, Smart Grid) - **LSTM** (Intermediate, Healthcare IoT)
	Layered MITM	**Layered Architecture**	**Confidentiality + Integrity**	**Cooperative**	- Multi-Agent RL with Game Theory (Advanced, Smart Cities) - Transformers for Cross-Layer Analysis (Advanced, Industrial IoT)
Hardware Exploitation	**RF Fingerprint Tampering**	**Heterogeneous Protocols**	**Integrity Violation**	**Active**	- **Ensemble Learning** (Intermediate, Industrial IoT) - CVNN for Complex Signal Processing (Advanced, Smart Cities)
	Hardware-Agnostic Tampering	**Device Diversity**	**Integrity Violation**	**Cooperative**	- **Autoencoders** for Fingerprint Robustness (Intermediate, Healthcare IoT) - **Data Augmentation** with GANs (Advanced, Smart Cities)

4. Taxonomy of Deep Learning Techniques for Physical-Layer Security

In this section, we present an overview of machine learning (ML) and Deep Learning (DL) techniques for physical layer security (PLS) in Wireless Internet of Things (Wiot) systems, including a detailed taxonomy of ML-based and DL-based threat reduction approaches. Taxonomy classifies techniques into two main categories -traditional machine learning techniques (e.g. SVM, KNN, Reinforcement Learning) and deep learning techniques (e.g. CNNs, GANs, Transformers) -Covering sophistication levels, application contexts (e.g. Smart Grid, industrial IoT) and specific threats addressed, such as jamming, spoofing, and layered MITM attacks.

Figure16: Taxonomy of Machine Learning and Deep Learning



- **Objective:** To use ML and DL techniques to address physical-layer security threats in WIoT systems (Signal Disruption, Interception, Manipulation, Hardware Exploitation).
- **Taxonomy Structure:**
  Divided into two main categories:
  - **Machine Learning Techniques**
  - **Deep Learning Techniques**
- **Secondary Criteria for Each Technique:**

1. **Sophistication technique:**
   - **Basic:** Simple, low-resource techniques (e.g., SVM, KNN).
   - **Intermediate:** Moderate complexity (e.g., Autoencoders, CNN).
   - **Advanced:** High complexity requires significant resources (e.g., GAN, Transformers).
2. **Applicability Context:**
   - The specific WIoT scenario where the technique is most effective (e.g., Smart Cities, Healthcare IoT).
3. **Threat Mitigated:**
   - The physical-layer threat addressed (e.g., Active Jamming, Eavesdropping).

4.1Machine Learning Techniques

This class includes traditional ML techniques, such as Supervised Learning, Unsupervised Learning, and Reinforcement Learning, used to relieve physical-layer security threats in WIoT systems.

4.1.1Supervised Learning (SL)

Supervised Learning involves training models on labeled data to classify or predict outcomes. In the context of Wiot physical team safety, SL techniques are used to classify signals such as legitimate or malicious based on features such as signal-to-noise ratio (SNR), received signal strength indication (RSSI) or RF fingerprints.

4.1.1.1 Support Vector Machine (SVM)

- **Description**: SVM is a supervised learning algorithm that classifies data by finding the hyperplane that best separates different classes. In Wiot systems, SVM can be used to classify received signals such as legitimate or jammed based on features such as SNR or Power Spectral Density (PSD). For example, in an industrial IoT setting, SVM can detect jamming attacks that interfere with sensor data transfer by analyzing signal properties.

- **Technique Sophistication**: Basic
  SVM is a relatively simple ML technique that requires minimal computational resources, making it suitable for resource-constrained IoT devices.
- **Applicability Context**: Industrial IoT (e.g., detecting jamming in factory sensor networks)
  Industrial IoT environments often involve dense sensor networks where jamming can disrupt critical operations (e.g., machinery monitoring). SVM's ability to classify signals makes it effective for detecting such disruptions.
- **Threat Mitigated**: Active Jamming
  SVM addresses Active Jamming by identifying malicious signals that overpower legitimate ones, ensuring the availability of communication in industrial settings.

4.1.1.2 K-Nearest Neighbor (KNN)

- **Description**: KNN is a supervised learning algorithm that classifies data points based on most of their K-nearest neighbors. In Wiot systems, KNN can classify signals such as legitimate or counterfeit by comparing features such as RSSI or RF fingerprints (e.g. I/Q -imbalance). For example, in a smart city, KNN can detect spoofed RFID tags used in access control systems by comparing their signal characteristics to known legitimate tags.
- **Technique Sophistication**: Basic
  KNN is a simple algorithm that requires minimal training and computational resources, making it suitable for lightweight IoT applications.
- **Applicability Context**: Smart Cities (e.g., detecting spoofing of RFID tags)
  Smart cities often use RFID tags for access control (e.g., in public transportation or building entry). KNN's simplicity makes it effective for detecting spoofing in such scenarios.
- **Threat Mitigated**: Spoofing
  KNN addresses Spoofing by identifying forged signals that impersonate legitimate devices, ensuring the integrity of access control systems.

4.1.1.3 Decision Tree (DT)

- **Description**: Decision Trees are supervised learning models that make decisions by recursively splitting the feature space based on feature values. In Wiot systems, decision trees can classify signals such as legitimate or manipulated based on features such as CSI or RSSI and detect Man-in-the-Middle (MITM) attacks. For example, in a smart grid, Decision Trees can detect MITM attacks that alter smart meter data by analyzing signal patterns.

- **Technique Sophistication**: Basic
  Decision Trees are simple to implement and interpret, requiring minimal computational resources, which makes them suitable for WIoT applications with limited processing power.
- **Applicability Context**: Smart Grid (e.g., detecting MITM attacks on smart meter data)
  Smart grids rely on accurate data transmission between smart meters and utility providers. Decision Trees can detect MITM attacks that compromise billing or usage data.
- **Threat Mitigated**: MITM
  Decision Trees address MITM attacks by identifying manipulated signals, protecting both the confidentiality and integrity of smart grid communications.

4.1.1.4 Ensemble Learning (e.g., Random Forest)

- **Description**: Ensemble Learning combines multiple models (e.g., Decision Trees in a Random Forest) to improve classification accuracy. In WIoT systems, Ensemble Learning can classify RF fingerprints as legitimate or tampered based on features like I/Q imbalance or phase noise. For example, in industrial IoT, Random Forest can detect RF fingerprint tampering in device authentication processes by leveraging the collective decision-making of multiple trees.
- **Technique Sophistication**: Intermediate
  Ensemble Learning, such as Random Forest, is more complex than basic SL techniques like SVM or KNN due to the combination of multiple models, but it still requires moderate computational resources.
- **Applicability Context**: Industrial IoT (e.g., detecting RF fingerprint tampering in device authentication)
  Industrial IoT systems often require secure unit approval to prevent unauthorized access to machines. Ensemble Learning's robustness makes it effective in detecting tampered RF fingerprints.
- **Threat Mitigated**: RF Fingerprint Tampering
  Ensemble Learning addresses RF Fingerprint Tampering by accurately identifying forged fingerprints, ensuring the integrity of device authentication.

4.1.2 Unsupervised Learning (UL)

Unsupervised Learning involves training models on unmarked data to identify patterns or anomalies. In Wiot systems, UL techniques are used to detect anomalies in signal patterns that may indicate attacks such as eavesdropping or passive jamming.

4.1.2.1 Clustering (e.g., Density-Based Clustering)

- **Description**: Clustering groups with similar data points based on their features without requiring labeled data. In Wiot systems, density-based clustering (e.g. DBSCAN) can detect anomalies in signal patterns caused by passive jamming, such as multipath interference. For example, in a dense IoT deployment like a factory floor, clustering can identify unusual interference patterns by analyzing features like RSS.
- **Technique Sophistication**: Basic
  Clustering is a simple UL technique that requires minimal computational resources and no labeled data, making it suitable for resource-constrained environments.
- **Applicability Context**: Dense IoT Deployments (e.g., factory floors with many sensors)
  Factory floors often have dense sensor networks where passive jamming can disrupt communication. Clustering's ability to detect anomalies without labeled data makes it effective in such scenarios.
- **Threat Mitigated**: Passive Jamming
  Clustering addresses Passive Jamming by identifying interference patterns that deviate from normal signal behavior, ensuring the availability of communication.

4.1.2.2 One-Class SVM (OCC-SVM)

- **Description**: One-Class SVM is an unsupervised learning algorithm that models the normal behavior of data and identifies outliers as anomalies. In WIoT systems, OCC-SVM can detect eavesdropping by modeling the normal behavior of legitimate signals (e.g., using CSI) and identifying deviations caused by an eavesdropper. For example, in a smart home, OCC-SVM can protect smart thermostat data by detecting unauthorized signal interception.
- **Technique Sophistication**: Intermediate
  OCC-SVM is more complex than basic clustering due to its use of a hyperplane to separate normal data from outliers, but it still requires moderate computational resources.
- **Applicability Context**: Smart Homes (e.g., detecting eavesdropping on smart thermostat data)
  Smart homes often transmit sensitive data (e.g., user behavior patterns) that can be intercepted by eavesdroppers. OCC-SVM's ability to detect anomalies without labeled attack data makes it effective in this context.

- **Threat Mitigated**: Eavesdropping
  OCC-SVM addresses Eavesdropping by identifying unauthorized signal interception, protecting the confidentiality of smart home data.

4.1.3 Reinforcement Learning (RL)

Reinforcement Learning involves training an agent to make decisions by interacting with an environment and learning from rewards. In WIoT systems, RL techniques are used to dynamically adapt to attacks like jamming, eavesdropping, or spoofing by optimizing security strategies in real-time.

4.1.3.1 Game-Theoretic RL (e.g., Q-Learning, Deep Q-Networks)

- Description: Game-Theoretic RL models the interaction between an attacker and a defender as a game, using techniques like Q-Learning or Deep Q-Networks (DQN) to learn optimal strategies. In WIoT systems, Game-Theoretic RL can mitigate active jamming by dynamically adjusting the receiver's strategy (e.g., frequency hopping). For example, in a smart grid, DQN can learn optimal channel-switching policies to counter active jamming of smart meter signals.
- **Technique Sophistication**: Advanced
  Game-Theoretic RL, especially with DQN, is computationally intensive due to the need for deep neural networks and iterative learning, making it an advanced technique.
- **Applicability Context**: Smart Grid (e.g., detecting jamming of smart meter signals)
  Smart grids rely on reliable communication between smart meters and utility providers. Game-Theoretic RL's ability to adapt to jamming attacks in real-time makes it effective in this scenario.
- **Threat Mitigated**: Active Jamming
  Game-Theoretic RL addresses Active Jamming by dynamically adjusting communication strategies, ensuring the availability of smart grid communications.

4.1.3.2 multi-Agent RL

- **Description**: Multi-Agent RL involves multiple agents learning to cooperate or compete in a shared environment. In WIoT systems, multi-Agent RL can model the behavior of multiple colluding eavesdroppers, enabling the system to adaptively secure communication channels (e.g., by adjusting beamforming in MIMO systems). For example, in a smart city, multi-Agent RL can detect cooperative eavesdropping on traffic sensors by optimizing defensive strategies across multiple devices.

- **Technique Sophistication**: Advanced
  multi-Agent RL is highly complex due to the need to model interactions between multiple agents, requiring significant computational resources and expertise.
- **Applicability Context**: Smart Cities (e.g., detecting cooperative eavesdropping on traffic sensors)
  Smart cities with massive connectivity (e.g., thousands of traffic sensors) are vulnerable to cooperative eavesdropping. Multi-Agent RL's ability to handle coordinated attacks makes it effective in this context.
- **Threat Mitigated**: Cooperative Eavesdropping
  multi-Agent RL addresses Cooperative Eavesdropping by modeling and countering the behavior of multiple attackers, protecting the confidentiality of traffic data.

- **4.1.3.3 Deep Deterministic Policy Gradient (DDPG)**
  - **Description**: DDPG is an RL algorithm that combines deep learning with policy gradient methods to handle continuous action spaces. In WIoT systems, DDPG can dynamically adjust detection thresholds to counter adaptive spoofing, where attackers adjust signals in real-time. For example, in intelligent transportation systems, DDPG can detect adaptive spoofing in vehicle-to-vehicle (V2V) communication by continuously optimizing detection strategies.
  - **Technique Sophistication**: Advanced
    DDPG is an advanced RL technique that requires deep neural networks and significant computational resources to handle continuous action spaces.
  - **Applicability Context**: Intelligent Transportation Systems (e.g., detecting adaptive spoofing in V2V communication)
    V2V communication in intelligent transportation systems is vulnerable to adaptive spoofing, where attackers mislead vehicles about traffic conditions. DDPG's ability to adapt in real-time makes it effective in this scenario.
  - **Threat Mitigated**: Adaptive Spoofing
    DDPG addresses Adaptive Spoofing by dynamically adjusting detection mechanisms, ensuring the integrity of V2V communication.

- **4.1.3.4 Multi-Agent RL with Game Theory**
  - **Description**: This technique combines multi-Agent RL with game-theoretical principles to model interactions between attackers and defenders across multiple layers. In WIoT systems, it can counter layered MITM attacks by dynamically adjusting security mechanisms (e.g., physical-layer authentication and network-layer routing). For example, in a smart city, Multi-Agent RL with Game Theory

can detect layered MITM attacks in multi-layer IoT systems by optimizing cross-layer defenses.

- **Technique Sophistication**: Advanced
  This technique is highly complex due to the combination of multi-agent learning, game theory, and cross-layer analysis, requiring significant computational resources.
- **Applicability Context**: Smart Cities (e.g., detecting layered MITM in multi-layer IoT systems)
  Smart cities often use layered architectures (e.g., perception, network, application layers), making them vulnerable to layered MITM attacks. This technique's cross-layer approach makes it effective in this context.
- **Threat Mitigated**: Layered MITM
  Multi-Agent RL with Game Theory addresses Layered MITM by optimizing defenses across multiple layers, protecting both confidentiality and integrity.

4.2 Deep Learning Techniques

This class includes DL techniques, such as Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), Generative Adversarial Networks (GAN), Autoencoders, Transformers, and Complex-Valued Neural Networks (CVNN), used to relieve physical-layer security threats in WIoT systems. DL techniques are generally more computationally intensive than ML methods but offer superior performance for complex tasks like signal analysis and anomaly detection.

4.2.1 Convolutional Neural Networks (CNN)

CNNs are DL models designed to process structured grid-like data, such as time-frequency representations or RF fingerprints. In WIoT systems, CNNs are used to analyze signal patterns and detect attacks like jamming or spoofing.

- **4.2.1.1 CNN for Time-Frequency Analysis**
  - **Description**: This technique uses CNNs to analyze time-frequency representations (e.g., spectrograms) of signals to detect passive jamming. In WIoT systems, CNNs can identify interference patterns caused by environmental manipulation (e.g., multipath interference). For example, in a smart city, CNNs can detect passive jamming affecting traffic sensors by processing RSSI data in the form of spectrograms.

- **Technique Sophistication**: Intermediate
  CNNs require moderate computational resources and expertise to design and train, making them an intermediate DL technique.
- **Applicability Context**: Smart Cities (e.g., detecting interference in traffic sensor networks)
  Traffic sensor networks in smart cities are vulnerable to passive jamming, which can disrupt traffic management. CNNs' ability to analyze time-frequency data makes them effective in this scenario.
- **Threat Mitigated**: Passive Jamming
  CNNs address Passive Jamming by identifying interference patterns, ensuring the availability of traffic sensor data.

- **4.2.1.2 CNN for RF Fingerprint Analysis**
  - **Description**: This technique uses CNNs to analyze RF fingerprints (e.g., transient amplitude, phase noise) to detect spoofing attempts. In WIoT systems, CNNs can distinguish between legitimate and forged RF fingerprints. For example, in industrial IoT, CNNs can prevent unauthorized control of machinery by identifying spoofed signals that impersonate legitimate devices.
  - **Technique Sophistication**: Intermediate
    CNNs for RF fingerprint analysis require moderate computational resources and expertise, like other CNN applications.
  - **Applicability Context**: Industrial IoT (e.g. to detect spoofing in machine control systems) Industrial IoT systems require secure unit approval to prevent unauthorized access to machines. CNNs' ability to analyze RF fingerprints makes them effective in this context.
  - **Threat Mitigated**: Spoofing
    CNNs address Spoofing by identifying forged RF fingerprints, ensuring the integrity of device authentication.

4.2.2 Recurrent Neural Networks (RNN)

RNNs are DL models implemented to process sequential data, such as time-series signals. In WIoT systems, RNNs are used to analyze temporal patterns in signals to detect attacks like eavesdropping or MITM.

- **4.2.2.1 RNN with Attention**
  - **Description**: This technique uses RNNs with attention mechanisms to analyze temporal patterns in CSI or RSSI data, focusing on suspicious signal patterns to detect coordinated eavesdropping attempts. In WIoT systems, RNNs with

attention can identify cooperative eavesdropping by multiple attackers. For example, in industrial IoT, this technique can detect coordinated eavesdropping in sensor networks by focusing on temporal anomalies.

  - **Technique Sophistication**: Advanced
    RNNs with attention mechanisms are complex due to the addition of attention layers, requiring significant computational resources and expertise.
  - **Applicability Context**: Industrial IoT (e.g., detecting cooperative eavesdropping in sensor networks)
    Industrial IoT sensor networks are vulnerable to cooperative eavesdropping, where multiple attackers collaborate to intercept data. RNNs with attention can effectively detect such coordinated attacks.
  - **Threat Mitigated**: Cooperative Eavesdropping
    RNNs with attention address Cooperative Eavesdropping by identifying temporal patterns indicative of coordinated attacks, protecting the confidentiality of sensor data.

- **4.2.2.2 Long Short-Term Memory (LSTM)**
  - **Description**: LSTM is a type of RNN designed to handle long-term dependencies in sequential data. In WIoT systems, LSTMs can analyze temporal sequences of signals (e.g., Channel Impulse Response, CIR) to detect MITM attacks that intercept and modify data. For example, in healthcare IoT, LSTMs can protect patient monitoring systems by detecting manipulated signals that indicate an MITM attack.
  - **Technique Sophistication**: Intermediate
    LSTMs are less complex than RNNs with attention but still require moderate computational resources due to their recurrent architecture.
  - **Applicability Context**: Healthcare IoT (e.g., detecting MITM attacks on patient monitoring systems)
    Healthcare IoT systems transmit sensitive patient data that can be intercepted and modified by MITM attacks. LSTMs' ability to analyze temporal sequences makes them effective in this scenario.
  - **Threat Mitigated**: MITM
    LSTMs address MITM attacks by detecting manipulated signals, protecting both the confidentiality and integrity of patient data.

4.2.3 Generative Adversarial Networks (GAN)

GANs are DL models that are divided into a generator and a discriminator that are trained adversarial. In WIoT systems, GANs are used to generate synthetic data for training robust models or to detect sophisticated attacks like adaptive spoofing.

- **4.2.3.1 GAN for Synthetic Signal Generation**
  - **Description**: This technique uses GANs to generate synthetic legitimate signals, which are then used to train a discriminator to detect adaptive spoofing. In WIoT systems, GANs can improve the robustness of detection models by providing diverse training data. For example, in a smart city, GANs can protect traffic management systems from adaptive spoofing by training a discriminator to identify spoofed signals that adapt to real-time conditions.
  - **Technique Sophistication**: Advanced
    GANs are highly complex due to their adversarial training process, requiring significant computational resources and expertise.
  - **Applicability Context**: Smart Cities (e.g., detecting adaptive spoofing in traffic management systems)
    Traffic management systems in smart cities are vulnerable to adaptive spoofing, where attackers dynamically adjust signals to mislead the system. GANs' ability to generate synthetic data makes them effective in this context.
  - Threat Mitigated: Adaptive Spoofing
    GANs address Adaptive Spoofing by training robust detection models, ensuring the integrity of traffic management data.
- **4.2.3.2 Data Augmentation with GANs**
  - **Description**: This technique uses GANs to generate synthetic RF fingerprints, which are used to train models that are robust to hardware-agnostic tampering. In WIoT systems, GANs can simulate diverse RF fingerprints to improve the generalization of detection models. For example, in a smart city, GANs can protect diverse IoT devices from hardware-agnostic tampering by training models to recognize a wide range of tampered fingerprints.
  - **Technique Sophistication**: Advanced
    Similar to other GAN applications, this technique is complex due to the adversarial training process and the need for significant computational resources.
  - **Applicability Context**: Smart Cities (e.g., detecting hardware-agnostic tampering in diverse IoT devices)
    Smart cities have diverse IoT devices (e.g., sensors, RFID tags), making them

vulnerable to hardware-agnostic tampering. GANs' ability to augment training data makes them effective in this scenario.

- **Threat Mitigated**: Hardware-Agnostic Tampering
  GANs address Hardware-Agnostic Tampering by training robust models to detect tampered RF fingerprints across diverse devices, ensuring the integrity of device authentication.

4.2.4 Autoencoders (AE)

Autoencoders are DL models that learn a compressed representation of data and are often used for anomaly detection. In WIoT systems, Autoencoders are used to detect anomalies in signals or RF fingerprints that indicate attacks like eavesdropping or tampering.

- **4.2.4.1 Autoencoders for Anomaly Detection**
  - **Description**: This technique uses Autoencoders to learn a compressed representation of legitimate signals (e.g., CIR or Channel Frequency Response, CFR) and detect anomalies caused by eavesdropping. In WIoT systems, Autoencoders can identify unauthorized signal interception by comparing reconstructed signals to the originals. For example, in healthcare IoT, Autoencoders can protect wearable device data by detecting eavesdropping attempts.
  - **Technique Sophistication**: Intermediate
    Autoencoders require moderate computational resources and expertise to design and train, making them an intermediate DL technique.
  - **Applicability Context**: Healthcare IoT (e.g., detecting eavesdropping on wearable device data)
    Wearable devices in healthcare IoT transmit sensitive patient data that can be intercepted by eavesdroppers. Autoencoders' ability to detect anomalies makes them effective in this context.
  - **Threat Mitigated**: Eavesdropping
    Autoencoders address Eavesdropping by identifying anomalies in signal patterns, protecting the confidentiality of patient data.
- **4.2.4.2 Autoencoders for Fingerprint Robustness**
  - **Description**: This technique uses Autoencoders to learn a robust representation of legitimate RF fingerprints and detect anomalies caused by hardware-agnostic tampering. In WIoT systems, Autoencoders can identify tampered fingerprints by comparing them to the learned representation. For example, in healthcare IoT,

Autoencoders can protect medical devices from impersonation by detecting tampered RF fingerprints.

- **Technique Sophistication**: Intermediate
  Similar to other Autoencoder applications, this technique requires moderate computational resources and expertise.
- **Applicability Context**: Healthcare IoT (e.g., detecting hardware-agnostic tampering in medical devices)
  Medical devices in healthcare IoT are vulnerable to hardware-agnostic tampering, where attackers emulate fingerprints across devices. Autoencoders' ability to learn robust representations makes them effective in this scenario.
- **Threat Mitigated**: Hardware-Agnostic Tampering
  Autoencoders address Hardware-Agnostic Tampering by detecting anomalies in RF fingerprints, ensuring the integrity of device authentication.

4.2.5 Transformer Models

Transformers are DL models that use self-attention mechanisms to process sequential data, often used for tasks requiring cross-contextual analysis. In WIoT systems, Transformers are used to analyze cross-layer data to detect complex attacks like layered MITM.

- **4.2.5.1 Transformers for Cross-Layer Analysis**
  - **Description**: This technique uses Transformers to analyze cross-layer data (e.g., physical-layer CSI and network-layer routing information) to detect layered MITM attacks. In WIoT systems, Transformers can identify patterns that indicate multi-layer manipulation. For example, in industrial IoT, Transformers can protect cross-layer communication in manufacturing systems by detecting layered MITM attacks that target both physical and network layers.
  - **Technique Sophistication**: Advanced
    Transformers are highly complex due to their self-attention mechanisms and large number of parameters, requiring significant computational resources and expertise.
  - **Applicability Context**: Industrial IoT (e.g., detecting layered MITM in cross-layer systems)
    Industrial IoT systems often use layered architectures, making them vulnerable to layered MITM attacks. Transformers' ability to analyze cross-layer data makes them effective in this context.

- **Threat Mitigated**: Layered MITM
  Transformers address Layered MITM by detecting multi-layer manipulation, protecting both confidentiality and integrity across layers.

4.2.6 Complex-Valued Neural Networks (CVNN)

CVNNs are DL models designed to process complex-valued data, such as I/Q signals in wireless communication. In WIoT systems, CVNNs are used to analyze RF signals and detect attacks like RF fingerprint tampering.

- **4.2.6.1 CVNN for Complex Signal Processing**
  - **Description**: This technique uses CVNNs to process complex-valued RF signals (e.g., I/Q data) to detect tampered RF fingerprints. In WIoT systems, CVNNs can distinguish between legitimate and forged fingerprints by analyzing complex signal characteristics. For example, in a smart city, CVNNs can protect access control systems by identifying forged RF fingerprints used in unauthorized access attempts.
  - **Technique Sophistication**: Advanced
    CVNNs are complex due to their ability to handle complex-valued data, requiring significant computational resources and expertise in signal processing.
  - **Applicability Context**: Smart Cities (e.g., detecting RF fingerprint tampering in access control systems)
    Access control systems in smart cities (e.g., for building entry) are vulnerable to RF fingerprint tampering. CVNNs' ability to process complex signals makes them effective in this scenario.
  - **Threat Mitigated**: RF Fingerprint Tampering
    CVNNs address RF Fingerprint Tampering by accurately identifying forged fingerprints, ensuring the integrity of access control systems.

The ML/DL taxonomy directly addresses the threats identified in the Physical-Layer Security Threats in WIoT taxonomy, ensuring a comprehensive mitigation strategy:

- **Signal Disruption (Active Jamming, Passive Jamming):**
  - Active Jamming: Mitigated by SVM (Supervised Learning) and Game-Theoretic RL (Reinforcement Learning), which detect and adapt to jamming attacks in industrial IoT and smart grid scenarios.

    - Passive Jamming: Mitigated by Clustering (Unsupervised Learning) and CNN for Time-Frequency Analysis (Deep Learning), which detect interference patterns in dense IoT deployments and smart cities.

- **Signal Interception (Eavesdropping, Cooperative Eavesdropping):**
    - Eavesdropping: Mitigated by OCC-SVM (Unsupervised Learning) and Autoencoders for Anomaly Detection (Deep Learning), which detect unauthorized signal interception in smart homes and healthcare IoT.
    - Cooperative Eavesdropping: Mitigated by Multi-Agent RL (Reinforcement Learning) and RNN with Attention (Deep Learning), which handle coordinated attacks in smart cities and industrial IoT.
- **Signal Manipulation (Spoofing, Adaptive Spoofing, MITM, Layered MITM):**
    - Spoofing: Mitigated by KNN (Supervised Learning) and CNN for RF Fingerprint Analysis (Deep Learning), which detect forged signals in smart cities and industrial IoT.
    - Adaptive Spoofing: Mitigated by DDPG (Reinforcement Learning) and GAN for Synthetic Signal Generation (Deep Learning), which adapt to dynamic attacks in intelligent transportation systems and smart cities.
    - MITM: Mitigated by Decision Tree (Supervised Learning) and LSTM (Deep Learning), which detect manipulated signals in smart grids and healthcare IoT.
    - Layered MITM: Mitigated by Multi-Agent RL with Game Theory (Reinforcement Learning) and Transformers for Cross-Layer Analysis (Deep Learning), which address multi-layer attacks in smart cities and industrial IoT.
- **Hardware Exploitation (RF Fingerprint Tampering, Hardware-Agnostic Tampering):**
    - RF Fingerprint Tampering: Mitigated by Ensemble Learning (Supervised Learning) and CVNN for Complex Signal Processing (Deep Learning), which detect tampered fingerprints in industrial IoT and smart cities.

Hardware-Agnostic Tampering: Mitigated by Autoencoders for Fingerprint Robustness and Data Augmentation with GANs (Deep Learning), which ensure robust detection across diverse devices in healthcare IoT and smart cities.

Table 7: Taxonomy of ML and DL Techniques for Physical-Layer Security in WIoT

Class	Technique	Description	Sophistication	Applicability Context	Threat Mitigated
Machine Learning	SVM	Classify signals via hyperplane	Basic	Industrial IoT	Active Jamming
	KNN	Neighbor-based classification	Basic	Smart Cities	Spoofing
	Game-Theoretic RL	Adapts to jamming via Q-Learning	Advanced	Smart Grid	Active Jamming
Deep Learning	CNN (Time-Freq.)	Analyzes spectrograms for jamming	Intermediate	Smart Cities	Passive Jamming
	GAN (Synthetic)	Generates signals for spoofing detect	Advanced	Smart Cities	Adaptive Spoofing
	Transformers	Cross-layer analysis for MITM	Advanced	Industrial IoT	Layered MITM

5. Review of Datasets for Physical-Layer Security

The rapid expansion of Wireless Internet of Things (WIOT) devices has amplified the need for robust physical-layer security mechanisms, particularly Physical-Layer Security (PLS). provides a comprehensive survey of Machine Learning (ML)-based PLS, offering a taxonomy of fingerprints, a compilation of open-source datasets, and future research directions. This section reviews the datasets listed in the paper, analyzes their availability through an Exploratory Data Analysis (EDA), evaluates physical-layer security, and provides recommendations for dataset selection to support our research on deep learning for physical-layer security in WIOT.

Growth of IoT Devices and Security Research

The increasing adoption of IoT devices underscores the urgency of addressing security challenges in WIOT. Figure 17 illustrates the growth of IoT devices and the corresponding increase in security-related research from 2020 to 2025. The number of IoT units is estimated to grow from approximately 10 billion in 2020 to 30 billion in 2025, while the percentage of safety-related papers rises from 12.3% to 31.5% in the same period. This trend highlights the growing academic focus on security as IoT adoption accelerates, justifying the relevance of our research into ML-based PLA for WIOT.

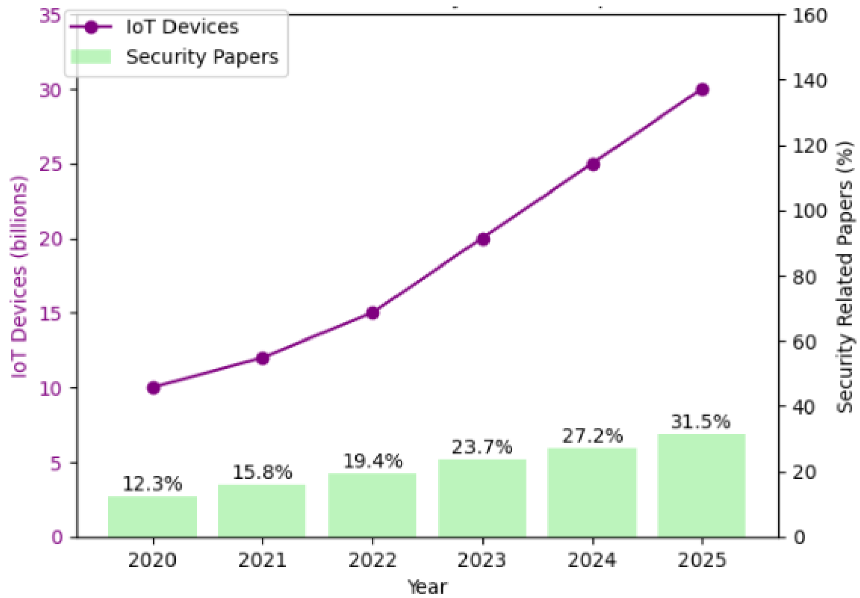


Figure17: Growth of IoT Devices and Security-Related Papers (2020-2025)

The paper compiles a list of 22 open-source datasets for RF and channel fingerprints, essential for developing and testing DL-based PLS schemes. These datasets are categorized into RF Fingerprint (12 datasets) and Channel Fingerprint (10 datasets). Table 1 provides a detailed overview of these datasets, including their category, reference, description, source/provider, and availability status.

Exploratory Data Analysis (EDA) of Dataset Metadata

To understand the availability and distribution of these datasets, we conducted an EDA on their metadata using Python. The following code was used to perform the analysis and generate visualizations:

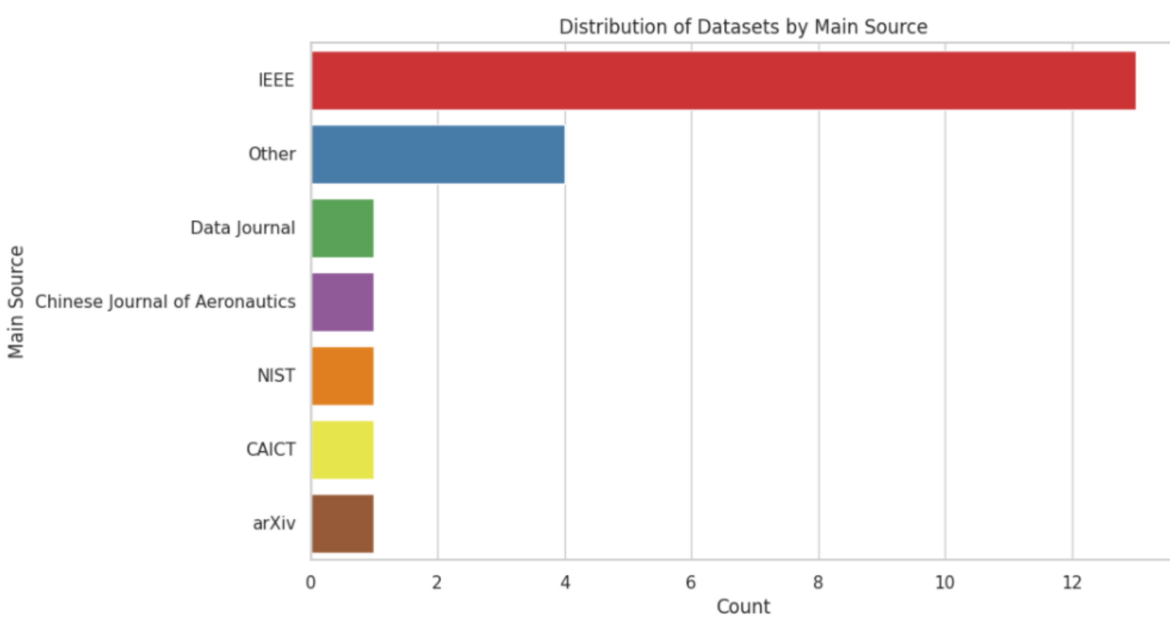


Figure18: Distribution of Datasets by Main Source

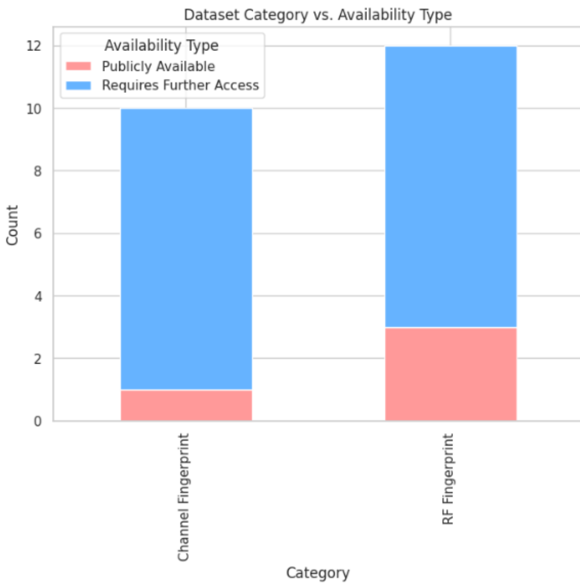


Figure19: Distribution of Datasets by Main Source

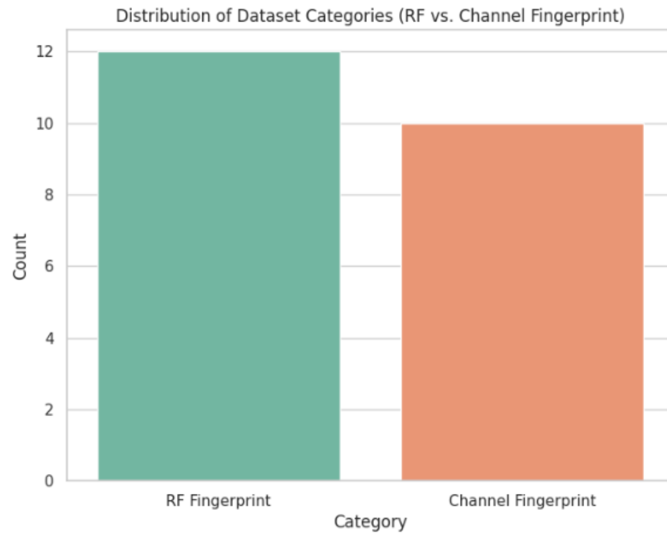


Figure20: Dataset Categories (RF vs. Channel Fingerprint)

Based on the EDA, we recommend the following datasets for immediate use in our experimental analysis:

- **Publicly Available Datasets:**
  - **WiSig Dataset ([]): Covers 174 Wi-Fi devices, ideal for RF fingerprinting in WIOT. Available at UCLA CORES Lab.**
  - **Drone Remote Controller RF Signal Dataset ([262]): Focuses on drone communications, a growing area in WIOT. Available via DOI at IEEE DataPort.**
  - **Mobile Communication Open Dataset ([]): Supports various wireless tasks in city scenarios. Available at CAICT.**
- **Datasets Requiring Further Access: For datasets like NIST ([]) and DeepMIMO ([]), we recommend contacting the authors or accessing through institutional subscriptions, as they offer novel insights into industrial and mmWave scenarios.**
- **Supplementary Kaggle Datasets: Explore Real-world Wireless Communication Dataset and DeepSlice & Secure5G - 5G & LTE Wireless Dataset for additional RF signal data, ensuring their relevance to physical-layer security.**

Table 8: Taxonomy of ML and DL Techniques for Physical-Layer Security in WIoT

Category	Reference	Name/Description	Availability Type	Recommended Use
RF Fingerprint		RF fingerprints from 16 USRP X310 devices	Requires Further Access	Contact authors for potential use in RF fingerprinting studies.
		I/Q datasets from 20 USRP X310/N210 devices		
		ADS-B signals from 140 aircraft		
		Signals from 60 commercial LoRa devices		
		Signals from 4 USRP X310 devices (IEEE		

		802.11a/LTE/5G NR)		
		Bluetooth signals from 86 smartphones	Publicly Available	Use for Bluetooth-based RF fingerprinting studies (DOI: 10.3390/data5020055).
		ADS-B signals from 728 aircraft	Requires Further Access	Contact authors for potential use in large-scale aviation security studies.
		WiFi signals from 174 devices	Publicly Available	Recommended for immediate use in RF fingerprinting for WIOT (URL: https://cores.ee.ucla.edu/downloads/datasets/wisig/).
		LoRa signals from 25 Pycom devices	Requires Further Access	Contact authors for potential use in LoRa-based WIOT security studies.
		Signals from 21 USRP N2932 devices (IEEE 802.15.4)	Requires Further Access	Contact authors for potential use in LoRa-based WIOT security studies.
		Signals from 17 drone remote controllers	Publicly Available	Recommended for immediate use in drone communication security studies (DOI: 10.21227/ss99-8d56).
		Signals from 7 DJI M100 drones	Requires Further Access	Contact authors for potential use in drone communication security studies.
Channel Fingerprint		CIR measurements from industrial scenarios	Requires Further Access	Contact authors for potential use in drone communication security studies.
		Dataset from real-world scenes of 40 big cities	Publicly Available	Recommended for immediate use in channel fingerprinting for urban WIOT (URL: https://www.mobileai-dataset.com).
		Extended WINNER channel model for 4G LTE	Requires Further Access	Contact authors for potential use in drone communication security studies.
		COST 2100 channel model for MIMO	Requires Further Access	
		DeepMIMO dataset for Massive MIMO and mmWave		
		CSI data from complex indoor environments		

		Generalized 5G NR dataset generator		
		SimRIS Channel Simulator for RIS-aided systems		
		ViWi dataset framework for vision-aided wireless		
		Underwater acoustic channel model		

References

[1] S. Kumar, P. Tiwari, and M. Zymbler, “Internet of Things is a revolutionary approach for future technology enhancement: a review,” *J Big Data*, vol. 6, no. 1, p. 111, Dec. 2019, doi: 10.1186/s40537-019-0268-2.

[2] R. Singh, A. Gehlot, S. Vaseem Akram, A. Kumar Thakur, D. Buddhi, and P. Kumar Das, “Forest 4.0: Digitalization of forest using the Internet of Things (IoT),” *Journal of*

King Saud University - Computer and Information Sciences, vol. 34, no. 8, pp. 5587–5601, Sep. 2022, doi: 10.1016/j.jksuci.2021.02.009.

[3] K. St. Germain and F. Kragh, “Physical-Layer Authentication Using Channel State Information and Machine Learning,” in *2020 14th International Conference on Signal Processing and Communication Systems (ICSPCS)*, IEEE, Dec. 2020, pp. 1–8. doi: 10.1109/ICSPCS50536.2020.9310070.

[4] J. D. Vega Sanchez, L. Urquiza-Aguiar, and M. C. Paredes Paredes, “Physical Layer Security for 5G Wireless Networks: A Comprehensive Survey,” in *2019 3rd Cyber Security in Networking Conference (CSNet)*, IEEE, Oct. 2019, pp. 122–129. doi: 10.1109/CSNet47905.2019.9108955.

[5] M. Azrour, J. Mabrouki, A. Guezzaz, and A. Kanwal, “Internet of Things Security: Challenges and Key Issues,” *Security and Communication Networks*, vol. 2021, pp. 1–11, Sep. 2021, doi: 10.1155/2021/5533843.

[6] N. Zhang, D. Chen, F. Ye, T.-X. Zheng, and Z. Wei, “Physical Layer Security for Internet of Things,” *Wirel Commun Mob Comput*, vol. 2019, pp. 1–2, Apr. 2019, doi: 10.1155/2019/2627938.

[7] H. Sharma and N. Kumar, “Deep learning based physical layer security for terrestrial communications in 5G and beyond networks: A survey,” *Physical Communication*, vol. 57, p. 102002, Apr. 2023, doi: 10.1016/j.phycom.2023.102002.

[8] F. Restuccia and T. Melodia, “Deep Learning at the Physical Layer: System Challenges and Applications to 5G and Beyond,” *IEEE Communications Magazine*, vol. 58, no. 10, pp. 58–64, Oct. 2020, doi: 10.1109/MCOM.001.2000243.

[9] T. Liu, G. Ramachandran, and R. Jurdak, “Post-Quantum Cryptography for Internet of Things: A Survey on Performance and Optimization,” Jan. 2024.

[10] J.-Y. Lee, W.-C. Lin, and Y.-H. Huang, “A lightweight authentication protocol for Internet of Things,” in *2014 International Symposium on Next-Generation Electronics (ISNE)*, IEEE, May 2014, pp. 1–2. doi: 10.1109/ISNE.2014.6839375.

[11] F. Pereira, R. Correia, P. Pinho, S. I. Lopes, and N. B. Carvalho, “Challenges in Resource-Constrained IoT Devices: Energy and Communication as Critical Success Factors for Future IoT Deployment,” *Sensors*, vol. 20, no. 22, p. 6420, Nov. 2020, doi: 10.3390/s20226420.

[12] A. B. Guiloufi, S. El khediri, N. Nasri, and A. Kachouri, “A comparative study of energy efficient algorithms for IoT applications based on WSNs,” *Multimed Tools Appl*, vol. 82, no. 27, pp. 42239–42275, Nov. 2023, doi: 10.1007/s11042-023-14813-3.

[13] A. Soni, R. Upadhyay, and A. Jain, “Internet of Things and Wireless Physical Layer Security: A Survey,” 2017, pp. 115–123. doi: 10.1007/978-981-10-3226-4_11.

[14] H. Jafari, O. Omotere, D. Adesina, H.-H. Wu, and L. Qian, “IoT Devices Fingerprinting Using Deep Learning,” in *MILCOM 2018 - 2018 IEEE Military Communications Conference (MILCOM)*, IEEE, Oct. 2018, pp. 1–9. doi: 10.1109/MILCOM.2018.8599826.

[15] S. Khan, C. Thapa, S. Durrani, and S. Camtepe, “Access-Based Lightweight Physical-Layer Authentication for the Internet of Things Devices,” *IEEE Internet Things J*, vol. 11, no. 7, pp. 11312–11326, Apr. 2024, doi: 10.1109/JIOT.2023.3331362.

[16] R. Mustafa, N. I. Sarkar, M. Mohaghegh, and S. Pervez, “A Cross-Layer Secure and Energy-Efficient Framework for the Internet of Things: A Comprehensive Survey,” *Sensors*, vol. 24, no. 22, p. 7209, Nov. 2024, doi: 10.3390/s24227209.

[17] C. Lv and Z. Luo, “Deep Learning for Channel Estimation in Physical Layer Wireless Communications: Fundamental, Methods, and Challenges,” *Electronics (Basel)*, vol. 12, no. 24, p. 4965, Dec. 2023, doi: 10.3390/electronics12244965.

[18] Y. Li, Y. Wang, X. Liu, P. Zuo, H. Li, and H. Jiang, “Deep-Reinforcement-Learning-Based Wireless IoT Device Identification Using Channel State Information,” *Symmetry (Basel)*, vol. 15, no. 7, p. 1404, Jul. 2023, doi: 10.3390/sym15071404.

[19] J. Bassey, X. Li, and L. Qian, “Device Authentication Codes based on RF Fingerprinting using Deep Learning,” *ICST Transactions on Security and Safety*, vol. 8, no. 29, p. 172305, Nov. 2021, doi: 10.4108/eai.30-11-2021.172305.

[20] O. T. Ajayi, S. O. Onidare, and H. Tajudeen, “A Study on Adversarial Machine Learning in Wireless Communication Systems,” 2024, pp. 384–392. doi: 10.1007/978-981-97-6937-7_46.

[21] N. Xie, J. Zhang, and Q. Zhang, “Security Provided by the Physical Layer in Wireless Communications,” *IEEE Netw*, vol. 37, no. 5, pp. 42–48, Sep. 2023, doi: 10.1109/MNET.121.2200110.

[22] P. Angueira *et al.*, “A Survey of Physical Layer Techniques for Secure Wireless Communications in Industry,” *IEEE Communications Surveys & Tutorials*, vol. 24, no. 2, pp. 810–838, Dec. 2022, doi: 10.1109/COMST.2022.3148857.

[23] A. Jagannath, J. Jagannath, and P. S. P. V. Kumar, "A Comprehensive Survey on Radio Frequency (RF) Fingerprinting: Traditional Approaches, Deep Learning, and Open Challenges," Jan. 11, 2022. doi: 10.36227/techrxiv.17711444.v2.

[24] W. Lee, S. Y. Baek, and S. H. Kim, "Deep-Learning-Aided RF Fingerprinting for NFC Security," *IEEE Communications Magazine*, vol. 59, no. 5, pp. 96–101, May 2021, doi: 10.1109/MCOM.001.2000912.

[25] Y. Liu, J. Wang, J. Li, S. Niu, and H. Song, "Machine Learning for the Detection and Identification of Internet of Things Devices: A Survey," *IEEE Internet Things J*, vol. 9, no. 1, pp. 298–320, Jan. 2022, doi: 10.1109/JIOT.2021.3099028.

[26] N. Soltani, K. Sankhe, J. Dy, S. Ioannidis, and K. Chowdhury, "More Is Better: Data Augmentation for Channel-Resilient RF Fingerprinting," *IEEE Communications Magazine*, vol. 58, no. 10, pp. 66–72, Oct. 2020, doi: 10.1109/MCOM.001.2000180.

[27] N. Xie, Z. Li, and H. Tan, "A Survey of Physical-Layer Authentication in Wireless Communications," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 1, pp. 282–310, Dec. 2021, doi: 10.1109/COMST.2020.3042188.

[28] Y. Liu, X. Wang, and J. Mei, "Hybrid Multiple Access and Service-Oriented Resource Allocation for Heterogeneous QoS Provisioning in Machine Type Communications," *Journal of Communications and Information Networks*, vol. 5, no. 2, pp. 225–236, Jun. 2020, doi: 10.23919/JCIN.2020.9130438.

[29] X. Fan, F. Wang, F. Wang, W. Gong, and J. Liu, "When RFID Meets Deep Learning: Exploring Cognitive Intelligence for Activity Identification," *IEEE Wirel Commun*, vol. 26, no. 3, pp. 19–25, Jun. 2019, doi: 10.1109/MWC.2019.1800405.

[30] H. Fang, X. Wang, and S. Tomasin, "Machine Learning for Intelligent Authentication in 5G and Beyond Wireless Networks," *IEEE Wirel Commun*, vol. 26, no. 5, pp. 55–61, Oct. 2019, doi: 10.1109/MWC.001.1900054.

[31] M. Padhiary, P. Roy, and D. Roy, "The Future of Urban Connectivity," 2024, pp. 33–66. doi: 10.4018/979-8-3693-6740-7.ch002.

[32] 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, pp. 17–27, Mar. 2017, doi: 10.1109/MIE.2017.2649104.

[33] R. Priyadarshani, K.-H. Park, Y. Ata, and M.-S. Alouini, "Jamming Intrusions in Extreme Bandwidth Communication: A Comprehensive Overview," Mar. 2024.

[34] M. Krishna Pasupuleti, “Autonomous Drone Swarms in Action: AI for Mission Coordination and Adaptive Navigation,” in *AI in Autonomous Drone Swarms: Coordinating Complex Missions*, National Education Services, 2024, pp. 76–95. doi: 10.62311/nesx/66227.

[35] B. M. ElHalawany, A. A. A. El-Banna, and K. Wu, “Physical-Layer Security and Privacy for Vehicle-to-Everything,” *IEEE Communications Magazine*, vol. 57, no. 10, pp. 84–90, Oct. 2019, doi: 10.1109/MCOM.001.1900141.

[36] P. Bellavista, G. Cardone, A. Corradi, and L. Foschini, “Convergence of MANET and WSN in IoT Urban Scenarios,” *IEEE Sens J*, vol. 13, no. 10, pp. 3558–3567, Oct. 2013, doi: 10.1109/JSEN.2013.2272099.

[37] J. Shehu Yalli, M. Hilmi Hasan, and A. Abubakar Badawi, “Internet of Things (IoT): Origins, Embedded Technologies, Smart Applications, and Its Growth in the Last Decade,” *IEEE Access*, vol. 12, pp. 91357–91382, 2024, doi: 10.1109/ACCESS.2024.3418995.

[38] S. Li, L. Da Xu, and S. Zhao, “The internet of things: a survey,” *Information Systems Frontiers*, vol. 17, no. 2, pp. 243–259, Apr. 2015, doi: 10.1007/s10796-014-9492-7.

[39] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, “Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications,” *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2347–2376, Dec. 2015, doi: 10.1109/COMST.2015.2444095.

[40] M. S. Farooq *et al.*, “A Survey on the Role of Industrial IoT in Manufacturing for Implementation of Smart Industry,” *Sensors*, vol. 23, no. 21, p. 8958, Nov. 2023, doi: 10.3390/s23218958.

[41] Md. N. Mowla, N. Mowla, A. F. M. S. Shah, K. M. Rabie, and T. Shongwe, “Internet of Things and Wireless Sensor Networks for Smart Agriculture Applications: A Survey,” *IEEE Access*, vol. 11, pp. 145813–145852, 2023, doi: 10.1109/ACCESS.2023.3346299.

[42] M. K. Banafaa *et al.*, “A Comprehensive Survey on 5G-and-Beyond Networks With UAVs: Applications, Emerging Technologies, Regulatory Aspects, Research Trends and Challenges,” *IEEE Access*, vol. 12, pp. 7786–7826, 2024, doi: 10.1109/ACCESS.2023.3349208.

[43] A. Diane, O. Diallo, and E. H. M. Ndoye, “A systematic and comprehensive review on low power wide area network: characteristics, architecture, applications and

research challenges," *Discover Internet of Things*, vol. 5, no. 1, p. 7, Jan. 2025, doi: 10.1007/s43926-025-00097-6.

[44] X. Kong, Y. Wu, H. Wang, and F. Xia, "Edge Computing for Internet of Everything: A Survey," *IEEE Internet Things J*, vol. 9, no. 23, pp. 23472–23485, Dec. 2022, doi: 10.1109/JIOT.2022.3200431.

[45] O. Zaporozhets, V. Isaienko, and K. Synylo, "Trends on current and forecasted aircraft hybrid electric architectures and their impact on environment," *Energy*, vol. 211, p. 118814, Nov. 2020, doi: 10.1016/j.energy.2020.118814.

[46] K. Aarika, M. Bouhlal, R. A. Abdelouahid, S. Elfilali, and E. Benlahmar, "Perception layer security in the internet of things," *Procedia Comput Sci*, vol. 175, pp. 591–596, 2020, doi: 10.1016/j.procs.2020.07.085.

[47] X. Zhang, G. Li, J. Zhang, A. Hu, Z. Hou, and B. Xiao, "Deep-Learning-Based Physical-Layer Secret Key Generation for FDD Systems," *IEEE Internet Things J*, vol. 9, no. 8, pp. 6081–6094, Apr. 2022, doi: 10.1109/JIOT.2021.3109272.

[48] M. Thankappan, H. Rifà-Pous, and C. Garrigues, "Multi-Channel Man-in-the-Middle attacks against protected Wi-Fi networks: A state of the art review," *Expert Syst Appl*, vol. 210, p. 118401, Dec. 2022, doi: 10.1016/j.eswa.2022.118401.

[49] R. Saini, D. Halder, and A. M. Baswade, "RIDS: Real-time Intrusion Detection System for WPA3 enabled Enterprise Networks," in *GLOBECOM 2022 - 2022 IEEE Global Communications Conference*, IEEE, Dec. 2022, pp. 43–48. doi: 10.1109/GLOBECOM48099.2022.10001501.

[50] M. Harvanek, J. Bolcek, J. Kufa, L. Polak, M. Simka, and R. Marsalek, "Survey on 5G Physical Layer Security Threats and Countermeasures," *Sensors*, vol. 24, no. 17, p. 5523, Aug. 2024, doi: 10.3390/s24175523.

[51] M. M. Saeed *et al.*, "A comprehensive survey on 6G-security: physical connection and service layers," *Discover Internet of Things*, vol. 5, no. 1, p. 28, Mar. 2025, doi: 10.1007/s43926-025-00123-7.

[52] K. Ramezanpour, J. Jagannath, and A. Jagannath, "Security and privacy vulnerabilities of 5G/6G and WiFi 6: Survey and research directions from a coexistence perspective," *Computer Networks*, vol. 221, p. 109515, Feb. 2023, doi: 10.1016/j.comnet.2022.109515.

[53] G. Leenders, G. Callebaut, G. Ottoy, L. Van der Perre, and L. De Strycker, “Multi-RAT for IoT: The Potential in Combining LoRaWAN and NB-IoT,” *IEEE Communications Magazine*, vol. 59, no. 12, pp. 98–104, Dec. 2021, doi: 10.1109/MCOM.008.2100382.

[54] D. Wang, A. Traspadini, M. Giordani, M.-S. Alouini, and M. Zorzi, “On the Performance of Non-Terrestrial Networks to Support the Internet of Things,” in *2022 56th Asilomar Conference on Signals, Systems, and Computers*, IEEE, Oct. 2022, pp. 881–887. doi: 10.1109/IEEECONF56349.2022.10052102.

[55] A. Malik, V. Parihar, B. Bhushan, R. Chaganti, S. Bhatia, and P. N. Astya, “Security Services for Wireless 5G Internet of Things (IoT) Systems,” 2023, pp. 169–195. doi: 10.1007/978-981-99-3668-7_9.

[56] A. T. Jawad, R. Maaloul, and L. Chaari, “A comprehensive survey on 6G and beyond: Enabling technologies, opportunities of machine learning and challenges,” *Computer Networks*, vol. 237, p. 110085, Dec. 2023, doi: 10.1016/j.comnet.2023.110085.

[57] A. Mosteiro-Sanchez, M. Barcelo, J. Astorga, and A. Urbieta, “Securing IIoT using Defence-in-Depth: Towards an End-to-End secure Industry 4.0,” *J Manuf Syst*, vol. 57, pp. 367–378, Oct. 2020, doi: 10.1016/j.jmsy.2020.10.011.

[58] Amrita, C. P. Ekwueme, I. H. Adam, and A. Dwivedi, “Lightweight Cryptography for Internet of Things: A Review,” *EAI Endorsed Transactions on Internet of Things*, vol. 10, Mar. 2024, doi: 10.4108/eetiot.5565.

[59] 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, pp. 20–27, Apr. 2015, doi: 10.1109/MCOM.2015.7081071.

[60] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, and G. Pantziou, “A survey on jamming attacks and countermeasures in WSNs,” *IEEE Communications Surveys & Tutorials*, vol. 11, no. 4, pp. 42–56, 2009, doi: 10.1109/SURV.2009.090404.

[61] X. Liu, X. Meng, H. Duan, Z. Hu, and M. Wang, “A Survey on Secure WiFi Sensing Technology: Attacks and Defenses,” *Sensors*, vol. 25, no. 6, p. 1913, Mar. 2025, doi: 10.3390/s25061913.

[62] Y. Chen, J. Yang, W. Trappe, and R. P. Martin, “Detecting and Localizing Identity-Based Attacks in Wireless and Sensor Networks,” *IEEE Trans Veh Technol*, vol. 59, no. 5, pp. 2418–2434, Jun. 2010, doi: 10.1109/TVT.2010.2044904.

[63] M. Conti, N. Dragoni, and V. Lesyk, “A Survey of Man In The Middle Attacks,” *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 2027–2051, Dec. 2016, doi: 10.1109/COMST.2016.2548426.

[64] J.-D. Kim, M. Ko, and J.-M. Chung, “Physical Identification Based Trust Path Routing Against Sybil Attacks on RPL in IoT Networks,” *IEEE Wireless Communications Letters*, vol. 11, no. 5, pp. 1102–1106, May 2022, doi: 10.1109/LWC.2022.3157831.

[65] H. S. Sanchez, D. Rotondo, M. L. Vidal, and J. Quevedo, “Frequency-based detection of replay attacks: application to a quadrotor UAV,” in *2019 8th International Conference on Systems and Control (ICSC)*, IEEE, Oct. 2019, pp. 289–294. doi: 10.1109/ICSC47195.2019.8950619.

[66] R. Melki, H. N. Noura, A. Chehab, and R. Couturier, “Machine Learning for Physical Layer Security: Limitations, Challenges and Recommendation,” in *2022 16th International Conference on Signal-Image Technology & Internet-Based Systems (SITIS)*, IEEE, Oct. 2022, pp. 53–60. doi: 10.1109/SITIS57111.2022.00017.

[67] M. Raeisi-Varzaneh, O. Dakkak, H. Alaidaros, and İ. Avci, “Internet of Things: Security, Issues, Threats, and Assessment of Different Cryptographic Technologies,” *Journal of Communications*, pp. 78–89, Feb. 2024, doi: 10.12720/jcm.19.2.78-89.

[68] A. Hassan, “Lightweight Cryptography for the Internet of Things,” 2021, pp. 780–795. doi: 10.1007/978-3-030-63092-8_52.

[69] L. Sun and X. Tian, “Physical Layer Security in Multi-Antenna Cellular Systems: Joint Optimization of Feedback Rate and Power Allocation,” *IEEE Trans Wirel Commun*, vol. 21, no. 9, pp. 7165–7180, Sep. 2022, doi: 10.1109/TWC.2022.3155775.

[70] A. Jagannath, J. Jagannath, and P. S. P. V. Kumar, “A Comprehensive Survey on Radio Frequency (RF) Fingerprinting: Traditional Approaches, Deep Learning, and Open Challenges,” Aug. 11, 2022. doi: 10.36227/techrxiv.17711444.v3.

[71] G. Li, C. Sun, J. Zhang, E. Jorswieck, B. Xiao, and A. Hu, “Physical Layer Key Generation in 5G and Beyond Wireless Communications: Challenges and Opportunities,” *Entropy*, vol. 21, no. 5, p. 497, May 2019, doi: 10.3390/e21050497.

[72] M. Nawaz and M. I. K. Babar, “IoT and AI for smart agriculture in resource-constrained environments: challenges, opportunities and solutions,” *Discover Internet of Things*, vol. 5, no. 1, p. 24, Mar. 2025, doi: 10.1007/s43926-025-00119-3.

[73] M. Li and Z. Dou, “Active eavesdropping detection: a novel physical layer security in wireless IoT,” *EURASIP J Adv Signal Process*, vol. 2023, no. 1, p. 119, Nov. 2023, doi: 10.1186/s13634-023-01080-5.

[74] W. Wu, S. Hu, D. Lin, and G. Wu, “Reliable resource allocation with RF fingerprinting authentication in secure IoT networks,” *Science China Information Sciences*, vol. 65, no. 7, p. 170304, Jul. 2022, doi: 10.1007/s11432-021-3284-y.

[75] M. Shakiba-Herfeh, A. Chorti, and H. V. Poor, “Physical Layer Security: Authentication, Integrity and Confidentiality,” Jan. 2020.

[76] J. Boodai, A. Alqahtani, and M. Frikha, “Review of Physical Layer Security in 5G Wireless Networks,” *Applied Sciences*, vol. 13, no. 12, p. 7277, Jun. 2023, doi: 10.3390/app13127277.

[77] X. Zhang, G. Li, J. Zhang, A. Hu, Z. Hou, and B. Xiao, “Deep-Learning-Based Physical-Layer Secret Key Generation for FDD Systems,” *IEEE Internet Things J*, vol. 9, no. 8, pp. 6081–6094, Apr. 2022, doi: 10.1109/JIOT.2021.3109272.

[78] S. A. Hoseini, F. Bouhafs, N. Aboutorab, P. Sadeghi, and F. den Hartog, “Cooperative Jamming for Physical Layer Security Enhancement Using Deep Reinforcement Learning,” in *2023 IEEE Globecom Workshops (GC Wkshps)*, IEEE, Dec. 2023, pp. 1838–1843. doi: 10.1109/GCWkshps58843.2023.10465104.

[79] S. Deka, K. Deka, N. T. Nguyen, S. Sharma, V. Bhatia, and N. Rajatheva, “Comprehensive Review of Deep Unfolding Techniques for Next-Generation Wireless Communication Systems,” Feb. 2025.

[80] X. Chen, S. Zhang, Q. Jiang, J. Chen, H. Huang, and C. Gu, “IoT-GAN: Anomaly Detection for Time Series in IoT Based on Generative Adversarial Networks,” 2022, pp. 682–694. doi: 10.1007/978-3-030-95388-1_45.

[81] X. Tang *et al.*, “Deep Graph Reinforcement Learning for UAV-Enabled Multi-User Secure Communications,” Apr. 2025.

[82] D. Huang, A. Al-Hourani, K. Sithamparanathan, and W. S. T. Rowe, “Deep Learning Methods for IoT Device Authentication Using Symbols Density Trace Plot,” *IEEE Internet Things J*, vol. 11, no. 10, pp. 18167–18179, May 2024, doi: 10.1109/JIOT.2024.3361892.

[83] B. T. Hasan and A. K. Idrees, “Edge Computing for IoT,” Feb. 2024, doi: 10.1007/978-3-031-50514-0_1.

[84] M. Zhang, E. Wei, and R. Berry, “Faithful Edge Federated Learning: Scalability and Privacy,” Jun. 2021.

[85] F. Aloraini, A. Javed, O. Rana, and P. Burnap, “Adversarial machine learning in IoT from an insider point of view,” *Journal of Information Security and Applications*, vol. 70, p. 103341, Nov. 2022, doi: 10.1016/j.jisa.2022.103341.

[86] O. A. Topal, S. Gecgel, E. M. Eksioglu, and G. K. Kurt, “Identification of Smart Jammers: Learning based Approaches Using Wavelet Representation,” Jan. 2019.

[87] G. Su, M. Dai, B. Chen, and X. Lin, “Deep reinforcement learning aided secure UAV communications in the presence of moving eavesdroppers,” *Journal of King Saud University - Computer and Information Sciences*, vol. 36, no. 4, p. 102047, Apr. 2024, doi: 10.1016/j.jksuci.2024.102047.

[88] J. Bassey, X. Li, and L. Qian, “Device Authentication Codes based on RF Fingerprinting using Deep Learning,” *ICST Transactions on Security and Safety*, vol. 8, no. 29, p. 172305, Nov. 2021, doi: 10.4108/eai.30-11-2021.172305.

[89] A. Bahramali, M. Nasr, A. Houmansadr, D. Goeckel, and D. Towsley, “Robust Adversarial Attacks Against DNN-Based Wireless Communication Systems,” in *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*, New York, NY, USA: ACM, Nov. 2021, pp. 126–140. doi: 10.1145/3460120.3484777.

[90] B. Kim, Y. E. Sagduyu, K. Davaslioglu, T. Erpek, and S. Ulukus, “Channel-Aware Adversarial Attacks Against Deep Learning-Based Wireless Signal Classifiers,” *IEEE Trans Wirel Commun*, vol. 21, no. 6, pp. 3868–3880, Jun. 2022, doi: 10.1109/TWC.2021.3124855.

[91] A. I. Newaz, N. I. Haque, A. K. Sikder, M. A. Rahman, and A. S. Uluagac, “Adversarial Attacks to Machine Learning-Based Smart Healthcare Systems,” in *GLOBECOM 2020 - 2020 IEEE Global Communications Conference*, IEEE, Dec. 2020, pp. 1–6. doi: 10.1109/GLOBECOM42002.2020.9322472.

[92] Z. Zhou *et al.*, “Model Inversion Attacks: A Survey of Approaches and Countermeasures,” Nov. 2024.

[93] S. Ennaji, F. De Gaspari, D. Hitaj, A. Kbidi, and L. V. Mancini, “Adversarial Challenges in Network Intrusion Detection Systems: Research Insights and Future Prospects,” Sep. 2024.

[94] J. Malik, R. Muthalagu, and P. M. Pawar, “A Systematic Review of Adversarial Machine Learning Attacks, Defensive Controls, and Technologies,” *IEEE Access*, vol. 12, pp. 99382–99421, 2024, doi: 10.1109/ACCESS.2024.3423323.

[95] P. Zhao, W. Zhu, P. Jiao, D. Gao, and O. Wu, “Data Poisoning in Deep Learning: A Survey,” Mar. 2025.

[96] Z. He, T. Zhang, and R. B. Lee, “Model inversion attacks against collaborative inference,” in *Proceedings of the 35th Annual Computer Security Applications Conference*, New York, NY, USA: ACM, Dec. 2019, pp. 148–162. doi: 10.1145/3359789.3359824.

[97] L. Li, “Comprehensive Survey on Adversarial Examples in Cybersecurity: Impacts, Challenges, and Mitigation Strategies,” Dec. 2024.