

Systematic Literature Review of Security and Privacy Management in LoRaWAN Networks

Kawthar Chroudi

University of Sousse

Mongi Ben Ameer

University of Sousse

Mohamed hadi Habaebi

habaebi@iiu.edu.my

International Islamic University Malaysia

Jalel Chebil

University of Sousse

Mohammed Abdulla Salim Al Husaini

Arab Open University

Jamel Bel hadj tahar

University of Sousse

Systematic Review

Keywords: Cryptographic key management, IoT security, LoRaWAN, LPWAN, Physical layer security, PRISMA, Privacy, Pseudonymization, Taxonomy

Posted Date: October 13th, 2026

DOI: <https://doi.org/10.21203/rs.3.rs-10831325/v1>

License:   This work is licensed under a Creative Commons Attribution 4.0 International License.

[Read Full License](#)

Additional Declarations: No competing interests reported.

Systematic Literature Review of Security and Privacy Management in LoRaWAN Networks

Kawthar Chroudi¹, Mongi Ben Ameer¹, Mohamed hadi Habaebi^{2*}, Jalel Chebil¹, Mohammed Abdulla Salim Al Husaini^{3*}, and Jamel Bel hadj tahar¹.

¹ NOCCS Laboratory, National Engineering School of Sousse (ENISO), University of Sousse, Sousse, Tunisia;

² Department of Electrical and Computer Engineering, International Islamic University Malaysia (IIUM), Kuala Lumpur, Malaysia;

* Correspondence: Mohamed hadi Habaebi (e-mail: habaebi@iium.edu.my); M.A.S.A (e-mail: mohammed.h@aou.edu.om).

³ Faculty of Computing Studies, Arab Open University, Muscat, Oman

Abstract

LoRaWAN, a leading Low-Power Wide-Area Network (LPWAN) technology, is widely adopted for IoT due to its wide coverage and low energy consumption, yet it remains vulnerable to multilayer security threats, including replay attacks, node tracking via static identifiers, metadata exposure, and limited cryptographic key management. This study presents a systematic literature review (SLR) following the PRISMA 2020 methodology. From 550 records identified across IEEE Xplore, ScienceDirect, SpringerLink, ACM Digital Library, MDPI, Scopus, and Google Scholar, 50 peer-reviewed studies published between 2019 and 2026 were selected using predefined inclusion and exclusion criteria. The review analyzes five research domains: cryptographic key management, privacy and pseudonymization, machine learning-based security, physical layer security, and emerging architectures such as blockchain and edge computing. It proposes a novel multi-axis taxonomy classifying existing solutions according to cryptographic strength, privacy protection, energy overhead, validation rigor, and scalability, providing a structured framework for comparison. Five major research gaps are identified, including the lack of lightweight dynamic pseudonymization schemes and automatic rekeying protocols ensuring forward and backward secrecy. Finally, the review outlines best practices and future directions, including duty cycle-aware rekeying, lightweight post-quantum cryptography, and federated or TinyML-based intrusion detection for next-generation LoRaWAN-based IoT deployments.

Keywords: Cryptographic key management; IoT security; LoRaWAN; LPWAN; Physical layer security; PRISMA; Privacy; Pseudonymization; Taxonomy.

1. Introduction

The rapid proliferation of the Internet of Things (IoT) is driving the deployment of billions of resource-constrained devices across critical domains such as smart cities, industrial automation, and connected healthcare [1]. In this context, communication technologies must simultaneously ensure scalability, energy efficiency, and reliable data transmission under strict hardware limitations [2]. Low Power Wide Area Networks (LPWANs), and particularly LoRaWAN, have emerged as a dominant solution due to their long-range communication capabilities and ultra-low power consumption [3]. However, the lightweight design of LoRaWAN introduces inherent security and privacy vulnerabilities [4]. These include exposure to replay attacks [5], device tracking and re-identification through message linkage and identifiers [6], metadata and privacy leakage and limitations in dynamic cryptographic key management [7]. Such weaknesses pose serious risks for large-scale and mission-critical IoT deployments [8].

Although extensive research has proposed various countermeasures, including cryptographic enhancements [9], [10], pseudonymization and privacy-preserving techniques [11], [12], machine learning-based intrusion and anomaly detection [13], [14], physical-layer security and authentication [13], [15], and emerging architectures such as blockchain and edge/fog computing [16], [17], existing solutions remain fragmented. Most approaches address isolated aspects of security or privacy,

without providing a unified framework capable of jointly optimizing security robustness, privacy preservation, and energy efficiency under LoRaWAN constraints [4], [8], [18].

To address this gap, this paper presents a systematic literature review (SLR) conducted in accordance with the PRISMA 2020 methodology. A total of 50 relevant studies were rigorously selected and analyzed from an initial corpus of scientific publications. The objective is to provide a comprehensive and structured synthesis of existing security and privacy mechanisms in LoRaWAN networks, while critically assessing their performance trade-offs and practical limitations.

Furthermore, this work introduces a novel multi-dimensional taxonomy that classifies solutions across key evaluation dimensions, including cryptographic strength, privacy level, energy overhead, scalability, and validation rigor. Based on this analysis, critical research gaps are identified, highlighting the lack of integrated, lightweight, and adaptive mechanisms tailored to constrained IoT environments [10], [8], [19], [18]. Finally, this study outlines promising research directions toward the design of efficient and scalable security and privacy frameworks for next-generation LoRaWAN systems.

1.1. Research questions

Four research questions structure the analytical framework of this review:

- RQ1: What are the significant privacy-preserving mechanisms protecting metadata and node identifiers in LoRaWAN networks, and how effective are they against passive adversaries?
- RQ2: How do different cryptographic and key management approaches compare with respect to forward/backward secrecy guarantees and re-keying overhead in LoRaWAN?
- RQ3: How can existing security solutions be comparatively assessed with respect to energy efficiency, latency, communication overhead, scalability, and validation evidence in constrained LoRaWAN environments?
- RQ4: What are the major research gaps and future directions in LoRaWAN security and privacy research as of 2026?

1.2. Research objectives

This study sets four primary research objectives:

To categorize and analyze the key security and privacy mechanisms proposed for LoRaWAN networks, covering cryptographic, physical-layer, ML-based, and emerging architectural approaches.

To evaluate the performance and energy-efficiency characteristics of the proposed solutions through a qualitative multi-criteria assessment of the available literature.

To investigate integration strategies addressing the inherent tension between lightweight operation and robust security guarantees.

To evaluate privacy measures and metadata protection protocols implemented in LoRaWAN security frameworks, with emphasis on identifier confidentiality and GDPR alignment.

1.3. Paper organization

The remainder of this paper is organized as follows. Section 2 presents the motivation, novelty, and contributions. Section 3 details the PRISMA 2020 methodology. Section 4 provides the technical background on IoT, LoRaWAN architecture, and identified vulnerabilities. Section 5 introduces the proposed taxonomy and classification of LoRaWAN security mechanisms. Section 6 presents the comparative evaluation and multi-criteria analysis of LoRaWAN security and privacy solutions. Section 7 defines the design requirements for secure and privacy-preserving LoRaWAN systems, maps the existing literature against these requirements, and positions this review with respect to the state of the art. Section 8 discusses the identified research gaps and future

research directions. Section 9 outlines the major challenges and best practices for secure LoRaWAN deployment. Finally, Section 10 concludes the paper.

2. Motivation, Novelty, and Contributions

The widespread deployment of LoRaWAN networks in mission-critical environments necessitates robust security frameworks. However, a significant portion of operational networks remains reliant on the LoRaWAN 1.0.x specification family, which harbors structural vulnerabilities. While LoRaWAN 1.1 introduced critical cryptographic enhancements, backward compatibility concerns and hardware replacement costs have bottlenecked its global adoption.

Existing literature reviews and surveys have explored various facets of IoT security and LoRaWAN vulnerabilities [4], [20], [21]. Yet, as summarized in Table 1, these studies exhibit structural deficiencies. Most existing works adopt a siloed approach focusing exclusively on threat taxonomies, specific cryptographic primitives, or isolated machine-learning detection systems without providing a cross-dimensional evaluation of how these mechanisms perform under strict Low-Power Wide-Area Network (LPWAN) constraints.

To address this fragmentation, this study provides a holistic, multi-dimensional analysis of the LoRaWAN security landscape. The primary novelties and contributions of this work are threefold:

Multi-Axis Taxonomy: We propose a novel, five-tier taxonomy that categorizes state-of-the-art security solutions across cryptographic, privacy-preserving, machine learning, physical layer, and emerging architectural domains.

Qualitative Benchmarking Framework: We introduce a multi-criteria evaluation matrix (Table 10) that benchmarks representative solutions across five critical dimensions: security strength, privacy preservation, energy efficiency, scalability, and validation rigor. This framework provides an objective baseline that is currently absent in the literature.

Gap-Oriented Research Roadmap: We systematically identify five critical research gaps (G1–G5), mapping each deficiency to current literature limitations and proposing actionable, constraint-aware research directions for next-generation LoRaWAN deployments. Table 1 compares representative studies and highlights the added value of this review.

Table 1. Comparison of Related Literature Reviews on LoRaWAN and IoT Security.

Ref	Year	Review Type	Number of Papers Reviewed	Target Protocol(s)	Main Focus	Main Contribution	Main Limitation
[4]	2025	Survey	Not specified	LoRa/LoRaWAN	Vulnerability taxonomy	Multi-layer attack analysis	No solution analysis, no performance comparison
[21]	2022	Review	Not specified	Generic Network IDS / Cybersecurity	ML/DL cybersecurity	Critical review of ML approaches	Limited LoRaWAN specificity
[16]	2024	A comprehensive SLR	20	Generic IoT (Blockchain-enabled IoT)	Trust management	Decentralized architecture	High energy overhead, no LoRaWAN analysis
[12]	2020	SLR	23	IoT authentication & privacy-preserving IdM protocols	Privacy identifiers	Pseudonymization taxonomy	No implementation or quantitative evaluation
[22]	2025	Survey	30	IoT communicate-on Protocols	Protocol comparison	Comparison of IoT protocols	No security depth, no

This Study	2026	SLR (PRISMA 2020)	50	LoRaWAN	Security, Privacy & Architecture	5-category taxonomy, 5-axis evaluation, research gaps	LoRaWAN research gaps
							Comprehensive multi-dimensional analysis

3. Methodology

This study follows the PRISMA 2020 (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) framework, which is the recognized standard for systematic literature reviews in engineering and computer science. The protocol ensures reproducibility, transparency, and minimization of selection bias across all phases of article identification, screening, and inclusion.

3.1. Search strategy

A systematic literature review was conducted using IEEE Xplore, sciencedirect, springerlink, ACM Digital Library, MDPI, and Scopus. Complementary searches were also performed using Google Scholar to identify additional relevant studies and ensure the completeness of the review. The search process was conducted between January 2026 and July 2026 using Boolean operators among predefined keyword sets. The PRISMA identification phase was updated in July 2026 to include the most recent eligible studies published during the review period.

3.2. Inclusion and exclusion criteria

The first set consists of network-related keywords including LoRaWAN security, LPWAN security, LoRa network privacy, and IoT LPWAN threats. The second set relates to cryptographic methods and includes key management in IoT, lightweight cryptography in LoRaWAN, AES 256 in IoT, and session key renewal. The third keyword set relates to privacy-preserving methods and includes pseudonymization in IoT, identifier privacy in LoRaWAN, metadata privacy in LPWAN, and IoT tracking. The fourth keyword set involves detection methods, which include LoRa intrusion detection, anomaly detection in IoT, machine learning-based LoRaWAN security, and RF fingerprinting in LoRa networks. Finally, the fifth keyword set includes architectural approaches such as blockchain-based IoT security, edge computing for IoT security, and federated learning in IoT settings.

Inclusion and exclusion criteria were defined a priori to ensure the scientific quality and thematic coherence of the selected corpus, as summarized in Table 2.

Table 2. Inclusion and Exclusion Criteria for Article Selection.

Code	Inclusion Criteria	Code	Exclusion Criteria
IC1	Peer-reviewed articles published in indexed journals or international conferences (IEEE, ACM, Elsevier, Springer, MDPI)	EC1	Non-peer-reviewed content: technical reports, theses, blog posts, white papers
IC2	Publication period 2019–2026; earlier studies are included only when considered foundational to the reviewed security mechanisms	EC2	Articles published before 2019 without foundational significance

IC3	Explicit treatment of LoRaWAN or constrained IoT security, privacy, or key management	EC3	Articles addressing cellular/cloud security without LoRaWAN/LPWAN component
IC4	Substantive technical, analytical, empirical, or systematic contribution supported by experimental evaluation, formal analysis, simulation, testbed validation, or systematic evidence synthesis	EC4	Articles lacking sufficient technical, analytical, empirical, or systematic evidence to support their conclusions
IC5	Full-text available in English	EC5	Articles with quality score below 3/5

3.3. Prisma 2020 selection process

The article selection process followed the four phases recommended by the PRISMA 2020 guidelines. During the identification phase, a total of 550 records were retrieved from the selected scientific databases, including IEEE Xplore, ScienceDirect, SpringerLink, ACM Digital Library, MDPI, and Scopus, while Google Scholar was used to identify additional relevant studies and ensure the completeness of the search.

During the deduplication phase, 200 duplicate records were removed, resulting in 350 unique records for screening. In the screening phase, the titles and abstracts of these records were evaluated according to the predefined inclusion and exclusion criteria, leading to the exclusion of 240 records that were unrelated to the research scope, published before the selected time period, non-peer-reviewed, or lacking sufficient relevance. Consequently, 110 articles were retained for full-text assessment.

During the eligibility phase, the full texts of the remaining articles were carefully examined. Sixty studies were excluded because they did not provide sufficient technical, analytical, empirical, or systematic evidence, did not specifically address LoRaWAN security or privacy, or lacked adequate methodological quality. Finally, 50 studies satisfied all eligibility criteria and were included in the qualitative synthesis and comparative multi-criteria analysis, as summarized in Table 3.

3.4. Quality assessment

Quality assessment criteria were set for each paper based on a grid with five parameters. Criterion Q1 (Objectives' clarity, weight 20%) analyzed whether the research questions and scope were formulated clearly enough. Criterion Q2 (Methodology, 25%) analyzed the validity and reliability of methods. Criterion Q3 (Results' validity, 25%) determined whether results were substantiated with experimental data or any other data. Criterion Q4 (Comparison to the state-of-the-art, 15%) was about comparing proposed advancements with existing ones. Criterion Q5 (Applicability, 15%) assessed the feasibility of applying proposed solutions in practical LoRaWAN networks. Papers getting less than 3 out of 5 points were eliminated at the initial stage.

Table 3. Prisma 2020 Select

PRISMA 2020 Flow Summary	
Phase 1	Identification: 550 records
Phase 2	Deduplication: 200 duplicates – 350 unique records
Phase 3	Screening: 350 records screened –240 excluded (book chapters, conference reports, pre-2019 articles) - 110 full-text assessed
Phase 4	Eligibility: 60 excluded (full-text articles with insufficient technical, analytical, empirical, or systematic evidence) - 50 studies included

Final corpus: 50 studies included (analytical core for taxonomy, gap identification, and multi-criteria comparison)

The overall study selection procedure is illustrated in Figure 1, providing a visual representation of the PRISMA 2020 workflow. The diagram presents the progression of the review through the identification, screening, eligibility, and inclusion stages, while also indicating the application of the predefined inclusion and exclusion criteria. Together with Table 3, the figure provides a complementary overview of the systematic selection process and the methodological structure adopted for the review.

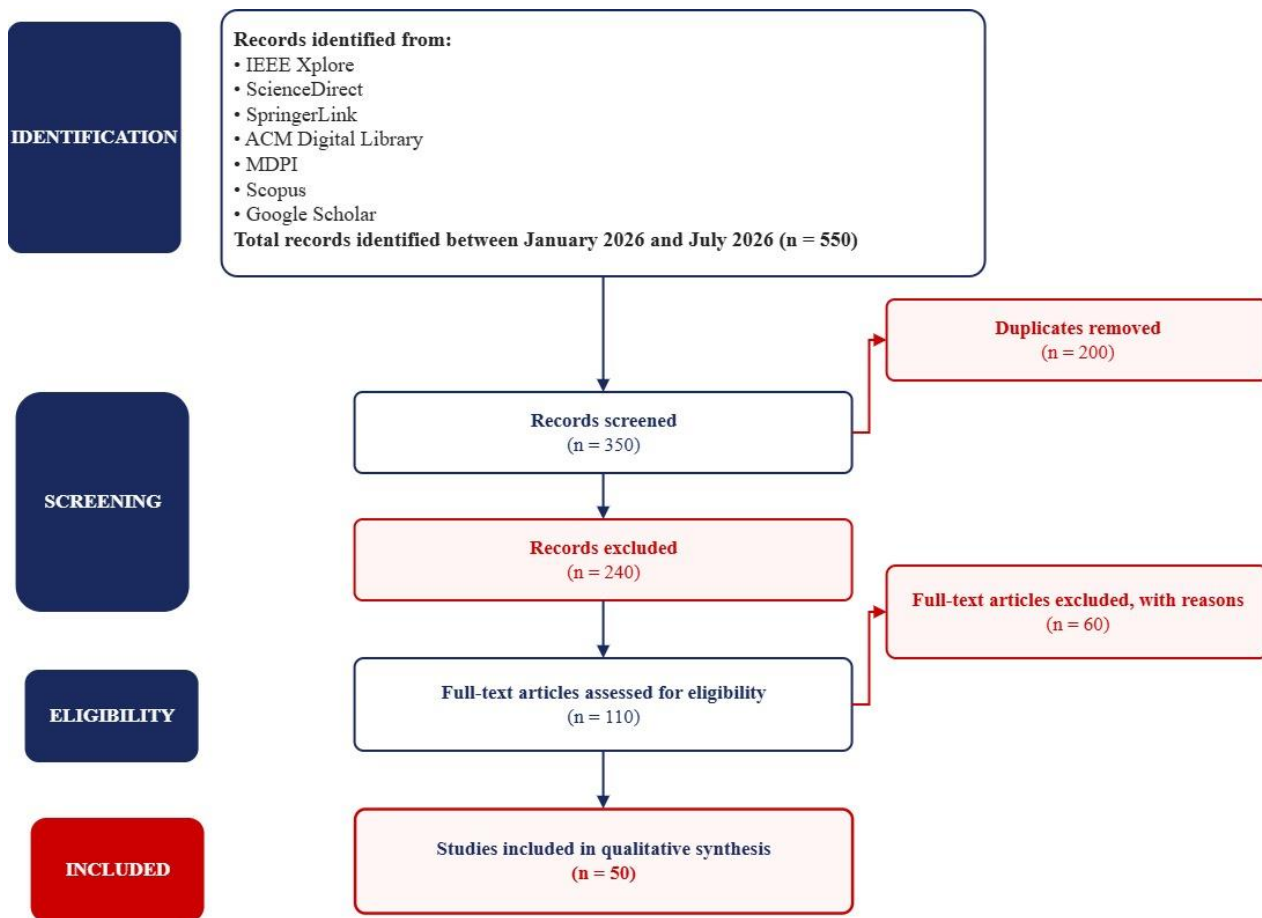


Figure 1. PRISMA 2020 flow diagram of the systematic literature review on LoRaWAN security (550 records identified; 50 studies included).

4. Technical Background

4.1. IoT and LPWAN Technologies

The Internet has transformed itself from just being an information delivery tool to being a fully-fledged technology-based infrastructure where devices can be controlled remotely, information can be gathered and analyzed, thus leading to the concept of the Internet of Things (IoT). The IoT means a collection of interconnected things or objects, communicating with each other using several protocols to exchange information and perform various tasks like monitoring, tracking, and management [23].

The major characteristic of this environment is the large number of interconnected devices through which information can be shared in domains such as health care, smart homes, industrial automation, and even national defense. However, IoT networks comprise resource-constrained nodes, which can operate on account of limitations in terms of memory, processing

capabilities, and energy constraints. Within IoT, authentication and authorization are the basic procedures that have to be implemented before the process of communication takes place [24].

LPWANs (Low Power Wide Area Networks) are wireless communication technologies designed for large-scale IoT and machine-to-machine (M2M) applications that require long-range connectivity, low data rates, energy efficiency, and low deployment costs. They are characterized by wide coverage areas, support for a large number of connected devices, low-cost hardware, and long battery lifetimes, making them suitable for applications such as smart cities, agriculture, healthcare, and logistics [25], [26]. In general, LPWAN technologies can provide coverage ranging from 1–5 km in urban environments to 10–40 km in rural areas, while maintaining low device and operating costs that facilitate large-scale IoT deployments with minimal overhead [26]. Among the main LPWAN technologies, Sigfox and LoRa operate in unlicensed ISM frequency bands and offer low-cost, low-power, and long-range connectivity. In contrast, NB-IoT, standardized by 3GPP, operates in licensed LTE bands and provides higher data rates, lower latency, and stronger quality-of-service guarantees, with data rates of up to 200 kbps. Consequently, Sigfox and LoRa are particularly suitable for applications requiring low-cost, long-life devices with infrequent data transmission, whereas NB-IoT is better suited to mission-critical IoT applications requiring higher reliability, scalability, and real-time communication capabilities [26].

This challenge led to the development of LPWAN technologies. A comparison of some LPWAN protocols is presented in Table 4. To contextualize the subsequent security analysis, this section first reviews the main characteristics of IoT and LPWAN technologies, with particular emphasis on LoRaWAN architecture, communication procedures, and inherent security constraints. This background provides the basis for understanding the security mechanisms and vulnerabilities discussed in the following sections.

Table 4. Comparative Overview of LPWAN Technologies

Technology	Range	Data Rate	Power	Frequency	Deployment
LoRaWAN	2–15 km	0.3–50 kbps	Very low (~25 mW TX)	ISM 868/915 MHz	Private / Public
NB-IoT	1–10 km	0.2–200 kbps	Low (~200 mW TX)	Licensed LTE	Operator-managed
Sigfox	10–40 km	0.1 kbps	Very low	ISM 868 MHz	Operator-managed
LTE-M	1–10 km	~1 Mbps	Moderate	Licensed LTE	Operator-managed
IEEE 802.11ah	1 km	0.15–18 Mbps	Low	ISM 900 MHz	Private

4.2. LoRaWAN Architecture and Operation

LoRaWAN adopts a star-of-stars topology consisting of three principal network components: end devices, gateways, and network servers. End devices, such as sensors and actuators, communicate with gateways through LoRa radio transmissions using different channels and data rates. Gateways act as transparent relay nodes that forward all received packets to the network server through standard IP-based backhaul technologies, including Ethernet, Wi-Fi, or cellular networks [27]. The network server represents the core intelligence of the system and performs several critical functions, including packet routing, frame deduplication, device authentication, frame counter management, acknowledgment handling, Adaptive Data Rate (ADR) control, and downlink scheduling. It also coordinates join procedures and roaming functionalities introduced in LoRaWAN v1.1. In parallel, the application server decrypts application payloads and delivers the processed information to end-user services while preserving application-level confidentiality [3], [27].

Besides providing communication services, LoRaWAN offers several built-in capabilities, including energy-efficient medium access control, channel management, GPS-free geolocation, and end-to-end security based on AES-128 encryption. The protocol employs a simple ALOHA-based access mechanism to minimize complexity and reduce energy consumption. Furthermore, LoRaWAN supports geolocation without requiring GPS hardware by exploiting Received Signal Strength Indicator (RSSI) or Time Difference of Arrival (TDOA) measurements from multiple gateways, enabling positioning accuracies ranging from approximately 20 m to 200 m depending on gateway density [27].

To accommodate diverse application requirements, LoRaWAN defines three device classes that provide different trade-offs between energy efficiency and communication latency. Class A devices, mandatory for all end nodes, are optimized for ultra-low power consumption and open two short receive windows only after an uplink transmission. Class B devices enhance downlink availability through periodically scheduled receive windows synchronized by gateway beacons, offering a compromise between latency and energy efficiency. In contrast, Class C devices maintain almost continuous listening, thereby minimizing communication delay at the expense of significantly higher power consumption [27].

Moreover, LoRaWAN incorporates an Adaptive Data Rate (ADR) mechanism that dynamically adjusts transmission parameters such as spreading factor and transmission power according to network conditions. This feature improves spectral efficiency, reduces airtime, minimizes energy consumption, and increases network capacity. Devices located closer to gateways can operate with lower spreading factors and higher data rates, thereby reducing channel occupancy and interference [27].

Finally, two activation mechanisms are available for end devices. Over-the-Air Activation (OTAA) dynamically generates fresh session keys during each join procedure, providing enhanced security and supporting roaming capabilities. Conversely, Activation by Personalization (ABP) relies on statically pre-configured session keys stored within the device, eliminating the join procedure but offering lower security and reduced flexibility. LoRaWAN security relies on AES-128 encryption and separates network-level and application-level.

Figure 2 illustrates the overall LoRaWAN architecture, highlighting the interactions between end devices, gateways, network servers, application servers, and cloud services.

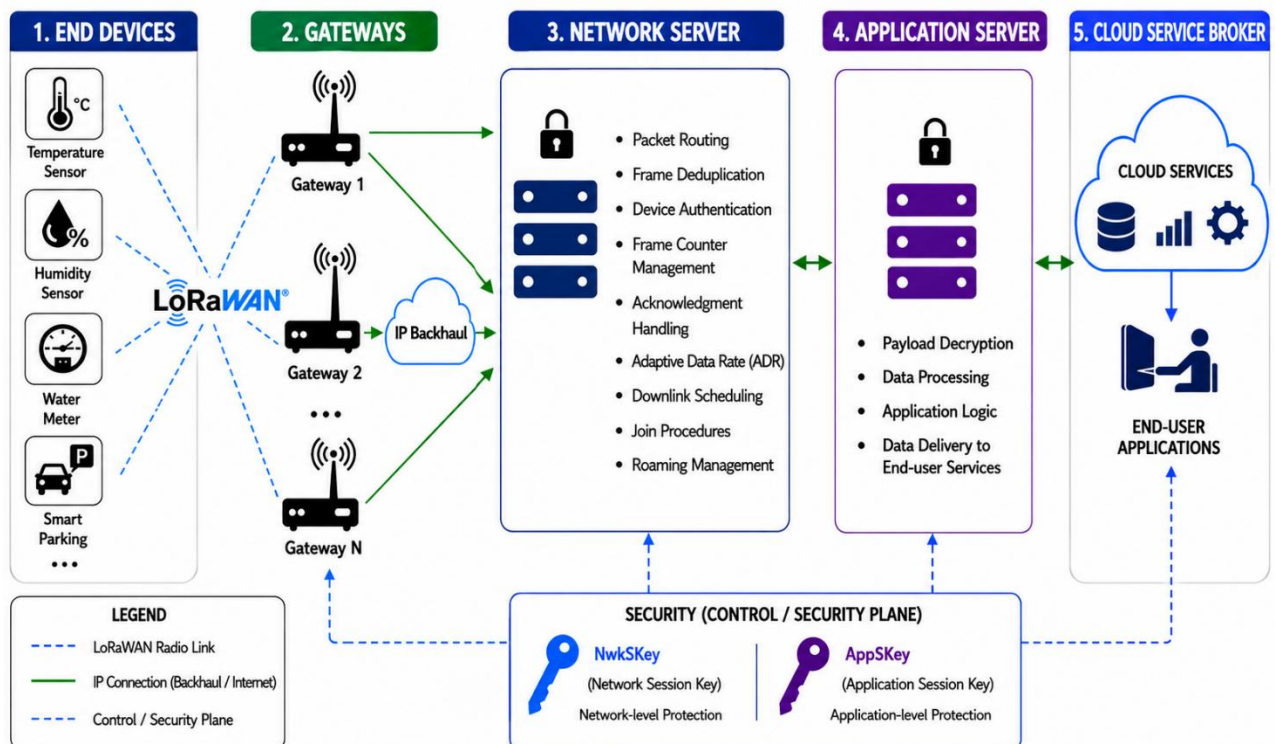


Figure 2. Secure LoRaWAN Architecture with Cloud Service Broker

4.3. Native Security Mechanisms (v1.0 and v1.1)

LoRaWAN uses a dual-key encryption scheme employing AES-128 cryptography. The Network Session Key (NwkSKey) ensures frame integrity with AES-CMAC used for the computation of Message Integrity Codes (MICs). The Application Session Key (AppSKey) provides payload confidentiality through AES-CTR encryption. In doing so, it guarantees that gateways and the network server do not have access to application messages while the application server cannot spoof network layer integrity codes [28]. Furthermore, the Network Server performs integrity verification using the NwkSKey and forwards encrypted payloads to the Application Server, which exclusively decrypts them using the AppSKey, thereby enforcing LoRaWAN's dual-layer security architecture [29].

LoRaWAN v1.1, which was standardized in 2017 and gradually adopted by industry players, offers several structural changes towards security enhancements: the NwkSKey is decomposed into three separate keys (FNwkSIntKey for uplink MIC computation, SNwkSIntKey for network-level validation, and NwkSEncKey for MAC command encryption); a dedicated Join Server is introduced to generate and distribute session keys independently from the Network Server; and the 32-bit frame counter replaces the 16-bit counter used in v1.0, greatly enhancing resilience against replay attacks [30]. In addition, version 1.1 introduces modifications to join procedures by replacing AppEUI with JoinEUI and AppNonce with JoinNonce, and supports multiple types of rejoin requests to enable secure session renewal and improved synchronization [30].

Formal security analyses have shown that several non-injective synchronization and agreement attacks affecting LoRaWAN v1.0 are mitigated in LoRaWAN v1.1 through enhanced key separation and authentication mechanisms [30]. Nevertheless, the overall security of LoRaWAN remains highly dependent on proper implementation, secure key management, and backend protection. Recent studies have highlighted practical deployment issues such as the use of static AppKeys, insecure backend APIs, and unencrypted communications between the Network Server and the Application Server, which may expose the network to replay attacks, rogue gateways, and key extraction attacks [29]. Moreover, storing AppSKey and NwkSKey inside end devices makes them vulnerable to side-channel attacks and physical node capture [29].

Despite these improvements, the structural weaknesses described in Table 5 remain in place

Table 5. LoRaWAN Vulnerability Taxonomy: Attack Categories, Layers, and Severity

Attack	Description	Layer	Severity	Key Refs.
Replay Attack	Re-transmission of captured valid frames to trigger unauthorized actions	MAC	High	[4], [28]
Node Tracking	Behavioral profiling and geolocation via static DevEUI/DevAddr identifiers in clear text	MAC / App	High	[12]
Metadata Exposure	Traffic analysis revealing activity patterns, timing, and gateway proximity without payload decryption	MAC / App	Medium	[12],[5]
Key Compromise	NwkSKey/AppSKey exposure via side-channel attacks, OTAA interception, or insecure storage	Application	Critical	[7], [28]
Jamming / DoS	Radio frequency flooding causing channel saturation and denial of service	PHY	High	[4], [3]

Spoofing / Impersonation	Identity impersonation via forged frames mimicking legitimate device signatures	MAC	High	[4], [13]
Wormhole Attack	Malicious relay creating tunnels between distant network nodes, bypassing geographic constraints	Network	Medium	[4]

Note on Severity Classification: Severity ratings in Table 5 are defined based on systemic impact and exploitability:

- **Critical:** Direct and complete compromise of cryptographic material or hardware integrity across deployed nodes, leading to full network exposure (e.g., key extraction, physical node capture).
- **High:** Active protocol manipulation, payload injection, or total service disruption without immediate key extraction (e.g., replay attacks, RF jamming, device impersonation).
- **Medium:** Passive information leakage, metadata exposure, or localized performance degradation without direct compromise of encrypted payload content (e.g., node tracking, ADR manipulation, wormhole attacks).

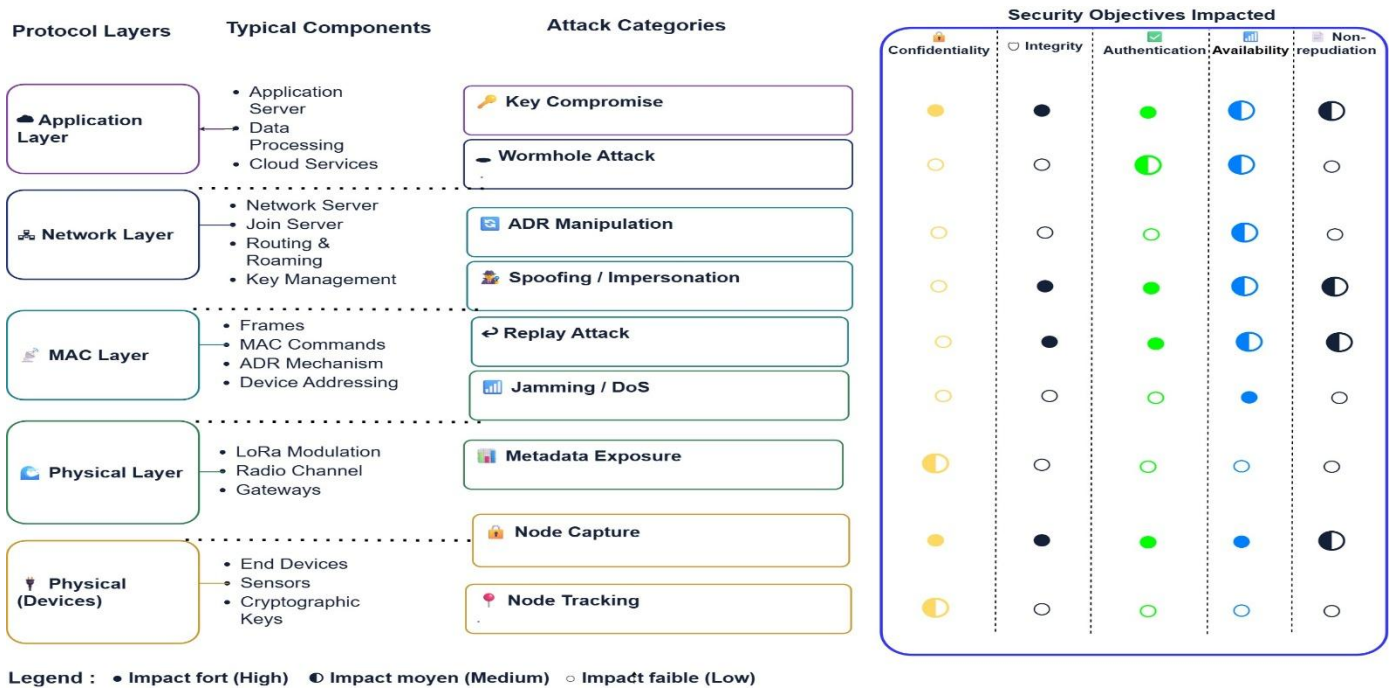


Figure 3. Layered Classification of LoRaWAN Attacks and Their Impact on Security Objectives

To provide a unified view of the LoRaWAN threat landscape, it is essential to organize attacks according to their corresponding protocol layers and their impact on fundamental security objectives. While existing analyses often describe vulnerabilities in isolation, a layered representation enables a clearer understanding of how different attack vectors target specific components of the system and compromise properties such as confidentiality, integrity, availability, authentication, and non-repudiation, as illustrated in Figure 3. Recent surveys emphasize that, although LoRaWAN employs robust AES-based cryptographic mechanisms, practical security depends not only on encryption but also on secure bootstrapping procedures, key lifecycle management, trusted gateways, backend infrastructure protection, and resilience against physical-layer attacks such as jamming and traffic analysis [30], [29].

5. Taxonomy and Classification of Security Mechanisms

Accordingly, based on the results of the systematic review of the 50 papers, we present a five-category taxonomy of security solutions for LoRaWAN. The taxonomy is based on the nature of the security approach and the corresponding layer of the LoRaWAN protocol. To ensure a consistent classification, each of the 50 selected studies was assigned to a single primary category according to its main research contribution. Although several studies address multiple aspects of LoRaWAN security, only the dominant contribution was considered for the taxonomy in order to avoid double counting. The resulting taxonomy, including the main security categories, the targeted protocol layers, and the primary mechanisms adopted by the reviewed studies, is presented in Table 6.

To complement the proposed taxonomy, Table 7 presents a qualitative mapping between the identified security countermeasure categories and the major security threats. The comparison illustrates the relative contribution of each category to mitigating replay attacks, tracking, metadata exposure, cryptographic key compromise, and jamming. Rather than replacing the taxonomy, this mapping complements it by highlighting the security coverage, strengths, and limitations of each category across different threat classes.

Three distinct security paradigms are also considered. Reactive approaches detect and respond to attacks after they occur. Proactive approaches aim to prevent attacks through mechanisms such as authentication and encryption. Hybrid approaches combine both prevention and detection capabilities. These paradigms provide an additional perspective for analyzing the reviewed security solutions in terms of energy consumption, security level, scalability, and validation processes. This complementary classification of security paradigms constitutes an additional contribution of the present work.

TABLE 6. Proposed Taxonomy of LoRaWAN Security Mechanisms

Category	Studies	Target Layer	Primary Mechanism
Cryptography & Key Management	[1], [5], [7], [8], [9], [10], [28], [31], [32], [19], [33], [34]	MAC / Application	Symmetric encryption, hierarchical key derivation, session re-keying
Privacy & Pseudonymization	[6], [11], [12], [35], [36], [37], [38], [39]	MAC / Application	Dynamic identifiers, anonymization, metadata obfuscation
Machine Learning Security	[14], [21], [40], [41], [42], [43], [44], [45], [46], [47]	Application / Cross-layer	IDS, anomaly detection, classification, RF fingerprinting with ML
Physical Layer Security	[13], [15], [18], [48], [49], [50], [51]	PHY	Channel-based key generation, RF fingerprinting, CSS properties
Emerging Architectures	[3], [4], [16], [17], [20], [22], [52], [53], [54], [55], [56], [57], [58]	Cross-layer	Blockchain, edge/fog computing, federated security offloading

TABLE 7. Qualitative Mapping of Security Countermeasure Categories Against Major Security Threats

Category	Replay	Tracking	Metadata	Key Compromise	Jamming
C1: Cryptography & Key Management (KMS)	●	○	○	●	–
C2: Privacy & Pseudonymization	–	●	●	–	–

Category	Replay	Tracking	Metadata	Key Compromise	Jamming
C3: Machine Learning-based Security	●	–	○	–	●
C4: Physical Layer Security	–	○	–	○	●
C5: Emerging Architectures	●	●	–	●	–

Legend: ● *Primary defense* ● *Secondary / partial defense* ○ *Indirect defense*
– *Not applicable*

5.1. Cryptography and Key Management

Cryptography represents the core security foundation of LoRaWAN, ensuring confidentiality, integrity, and authentication through the AES-128 mechanism. However, several limitations remain, including static key deployment, limited forward secrecy, and the absence of efficient automatic re-keying mechanisms. To address these issues, the feasibility of replacing AES-128 with AES-256 on ARM Cortex-M based LoRaWAN devices has been investigated. The results showed that AES-256 introduces only a moderate computational overhead without increasing communication overhead, demonstrating that stronger cryptography can still be practical for constrained IoT environments [9].

Regarding key management, a lightweight hierarchical key derivation and periodic renewal scheme compatible with LoRaWAN 1.1 has been proposed, enabling partial re-keying while reducing communication overhead and improving forward secrecy [7]. Similarly, a secure session key generation method based on one-way cryptographic functions and server-side entropy injection has been introduced to strengthen OTAA join security without requiring modifications on end devices [28].

Recent research has also focused on lightweight cryptographic primitives suitable for resource-constrained IoT devices [59]. A lightweight cryptographic hash function based on the New Mersenne Number Transform (NMNT) and sponge construction has been proposed to support variable block sizes and configurable digest lengths [59]. Experimental evaluations performed on Contiki OS using the Cooja simulator showed that the proposed scheme requires less memory and lower power consumption than several existing lightweight hash functions while exhibiting favorable computational efficiency [59]. Statistical analyses further demonstrated strong diffusion and confusion properties, successful NIST randomness tests, and resistance against collision, pre-image, birthday, differential, and meet-in-the-middle attacks [59].

The analysis also highlights the growing importance of re-keying mechanisms in LoRaWAN. Existing approaches include time-based, event-driven, and hybrid re-keying strategies, each offering different trade-offs between security, adaptability, and communication overhead [7]. Nevertheless, LoRaWAN constraints such as duty-cycle limitations, uplink-dominant communication, and synchronization issues make conventional explicit re-keying protocols difficult to deploy efficiently [7].

To overcome these limitations, recent studies have explored lightweight and implicit re-keying mechanisms, including hierarchical key derivation, key evolution through hash functions, and piggybacking techniques [7]. These methods significantly reduce signaling overhead while maintaining forward secrecy and improving resilience in constrained environments [7]. In addition, lightweight cryptographic primitives characterized by low memory requirements, reduced power consumption, variable digest lengths, and strong resistance against cryptanalytic attacks have emerged as promising solutions for resource-constrained IoT systems [59]. Overall, the conducted taxonomy suggests that implicit and hybrid re-keying approaches offer an effective compromise between security, efficiency, and communication cost in LoRaWAN networks [7].

5.2. Privacy and Pseudonymization

Privacy in LoRaWAN is threatened by the transmission of static identifiers such as DevEUI, AppEUI, and DevAddr in plaintext within packet headers [12]. Even when payloads are protected using strong encryption schemes, attackers can still perform tracking, device profiling, and location inference through passive traffic analysis [12]. Therefore, identifier protection mechanisms are required in addition to traditional cryptography [12]. Akil et al. [12] proposed a taxonomy of pseudonymization approaches for IoT systems, including static pseudonymization, dynamic pseudonymization, and unlinkability-based schemes [12]. Static pseudonymization provides limited protection because identifiers remain constant over time, whereas dynamic pseudonymization periodically changes identifiers to reduce long-term tracking risks [12]. Unlinkability-based approaches offer stronger privacy by assigning random identifiers for each session, although they introduce higher management complexity [12]. Ahmed et al. [35] proposed a Privacy-by-Design framework for IoT and 5G systems based on data minimization, temporal obfuscation, and traffic shaping principles that can also be adapted to LoRaWAN environments [35]. Complementary techniques such as dummy traffic generation [38] and randomized transmission scheduling [6] were also suggested to reduce traffic analysis risks, despite their additional energy consumption [38], [6].

The analysis distinguishes two main dynamic pseudonymization strategies in LoRaWAN: periodic identifier rotation and event-driven rotation [12]. Periodic rotation updates identifiers at fixed intervals, providing predictable privacy protection but lacking adaptability to changing traffic conditions [12]. Event-driven rotation updates identifiers according to network activity or security events, improving adaptability but increasing signaling and synchronization complexity [12]. A major challenge in both approaches is desynchronization between end devices and the network server, particularly because LoRaWAN Class A devices rarely receive downlink messages [12]. Packet losses, transmission delays, and duty-cycle restrictions may therefore lead to synchronization failures and packet rejection [12]. To address this issue, lightweight resynchronization techniques have been proposed, including predictive identifier generation based on shared cryptographic functions and sliding window verification, as well as implicit synchronization through uplink messages [12].

Finally, the proposed LoRaWAN-specific taxonomy classifies pseudonymization schemes into static, periodic, event-driven, predictive/deterministic, and hybrid approaches [12]. The analysis concludes that predictive and hybrid pseudonymization mechanisms are the most promising solutions for LoRaWAN because they provide stronger privacy guarantees while remaining compatible with the network's resource and communication constraints [12]. In line with the privacy by design paradigm, Akram et al. [60] introduced a lightweight authentication protocol integrating physically unclonable functions (PUFs) to eliminate static key storage and enhance resilience against device cloning and key extraction [60]. This protocol demonstrates that privacy can be embedded at the architectural level, combining anonymity, mutual authentication, and energy efficiency, thereby offering a practical instantiation of privacy by design principles in LoRaWAN [60].

Traditional pseudonymization approaches such as static pseudonymization [12] and dummy traffic generation [38] provide partial protection but suffer from long-term traceability and high energy overhead [12], [38]. Dynamic pseudonymization [12] and randomized scheduling [6] improve adaptability but introduce synchronization challenges and latency [12], [6]. In contrast, Privacy-by-Design frameworks [35] emphasize systemic principles like data minimization and traffic shaping, which can be adapted to LoRaWAN but remain resource-intensive [35]. The PUF-based lightweight authentication protocol [60] represents a significant advancement by embedding privacy directly into the hardware and protocol design, eliminating static identifiers, and ensuring resilience against physical and cryptographic attacks [60]. This comparative analysis highlights that while classical methods mitigate specific risks, privacy by design solutions such as PUF-based authentication offer holistic protection by combining privacy, security, and efficiency in a single architectural framework [60].

Moreover, it is important to note that authorization has not yet been studied in the context of LoRaWAN. According to [61], authorization in IoT security refers to restricting actions and operations that authenticated users can perform, thereby preventing safety breaches through enforced user restrictions. While authentication mechanisms in LoRaWAN have been explored, the dimension of authorization deciding what a device or user is allowed to do once authenticated remains an open research challenge [61].

5.3. Machine Learning-Based Security

Machine learning (ML) and deep learning (DL) techniques have become important approaches for detecting security threats in IoT and LoRaWAN networks because of their ability to identify complex attack patterns and zero-day attacks that traditional signature-based systems cannot detect [21]. Salas et al. [40] proposed a lightweight Deep Neural Network (DNN) framework for IoT attack detection using the CIC-BCCC-NRC TabularIoTAttack-2024 dataset, achieving a high F1-score of 0.997 for binary attack classification and 0.977 for multiclass classification [40]. The study introduced a z-filter pruning algorithm to remove outliers and optimize the model for edge computing, with results showing that pruning reduced inference memory consumption by up to 40% while causing less than 0.3% reduction in the F1-score [40]. The proposed DNN architecture incorporates batch normalization after each hidden layer's linear response, a z-filter to remove response components with z-score greater than the defined z-threshold (effectively eliminating noisy data and outliers through training epochs), Leaky-ReLU activation function to prevent dead neurons, and a dropout sublayer to reduce overfitting [40]. The decision-maker calculates the mean probability of the selected categories for each observation, and if this value is higher than or equal to 0.90, it selects this output as the predicted categories; otherwise, it stores the model in a buffer and reduces the z-threshold by 0.25 to retrain with a lower threshold [40]. The study also implemented binary and standalone multiclass classifiers using traditional ML algorithms including Decision Tree, Random Forest, Support Vector Machine, Linear Discriminant Analysis, and Gaussian Naive Bayes, with the DNN achieving statistically significantly higher performance than traditional ML classifiers in both cases, as confirmed by the unidirectional Wilcoxon rank-sum test with p-values lower than the significance level of 0.01 [40]. The mean inference times for simulated normal traffic and reconnaissance attacks were consistently low, with vulnerability scan attacks resulting in the highest mean inference time at 12.583 ms for the secure virtual IoT device and 11.148 ms for the insecure device, demonstrating the lightweight nature of the proposed DNN and its suitability for deployment in gateways and edge-based IoT environments [40]. However, the evaluation relies exclusively on the CIC-BCCC-NRC TabularIoTAttack-2024 dataset, which only captures traffic patterns at the transport layer, and as acknowledged by the authors, future datasets could be improved by including traffic patterns from lower layers such as the data link layer [40]. Similarly, the authors note that the dataset is based on traffic pattern recognition at the transport layer level, and future datasets should include traffic patterns from lower layers, such as the Address Resolution Protocol (ARP) corresponding to general scan attacks for finding open ports [40]. Pourghasem et al. [13] developed a multi-attribute machine learning approach for detecting spoofing attacks in LoRaWAN at the physical layer, using four radio-frequency features RSSI, SNR, frequency offset, and timing offset combined through an ensemble classifier, achieving more than 95% detection accuracy without requiring modifications to the LoRaWAN protocol stack [13]. Their solution ensures backward compatibility and avoids additional communication overhead, with the authentication process performed entirely at the gateway side, introducing no computational overhead on end devices [13]. The study evaluated ML models including Logistic Regression, Random Forest, and K-Nearest Neighbors, and DL models including Multi-Layer Perceptron and Convolutional Neural Networks, with Random Forest achieving the highest accuracy among ML models (83.74%), while MLP and CNN delivered competitive performance with higher resource demands [13]. The feature importance analysis using Random Forest identified battery level as the most significant attribute (44.81%), followed by altitude (32.22%) and RSSI (22.86%), reinforcing the importance of combining dynamic and static physical-layer attributes for effective spoofing detection [13]. The computational efficiency analysis revealed that while ML models like Logistic Regression and K-Nearest Neighbors are lightweight with training times as low as 0.002 seconds and memory usage as low as 0.12 MB, DL models such as MLP require 26.3 MB of memory and 1.83 seconds training time, making them impractical for edge deployment on LoRaWAN Class A devices without significant optimization [13]. Halbouni et al. [21] analyzed the challenges of applying ML and DL techniques to IoT cybersecurity in resource-constrained environments, identifying several limitations including inference latency between 10 and 100 ms, high memory requirements ranging from 4 to 64 MB for standard DNN models, and the lack of interpretability in deep learning decisions [21]. These constraints make deploying complex ML/DL models difficult on LoRaWAN Class A devices, which typically provide only 256 KB of RAM [21]. Halbouni et al. [21] further emphasized that deep learning models require high processing power and that a major challenge for intrusion detection systems is maintaining an up-to-date dataset with sufficient records to cover the majority of attack types [21]. The review also identified that datasets not based on reality may result in mistaken studies, and that IDS models face significant challenges when implemented in real-world environments, as models developed in laboratories should be validated in real-world conditions to ensure their efficiency [21]. The study also highlighted that the interpretability of deep learning models remains a challenge, as it is difficult to specify how neurons should be modeled and how the layers should interact, making it difficult to explain how the result was obtained [21]. Pourghasem et al. [13] acknowledged that while their multi-attribute approach combining RSSI, battery level, and altitude is promising, the battery level and altitude attributes were synthesized

rather than collected from real deployments, which may affect generalizability to practical scenarios [13]. The authors also noted that their proposed PLA scheme introduces additional processing at the Application Server level, which may increase latency a critical factor for time-sensitive IoT applications yet they did not quantify this latency impact [13]. The study further acknowledged that the experimental distances were limited to a specific range, and while the range was sufficient to expose line-of-sight and interference effects, LoRaWAN typically operates over multiple-kilometer links, which warrant exploration in future works [13]. The study also noted that the proposed scheme's performance under varying environmental conditions that could affect RSSI readings, such as weather changes, seasonal foliage variations, or moving obstructions, was not evaluated [13]. Finally, both studies acknowledge that current datasets and evaluation methodologies have limitations, including the absence of traffic patterns from lower protocol layers and the need for validation in real-world LoRaWAN deployments rather than laboratory or simulated environments [13], [21], [40].

5.4. Physical Layer Security

Physical Layer Security (PLS) techniques rely on inherent wireless channel characteristics, such as reciprocity, spatial decorrelation, and temporal variation, to provide lightweight security mechanisms without depending on computationally expensive cryptographic algorithms [20], [21], [52]. These methods are particularly suitable for LoRaWAN devices due to their limited computational and energy resources [11]. PLS leverages the unique physical properties of the wireless channel, including temporal and spatial characteristics, to enable the mapping of diverse locations with varying spatiotemporal environmental factors [61]. Unlike traditional cryptographic approaches that rely on computational hardness assumptions, PLS exploits the randomness, reciprocity, and spatial decorrelation of wireless channels to enable secret key generation between legitimate devices [61]. The fundamental premise of PLS is that the wireless channel between two communicating parties exhibits reciprocal properties, meaning that the channel characteristics measured at one end are highly correlated with those measured at the other end, while an eavesdropper at a different location experiences statistically independent channel conditions [61]. This spatial decorrelation ensures that only legitimate users sharing the same propagation environment can extract correlated channel features, whereas unauthorized nodes cannot obtain the same information [61]. Additional physical layer parameters, such as node temperature, battery level, Received Signal Strength Indicator (RSSI), and Link Quality Indicator (LQI), can enhance the ability to make more precise decisions for authentication and authorization processes [61]. PLS techniques have been identified as viable solutions for future communication networks, including IoT networks, as they can be incorporated into the communication stack with standard physical layer characteristics without requiring significant changes to existing protocol stacks, thereby adding an additional layer of security [61].

Anisah et al. [49] introduced LoRa-PRIME, a secret key generation framework based on channel reciprocity between communicating devices. The framework incorporates two main mechanisms: a Periodic Bit Reversal (PRK) technique to improve key randomness by alternating bit extraction patterns, and a Modified Adaptive Quantization (ADQ) algorithm that dynamically adapts quantization thresholds according to local channel conditions [49]. Designed for cooperative LoRa relay networks, the scheme achieved key generation overheads below 5% of normal transmission overhead and bit error rates lower than 0.01 in static channel environments [49]. The approach enables cryptographic-grade key generation without requiring modifications to higher-layer LoRaWAN protocols [49]. Experimental evaluations conducted under indoor LOS, indoor NLOS, and outdoor NLOS scenarios demonstrated that the 4-bit modified ADQ achieved key agreement rates up to 0.9745 and key generation rates up to 33.04 bps, outperforming existing Sky-Glow quantization methods [49]. The proposed PRK mechanism improved randomness quality, increasing the number of NIST-compliant keys from 4 to 14 in indoor LOS scenarios [49]. However, several limitations must be acknowledged. The security evaluation assumes a passive eavesdropper model and does not consider active adversaries capable of injecting malicious signals or performing man-in-the-middle attacks during the channel probing phase [49]. The experimental validation was conducted with devices positioned at relatively short distances within a laboratory and parking lot environment, and the framework's performance over extended LoRa communication ranges (multiple kilometers) has not been verified [49]. The channel probing phase dominates the overall execution time, contributing more than 85% of the total runtime, which may limit the framework's applicability in highly mobile or time-varying channel environments where rapid key renewal is required [49]. The energy consumption measurement of 6.619 J per key, while lower than several reported implementations, is based on an estimated execution time scaled from a laptop processor to an ESP32 using a frequency ratio, without direct measurement on the target hardware, introducing potential inaccuracies [49]. The PRK mechanism is deterministic and only rearranges existing bits rather than

generating new entropy, which means it cannot compensate for fundamental weaknesses in the initial channel entropy source [49]. The study acknowledges that NIST tests requiring longer input sequences, such as Maurer's Universal Statistical Test and Linear Complexity Test, were not applicable due to the 256-bit key length, leaving certain randomness aspects unevaluated [49]. The relay-assisted architecture introduces additional security concerns regarding the semi-trusted relay, and while cooperative jamming reduces the relay's ability to reconstruct the key, the authors do not provide a formal security proof or quantitative analysis of the information leakage to the relay [49].

RF fingerprinting techniques exploit hardware imperfections in LoRa transceivers, such as variations in oscillators, power amplifiers, and analog-to-digital converters, to create unique device signatures for authentication purposes [10], [15]. These hardware-based characteristics are difficult to reproduce, making RF fingerprinting an effective complement to traditional protocol-layer security mechanisms [10], [13].

Pourghasem et al. [13] extended their machine learning-based spoofing detection framework to propose a multi-attribute physical layer authentication scheme. Their method combines four signal features RSSI, SNR, carrier frequency offset, and timing advance deviation—through an ensemble machine learning classifier [13]. Experimental results demonstrated authentication accuracy above 95% under laboratory conditions [13]. In addition, the authentication process is entirely performed at the gateway side, introducing no computational overhead on end devices and maintaining full backward compatibility with existing LoRaWAN deployments [13]. The study evaluated ML models including Logistic Regression, Random Forest, and K-Nearest Neighbors, and DL models including Multi-Layer Perceptron and Convolutional Neural Networks, with Random Forest achieving the highest accuracy among machine learning models (83.74%) [13]. Feature importance analysis identified battery level as the most significant attribute (44.81%), followed by altitude (32.22%) and RSSI (22.86%) [13]. However, several critical limitations warrant consideration. The authentication accuracy above 95% is reported only under controlled laboratory conditions, and the performance under realistic deployment scenarios with environmental variations, such as weather changes, seasonal foliage, or moving obstructions that could affect RSSI and SNR, has not been evaluated [13]. The dataset used in the study is only partially real-world; while RSSI values are sourced from the LoED dataset, battery level and altitude are synthesized rather than collected from actual sensor deployments [6], [13]. This raises concerns about the generalizability of the results to practical scenarios where battery consumption patterns and altitude variations may differ significantly [13]. The computational efficiency analysis reveals that while ML models like Logistic Regression are lightweight (0.80 MB memory, 0.002 s training time), DL models such as MLP require 26.3 MB of memory far exceeding the typical 256 KB RAM available on LoRaWAN Class A devices making them impractical for edge deployment without significant optimization [13]. The study does not evaluate the scheme's performance under varying environmental conditions that could affect RSSI readings, such as weather changes, seasonal foliage variations, or moving obstructions [13]. The proposed scheme introduces additional processing at the Application Server level, which may increase latency a critical factor for time-sensitive IoT applications yet the authors do not quantify this latency impact [13]. The study acknowledges that the experimental distances were limited to a specific range, and while the range was sufficient to expose line-of-sight and interference effects, LoRaWAN typically operates over multiple-kilometer links, which warrant exploration in future works [13]. The feature importance analysis, while identifying battery level as the most influential attribute, does not address how an attacker could potentially manipulate or spoof battery level readings, nor does it discuss the practical challenges of accurately measuring battery level in heterogeneous sensor deployments [13]. The authors note that future datasets could be improved by including traffic patterns from lower layers, such as the data link layer, but do not address how the proposed scheme would perform if such lower-layer data were incorporated or if attackers exploited vulnerabilities at those layers [13]. Finally, the study does not consider adaptive adversaries that could gradually adjust their physical attributes to evade detection over time, representing a significant gap in the security evaluation [13]. Taken together, while both studies demonstrate promising approaches for physical layer security in LoRaWAN, their limitations highlight the need for real-world validation, consideration of active adversary models, and optimization for resource-constrained edge deployment [49], [13].

5.5. Emerging Architectural Approaches

The advantages of blockchain-based security include decentralized identity management, immutable audit logs, and distributed key storage for IOT and LoRaWAN applications. Almarri et al [16] conducted an analysis of 47 studies and highlighted the significant potential of blockchain technology for strengthening IoT security. However, they also identified

several barriers to its practical adoption, including scalability limitations, interoperability issues among heterogeneous IOT platforms, high computational and storage requirements, and the lack of standardized frameworks for blockchain integration. existing blockchain technologies also present significant challenges when deployed in LoRaWAN due to latency and energy consumption constraints. For example, ethereum's proof of work (pow) consensus introduces delays exceeding 10 seconds, making it unsuitable for delay-sensitive LoRaWAN applications. Although permissioned blockchain platforms such as hyperledger fabric and iota tangle mitigate some latency and energy issues, large-scale deployment remains challenging. Merrad et al [62] further analyzed the performance of major blockchain consensus algorithms by comparing their security properties, scalability, energy efficiency, throughput, latency, and decentralization trade-offs. Their review demonstrates that the choice of the consensus mechanism is a determining factor in the overall performance of blockchain-based systems. Nevertheless, a critical analysis of both studies reveals that blockchain cannot yet be considered a universal security solution for LoRaWAN. existing consensus mechanisms inevitably sacrifice one or more desirable properties to improve others. While pow provides strong security guarantees and high data integrity, it suffers from excessive energy consumption, limited transaction throughput, long confirmation delays, and vulnerability to issues such as mining centralization and 51% attacks. conversely, alternative consensus mechanisms, including proof of stake (pos), practical byzantine fault tolerance (pbft), and permissioned blockchain frameworks, improve throughput and significantly reduce energy consumption but often rely on stronger trust assumptions, reduced decentralization, or increased communication complexity. Furthermore, the computational, storage, and communication overhead required to execute blockchain consensus remains incompatible with the constrained resources of LoRaWAN end devices, particularly battery-powered sensors. Consequently, blockchain-based security is currently more appropriate for deployment at gateways, edge/fog nodes, or cloud infrastructures, where sufficient computational resources are available. These findings suggest that blockchain should be regarded as a complementary security layer rather than a standalone solution for LoRaWAN. future research should therefore focus on lightweight consensus mechanisms, hybrid blockchain architectures, and resource-aware security frameworks capable of jointly optimizing security, scalability, latency, and energy efficiency in large-scale LoRaWAN deployments. Nia and Jha [20] introduced a multi-level edge/fog computing security system where computationally expensive security tasks, such as cryptographic functions, anomaly detection, and key exchange management, are delegated to edge devices placed close to LoRaWAN gateways. In this way, the end devices can benefit from more powerful edge resources while ensuring end-to-end security. Their architecture is particularly suitable for LoRaWAN gateways since they have greater computational resources compared to class a device. Despite these advantages, the proposed architecture introduces additional infrastructure complexity and relies heavily on the availability and trustworthiness of edge/fog nodes. furthermore, the study does not comprehensively evaluate scalability, resource management, or the resilience of the system under large-scale LoRaWAN deployments.

5.6. Taxonomy vs. Threat Model Mapping Matrix

To evaluate the practical applicability of the proposed taxonomy, the five security categories (C1: Cryptography & Key Management, C2: Privacy & Pseudonymization, C3: Machine Learning-Based Security, C4: Physical Layer Security, and C5: Emerging Architectures) are mapped against the operational profiles of LoRaWAN device classes (Class A, Class B, and Class C) and their target threat models.

Class A End-Devices (Resource-Constrained Edge): Characterized by battery-powered operation and severe downlink limitations, Class A devices can only support lightweight primitives from C1 (e.g., AES-256 optimizations [9] or implicit re-keying schemes [7], [28] and low-overhead mechanisms from C2 (e.g., PUF-based dynamic identification [61]). High-level ML models (C3) or heavy blockchain mechanisms (C5) are impractical at this level due to severe memory limitations (RAM ≤ 256 KB) and processing latency overheads [21].

Class B End-Devices (Periodic Synchronized Operations): Supporting scheduled receive windows, Class B devices are suitable for synchronized lightweight re-keying schemes (C1) [7], periodic identifier updates and dynamic pseudonymization (C2) [12], and cooperative physical-layer channel probing (C4) such as secret key generation using channel reciprocity [49].

Class C & Infrastructure Nodes (Mains-Powered / Gateways & Servers): Mains-powered Class C nodes, edge gateways, and network/application servers possess sufficient energy and computational capacity to execute complex ML-based

intrusion and spoofing detection systems (C3) [40], [21], [13], compute-intensive Physical Layer Security analyses (C4) [10], [13], and decentralized blockchain consensus or security offloading frameworks (C5) [20], [16], [62].

TABLE 8. Mapping of Security Taxonomy Categories (C1–C5) Across LoRaWAN Operational Profiles

Security Category (Section V)	Primary Target Layer	Target Threat Model / Attacks Mitigated	Suitable LoRaWAN Device Class / Deployment Target	Implementation Feasibility / Resource Constraints	References
C1: Cryptography & Key Management	MAC / Application	Key Compromise, Replay Attacks, Impersonation	Class A, B, C (End-devices & Backend)	High: Lightweight AES/hash schemes suit Class A; dynamic rekeying mainly for Class B/C.	[7], [9], [28], [59]
C2: Privacy & Pseudonymization	MAC / Application	Node Tracking, Metadata Exposure, Eavesdropping	Class A, B, C (End-devices & Network Server)	High: PUF/predictive schemes for Class A; synchronized rotation for Class B/C.	[6], [12], [32]/[34], [35], [37]/[38], [61]
C3: Machine Learning Security	Application / Cross-layer	Anomaly Detection, Jamming/DoS, Spoofing	Gateways, Edge & Cloud	Medium–Low on end devices; inference offloaded to gateways/edge.	[13], [21], [40]
C4: Physical Layer Security (PLS)	PHY	Spoofing, Impersonation, Eavesdropping, Node Capture	Class A, B, C & Gateways	High at gateway side; minimal end- device overhead.	[10], [11], [13], [15], [20], [21], [52], [49], [61]
C5: Emerging Architectures	Cross-layer / System-wide	Unauthorized Access, Data Tampering, Single Point of Failure	Gateways, Fog Nodes, Network Servers	Infrastructure- only; consensus and audit logging at Edge/Cloud.	[16], [20], [62]

6. Comparative Evaluation and MultiCriteria Analysis of LoRaWAN Security and Privacy Solutions

6.1. Detailed Comparison of Included Studies

This section provides a technical comparative analysis of the selected LoRaWAN security solutions, evaluating each approach in terms of underlying mechanisms, targeted layers, and practical constraints. The analysis highlights key trade-offs between security strength, privacy preservation, energy overhead, and scalability, while exposing the fragmentation of existing approaches and their limited integration across multiple dimensions. The detailed comparison of contributions and limitations is summarized in Table 9.

TABLE 9. Comprehensive Synthesis of 50 Representative Studies on LoRaWAN Security and Privacy (2019–2026)

Ref	Year	Category	Objective	Technique	Advantages	Limitations
[4]	2025	Survey	Multi-layer vulnerability analysis	Systematic review	Global threat perspective	No solution proposed
[48]	2022	Survey	Analyze vulnerabilities, attacks, countermeasures, and security-enhancing techniques at the LoRaWAN physical layer	Comprehensive literature review and state-of-the-art analysis	Comprehensive coverage of physical-layer vulnerabilities and protection mechanisms; identifies research gaps and future directions	Focused on physical-layer security, limited practical deployment evaluation
[40]	2025	ML / IDS	IoT attack detection	DNN + z-filter pruning	F1=0.997; edge-deployable	Dataset specificity; end-device infeasible
[9]	2023	Cryptography	AES-256 for LoRaWAN	ARM Cortex-M implementation	Feasibility confirmed; +15–30% CPU	No forward secrecy; simulation only
[35]	2024	Privacy	Privacy-by-Design for 5G/IoT	Metadata minimization	GDPR alignment	Not LoRaWAN-specific
[20]	2023	Framework	Multi-layer security	Edge offloading	Reduces end-device burden	Infrastructure required
[21]	2022	ML Review	ML/DL barriers for IoT	Critical literature analysis	Deployment barrier quantification	No quantitative LoRaWAN comparison
[52]	2021	Autonomic IoT	Self-adaptive security	Autonomic system model	Intelligent adaptation	High complexity
[11]	2020	Privacy	Data anonymization	Anonymization schemes	Privacy protection	Performance impact
[49]	2026	PHY Security	Channel-based key generation	LoRa-PRIME (PBR + MAQ)	<5% overhead; testbed validated	Relay topology required
[7]	2023	Key Mgmt	Lightweight KMS	Hierarchical key derivation	Structured key lifecycle	Manual trigger; no backward secrecy
[28]	2020	Cryptography	Secure JOIN procedure	One-way function + server entropy	Resistance to key derivation attacks	No physical testbed
[31]	2022	Authentication	Mutual authentication IoT	Mutual auth protocol	Reduces spoofing	Communication overhead
[10]	2023	Lightweight Crypto	Constrained IoT security	Lightweight encryption	Low energy consumption	Reduced security strength
[16]	2024	Blockchain	Decentralized trust	Distributed ledger	Auditability; non-repudiation	Consensus latency >5 s;

							energy prohibitive
[12]	2020	Privacy	Identifier management	Pseudonymization taxonomy	Foundation for dynamic pseudonymization	No LoRaWAN implementation	
[22]	2025	Survey	IoT protocol comparison	Systematic survey	Broad protocol coverage	No security depth	
[6]	2021	Privacy	Traffic obfuscation	Transmission randomization	Reduces traffic analysis risk	Energy overhead; QoS impact	
[3]	2022	Survey	LoRaWAN state of the art	Comprehensive survey	Architecture and vulnerability overview	No new security contributions	
[13]	2025	PHY Auth	RF fingerprinting + ML	Multi-attribute classification	>95% spoofing detection; zero device overhead	Lab conditions; dense deployment untested	
[8]	2022	Attack Analysis	LoRaWAN attack taxonomy	DoS, replay, jamming analysis	Structured threat taxonomy	No countermeasures proposed	
[42]	2023	IDS	ML-based attack detection	ML IDS	Good precision	Computational cost	
[14]	2024	Lightweight IDS	Energy-efficient detection	Optimized ML	Low energy	Reduced precision	
[5]	2021	Replay Protection	Replay attack mitigation	Timestamp/nonce scheme	Reduces replay exposure	Synchronization required	
[36]	2023	Traffic Analysis	Passive attack analysis	Pattern recognition	Threat characterization	Privacy implications demonstrated	
[15]	2023	Physical Layer Security	Authenticate LoRaWAN devices using polarization-based physical fingerprints	Polarization Fingerprint + Ensemble CNN	Accurate authentication, spoofing resistance, supports mobile devices, protocol-transparent.	pecialized hardware requirements, higher computational cost, limited large-scale validation	
[53]	2024	Hybrid Security	Multi-layer protection	Crypto + ML combination	Broad robustness	High implementation complexity	
[41]	2023	Anomaly Detection	Unknown attack detection	Autoencoder-based	Zero-day detection capability	Training data requirement	
[1]	2021	DoS Mitigation	Rate limiting	Network-level protection	Reduces overload	Performance impact	

[32]	2021	Security protocol	Secure LoRaWAN v1.1 key management	Key management and session key generation	Improves key security and supports secure key updates	Increased protocol complexity and computational overhead
[39]	2022	Energy Efficiency	SF/ADR optimization	Power management	Extended device lifetime	QoS trade-off
[19]	2023	Energy-aware Sec.	Eco-efficient security	Lightweight crypto	Good energy/security balance	Reduced security strength
[43]	2024	Edge IDS	Distributed detection	Edge-based IDS	Latency reduction	Infrastructure dependency
[50]	2023	Scalability Survey	Maximize network capacity and scalability by mitigating collision and interference at PHY and MAC layers.	Long range (1–10 km) Dynamic ADR tuning	SF tuning, SIC/NOMA, multi-gateway. Slotted/CSMA, CAD, scheduling	Strict Duty Cycle limits (1%) High ALOHA collision rates Severe co-SF interference
[54]	2021	Systematic Literature Review (SLR)	Analyze LPWAN applications in IoT	LPWAN for IoT	Long range, low power, low cost	Low data rate, scalability and security challenges
[51]	2021	Smart grid	Enable AMI communication	LoRa-based IoT architecture with ADR	Energy-efficient, scalable	Limited to AMI; no advanced security/privacy
[18]	2022	Real Deployment	LoRaWAN testbed	Physical testbed	Realistic results	High deployment cost
[44]	2024	Secure Edge AI	TinyML IDS	On-device ML inference	Low latency	Limited precision
[55]	2023	Resource Allocation	Intelligent scheduling	Optimization algorithms	Global resource efficiency	High complexity
[17]	2022	IoT Integration	Multi-layer architecture	System integration	Interoperability	Standardization difficulty
[56]	2023	Hybrid Security	Multi-layer security	Crypto + ML + PHY	Comprehensive protection	High complexity
[45]	2024	Privacy-Preserving Intrusion Detection	Detect cyberattacks while preserving data privacy	Federated Learning with a deep learning-based IDS	Preserves privacy; collaborative learning; scalable	Communication overhead; limited to SDN; affected by non-IID data
[37]	2023	Privacy Leakage Analysis	Detect privacy leakage in LoRaWAN communications	Traffic analysis and metadata-based inference attacks	Reveals privacy risks despite encryption; validated on a real	Limited to smart parking; no privacy-preserving

					LoRaWAN deployment	solution proposed
[46]	2025	Adaptive Security	Context-aware protection	Dynamic security system	Flexible response	Implementation difficulty
[33]	2024	Secure LoRaWAN	Protocol enhancement	Enhanced LoRaWAN stack	Reinforced security	Non-standardized
[38]	2025	Survey	Review AIoT security and applications	ML, DL, FL, Blockchain, 6G	Comprehensive overview	No proposed or validated solution
[47]	2024	TinyML	Embedded AI	On-device inference	Low energy consumption	Performance limits
[57]	2026	Survey / Umbrella Review	LPWAN security assessment	Umbrella review	Comprehensive evaluation of LPWAN security; identifies research gaps	Not limited to LoRaWAN security mechanisms
[34]	2020	Physical-Layer Security	Secret key generation	Time-frequency channel reciprocity + filter-bank	Exploits channel randomness; no direct key transmission	Sensitive to channel reciprocity, noise and synchronization
[58]	2024	Future IoT Security	AI + 6G + Edge vision	Integrated AI/6G/Edge framework	Highly promising direction	Largely theoretical

6.2. Multi-Criteria qualitative Comparison

Table 10 provides a multi-criteria qualitative comparison of ten representative security and privacy solutions selected from the 50 included studies. The evaluation assesses each approach across five key operational dimensions: Security Strength, Privacy Protection, Energy Efficiency, Scalability, and Validation Rigor.

To ensure objective and reproducible scoring, ratings are assigned on a 5-point qualitative scale defined according to the explicit criteria outlined in the legend below.

TABLE 10. Multi-Criteria Comparison of LoRaWAN Security Approaches (★ = Weak - ★★★★★ = Excellent)

Approach	Security	Privacy	Energy	Scalability	Validation	Category
AES-256 Enhancement [9]	★★★★☆	★★★☆☆	★★★☆☆	★★★★☆	Simulation	C1
Lightweight KMS [7]	★★★★☆	★★★☆☆	★★★★☆	★★★★☆	Formal	C1
Secure Session Keys [28]	★★★★☆	★★☆☆☆	★★★★☆	★★★★☆	Formal Verification	C1
Pseudonymization Survey [12]	★★★☆☆	★★★★★	★★★★☆	★★★★☆	SLR	C2
DNN-IDS [40]	★★★★☆	★★★☆☆	★★☆☆☆	★★★☆☆	Dataset	C3
ML Review [21]	★★★★☆	★★★☆☆	★★☆☆☆	★★★☆☆	Literature	C3
LoRa-PRIME [49]	★★★★☆	★★★☆☆	★★★★☆	★★★★☆	Testbed	C4

RF Fingerprinting [13]	★★★★☆	★★★★☆	★★★★☆	★★★★☆	Testbed+ML	C4
Blockchain IoT [16]	★★★★☆	★★★★☆	★★☆☆☆	★★☆☆☆	SLR+PoC	C5
Vulnerability Survey [4]	★★★★★	★★★★☆	★★☆☆☆	★★★★☆	Survey	C1–C5

For better readability, the legend and detailed explanations of the symbols and footnotes used in Table 10 are presented separately in Table 11.

Table 11. Legend and explicit criteria

Dimension	★	★★	★★★	★★★★	★★★★★
Security Strength	Conceptual or informal analysis	Basic passive attack protection	Robust confidentiality; vulnerable to active attacks	Strong active attack mitigation (replay, spoofing)	Comprehensive multi-layer protection with provable security
Privacy Protection	Static identifiers; no privacy	Basic encryption without identity obfuscation	Partial metadata protection or static pseudonyms	Dynamic identifier rotation; tracking resistance	Full unlinkability and Zero-Knowledge guarantees
Energy Efficiency	Prohibitive penalty (>30%)	High overhead (15–30%); gateways only	Moderate footprint (5–15%); Class B/C	Low overhead (1–5%); Class A optimized	Negligible impact (<1% overhead)
Scalability	Single-node/link level only	Limited by high latency (>5 s)	Moderate density; duty-cycle limited (1%)	High scalability across multi-cell deployments	Massive IoT capability (>10,000 devices/gateway)
Validation Rigor	Conceptual/review only	Theoretical or basic analytical model	Software simulation (NS-3, MATLAB) / datasets	Formal mathematical proof (AVISPA, BAN logic)	Empirical validation on physical hardware testbed

6.3. Trade-off Analysis: Security – Energy – Privacy

The multi-criteria comparison reveals a fundamental three-way trade-off between security strength, energy efficiency, and privacy protection. No single approach in the current literature simultaneously achieves high performance across all five evaluation dimensions. This limitation represents a core open challenge in LoRaWAN security research.

Cryptographic approaches provide the strongest mathematical security guarantees; however, they incur significant energy consumption and offer limited privacy enhancement beyond encryption. For instance, You et al. [63] proposed an enhanced LoRaWAN security protocol that strengthens end-to-end security, perfect forward secrecy, and replay attack resistance through ECDH and ECDSA while maintaining compatibility with the LoRaWAN architecture. Although the protocol was formally verified using BAN logic and AVISPA, its reliance on public-key cryptography increases computational complexity and energy consumption, limiting its suitability for highly resource-constrained end devices. Furthermore, the proposed scheme focuses primarily on cryptographic protection without incorporating complementary mechanisms such as physical-layer authentication or intelligent intrusion detection.

Physical-layer approaches enable energy-efficient authentication, but they require additional gateway-level infrastructure and are highly sensitive to environmental conditions.

Privacy-preserving approaches offer strong privacy protection with minimal energy overhead, yet they provide limited resistance against active attacks. For example, Akram et al. [60] proposed a lightweight privacy-preserving LoRaWAN authentication protocol based on Physically Unclonable Functions (PUFs) and lightweight cryptographic primitives to achieve mutual authentication, privacy preservation, and secure session key establishment with low computational,

communication, latency, and energy overhead. Nevertheless, the protocol mainly focuses on authentication and privacy preservation without integrating complementary security mechanisms, such as intrusion detection, physical-layer authentication, or adaptive attack mitigation. Furthermore, its experimental validation is limited to a relatively small-scale LoRaWAN testbed, leaving its scalability and robustness in large-scale heterogeneous deployments insufficiently investigated. Machine learning-based approaches achieve high detection accuracy, but they are generally infeasible for deployment on end devices and require substantial computational resources at the gateway level.

Finally, emerging architectural approaches introduce promising decentralized and integrated security frameworks. For example, a recent game-theoretic adaptive routing framework [64] combines Stackelberg game theory, reinforcement learning, trust management, and adaptive routing within a unified architecture. By offloading computationally intensive optimization to the network server while keeping lightweight operations at end devices, the framework achieves less than 1% additional energy overhead and demonstrates improved security, routing efficiency, and scalability in simulation. However, its evaluation relies exclusively on simulation-based experiments in multi-hop LoRaWAN environments, and the proposed architecture introduces considerable algorithmic complexity while requiring centralized computation and continuous coordination between network components. Consequently, its applicability to large-scale real-world deployments and standard single-hop LoRaWAN architectures remains to be experimentally validated. This fragmentation highlights the necessity of hybrid multi-layered security architectures, a direction consistently identified across the reviewed literature [4], [20], [22], yet still lacking practical and validated implementations in real LoRaWAN environments. The limitations observed in recent cryptographic and privacy-preserving solutions [63], [60] further reinforce the need for integrated security frameworks capable of jointly addressing security, privacy, energy efficiency, and deployment constraints.

7. Requirements, Gap-Oriented Synthesis, and Positioning

To establish a benchmark for evaluating existing countermeasures and guiding future architectures, LoRaWAN security and privacy mechanisms must be analyzed against the operational reality of Low-Power Wide-Area Networks (LPWANs). This section defines the core design requirements for secure LoRaWAN deployments, maps state-of-the-art literature against these criteria, synthesizes existing gaps, and positions this review within the current research landscape

7.1. System Design Requirements for Secure LoRaWAN

The severe resource constraints of LoRaWAN end devices specifically limited battery capacity, low processing power, narrow bandwidth, strict regional duty-cycle limitations (typically 1% or 0.1%), and sparse downlink availability dictate that security mechanisms cannot rely on conventional Internet-scale protocols. Instead, a viable security framework must satisfy three categories of design requirements:

1. Functional Requirements

Lightweight Dynamic Pseudonymization: To prevent behavioral profiling and location tracking via static header identifiers (such as DevEUI and DevAddr), mechanisms must dynamically rotate identifiers without exposing plaintext mappings over the radio interface.

Forward and Backward Secrecy: Automatic session key renewal protocols must ensure that compromising a current session key reveals neither past communications (forward secrecy) nor future session keys (backward secrecy).

Desynchronization Resilience: Given the lossy nature of LoRaWAN radio links and the unacknowledged nature of Class A uplinks, pseudonym rotation and re-keying protocols must include implicit synchronization or low-overhead recovery mechanisms to prevent permanent device isolation.

Metadata Privacy: Protection must extend beyond payload encryption to mitigate traffic analysis, transmission timing inference, and gateway proximity tracking.

2. Performance Requirements

Minimal Energy Overhead: Security procedures (cryptographic computations, transmissions, and listening windows) should add no more than 3% to 5% baseline energy consumption, preserving multi-year battery lifetimes.

Duty-Cycle Compliance: Control signaling for key management and privacy preservation must fit within strict regional duty-cycle budgets and maximum payload length constraints (e.g., 51 to 222 bytes depending on the Data Rate).

Low Computational Footprint: Cryptographic primitives and anomaly detection models must run efficiently on microcontrollers with constrained memory (e.g., ARM Cortex-M with ≤ 32 KB RAM and ≤ 256 KB Flash).

3. Operational and Architectural Requirements

Backward Compatibility: Proposed mechanisms should operate seamlessly over standard LoRaWAN 1.0.x and 1.1 protocol stacks without requiring hardware modifications to existing gateways or network servers.

Network Scalability: Security architectures must scale efficiently to support dense deployments comprising thousands of end devices per gateway without inducing server-side processing bottlenecks or channel congestion.

Seamless Integration: Frameworks should support straightforward integration with edge/fog nodes and cloud service brokers while maintaining end-to-end security separation between network and application layers.

7.2. Comparative Mapping of Literature Against Requirements

Existing literature has addressed isolated aspects of these requirements, but coverage across all functional, performance, and operational dimensions remains highly fragmented. Table 12 maps representative research categories against the proposed design requirements

Table 12. Comparative Analysis of Existing LoRaWAN Security Approaches: Systematic evaluation across functional, performance, and security criteria.

Approach Category	Pseudonymization	Re-Keying	Energy Efficiency	Duty-Cycle Aware	Desync Resilience	Key Limitations
Identifier Privacy Frameworks	● ¹	✗	✓	●	✗	Theoretical; lacks hardware/protocol validation
Lightweight Key Management	✗	● ²	✓	✓	●	Lacks automatic re-keying; limited secrecy
Secure JOIN Enhancements	✗	● ³	✓	✓	✓	Restricts protection to the initial attachment (OTAA JOIN procedure) without supporting runtime key updates
Traffic Obfuscation Schemes	● ⁴	✗	✗	✗	N/A	Prohibitive energy overhead; triggers duty-cycle limits
ML / DL Anomaly Detection	✗	✗	✗	N/A	N/A	High memory/compute cost; infeasible on end devices
Physical Layer Security (PLS)	✗	●	✓	✓	✗	Environment-sensitive; requires

Approach Category	Pseudonymization	Re- Keying	Energy Efficiency	Duty- Cycle Aware	Desync Resilience	Key Limitations
						specialized hardware

Legend:

✓ = Criterion fully satisfied ● = Criterion partially or conditionally satisfied ✗ = Criterion not satisfied N/A = Not applicable

¹ Proposed primarily at a conceptual level without formal protocol integration or physical testbed validation.

² Provides structured key derivation but lacks dynamic, event-driven, or automated trigger mechanisms.

³ Restricts protection to the initial attachment (OTAA JOIN procedure) without supporting runtime key updates.

⁴ Achieves privacy as a secondary effect of transmission padding or dummy traffic, severely increasing power drain.

7.3. Gap-Oriented Synthesis and Unaddressed Core Limitations

Comparing the state of the art against the defined design requirements reveals three systemic limitations in current LoRaWAN security research:

Structural Separation of Pseudonymization and Key Management: Existing studies treat identifier privacy and session re-keying as independent problems. In practice, these mechanisms are deeply complementary: updating identifiers without refreshing cryptographic keys leaves traffic susceptible to cryptographic linkage, while updating keys without rotating identifiers permits metadata tracking. No existing scheme provides a unified, lightweight protocol that jointly executes dynamic pseudonymization and session key renewal.

Lack of Duty-Cycle-Aware Protocol Adaptability: High-overhead security protocols designed for broadband wireless networks fail when applied to LPWANs. Most proposed re-keying and privacy schemes ignore regional duty-cycle restrictions and Class A downlink limits (where receive windows open only briefly following an uplink). Consequently, explicit multi-way handshakes frequently cause frame loss, duty-cycle exhaustion, and protocol failure.

Neglect of Real-World Deployment and Lossy Downlink Constraints: A significant portion of published solutions relies on ideal channel assumptions or simulation models that overlook packet loss. In lossy environments, unacknowledged identifier rotations or re-keying commands frequently cause desynchronization between the end device and the Network/Join Server. Current literature lacks lightweight, desynchronization-resilient recovery mechanisms that do not require expensive re-attachments or complete OTAA re-joins.

7.4. Positioning of This Review

In contrast to existing surveys that offer isolated threat taxonomies, single-layer analyses, or standalone cryptographic reviews, this work provides a holistic, requirement-driven synthesis of the LoRaWAN security landscape. By explicitly linking multi-layer attack vectors to functional and performance requirements, evaluating state-of-the-art countermeasures through a multi-criteria benchmarking matrix, and defining a gap-oriented roadmap, this study establishes a practical foundation for designing next-generation, energy-efficient, and privacy-preserving LoRaWAN security architectures.

8. Research Gaps and Future Directions

While the preceding sections have provided a comprehensive review of the state of the art in LoRaWAN security, several critical research gaps remain unresolved, particularly in lightweight pseudonymization, low-overhead re-keying, metadata

protection, large-scale experimental validation, and explainable intrusion detection. This section identifies and analyzes these gaps through a structured taxonomy and discusses future research directions toward the development of secure, scalable, resource-efficient, and privacy-preserving LoRaWAN security solutions.

8.1. Identified Research Gaps

Based on the systematic analysis of the 50 included studies and the five-category taxonomy, five critical research gaps have been identified and characterized in Table 13.

Table 13. Research Gaps Identified and Proposed Future Research Directions

Code	Severity	Research Gap	Implicated Studies	Proposed Direction
G1	Critical	Absence of lightweight dynamic pseudonymization specific to LoRaWAN Classes A/B/C duty-cycle constraints	[16, 5]	Adaptive rotating identifiers consuming <3% of LoRaWAN duty-cycle budget with desynchronization recovery
G2	Critical	Lack of automatic re-keying protocols guaranteeing forward/backward secrecy at low communication overhead	[11, 12, 4]	Duty-cycle-aware re-keying with a 2-frame signaling overhead limit and hierarchical key refresh
G3	High	Insufficient protection of LoRaWAN-specific metadata (timestamps, RSSI, gateway IDs, transmission patterns)	[16, 1, 5]	Traffic shaping, dummy transmission injection, channel randomization at the gateway level
G4	High	Scarcity of large-scale physical testbed validation for LoRaWAN security mechanisms	[1, 11, 3]	Standardized open-source benchmarking framework with common datasets and evaluation metrics
G5	Moderate	Absence of explainable (XAI) lightweight ML intrusion detection solutions for constrained LoRaWAN devices	[7, 3]	Federated learning or interpretable TinyML models deployable at gateway with explainability guarantees

8.2. Future Research Directions

Based on the findings of this review, it is evident that existing LoRaWAN security solutions remain fragmented, with most approaches addressing only specific aspects of security or privacy rather than providing comprehensive protection. Future research should therefore focus on the design of integrated security frameworks capable of simultaneously ensuring data confidentiality, integrity, authentication, intrusion prevention, and user privacy while preserving the low-power characteristics of LoRaWAN devices.

From an architectural perspective, the adoption of multi-layer (cross-layer) security architectures represents a promising direction. Such architectures can combine complementary security mechanisms operating at different protocol layers to provide end-to-end protection without imposing excessive computational or energy overhead on constrained IoT devices.

Future research should also investigate adaptive and context-aware security mechanisms capable of dynamically balancing security, privacy, latency, and energy consumption according to application requirements.

Recent advances in lightweight Artificial Intelligence (AI), particularly TinyML and Federated Learning, also offer promising opportunities for enhancing LoRaWAN security. These technologies enable distributed intrusion detection, anomaly detection, and intelligent network monitoring while preserving data privacy by limiting the transmission of sensitive information. Nevertheless, their deployment in resource-constrained LPWAN environments remains an open research challenge that requires lightweight and energy-efficient implementations.

Deploying real-time Physical (PHY) and MAC layer anomaly detection directly on edge gateways is essential for identifying sophisticated attacks, such as RF jamming, rogue gateway spoofing, and preamble manipulation, before malicious traffic reaches cloud core networks [65]. However, commercial LoRaWAN gateways are strictly resource-constrained, typically equipped with embedded microcontrollers or low-power SoCs featuring limited memory [65]. While quantized deep autoencoders and MobileNets can detect anomalies from PHY metrics (e.g., RSSI, SNR, Carrier Frequency Offset, and ToA), their black-box nature prevents network orchestrators from understanding the root cause of detection triggers or distinguishing malicious interference from routine environmental path loss [66]. To bridge this gap, future research must establish Explainable TinyML (X-TinyML) frameworks optimized for microcontrollers. Research should focus on low-overhead feature extraction pipelines and transparent decision models, such as tree-based ensemble pruning, symbolic regression, and lightweight Shapley additive explanations (SHAP) approximations. These models must compute local attribution scores within sub-millisecond inference windows while executing entirely within sub-512 KB RAM bounds, enabling automated and interpretable security enforcement at the network edge [66].

Another promising research direction concerns the integration of Post-Quantum Cryptography (PQC) into LoRaWAN networks. Post-quantum cryptography refers to cryptographic algorithms designed to remain secure against attacks from both classical and quantum computers while being executable on conventional hardware. Although PQC has recently attracted considerable attention in the cybersecurity community, its adoption in LoRaWAN remains very limited due to the stringent constraints on memory, computation, communication overhead, and energy consumption of IoT devices. Future work should therefore investigate lightweight post-quantum cryptographic schemes and hybrid cryptographic architectures that can provide long-term security without significantly degrading network performance or device lifetime.

The advent of quantum computing necessitates transitioning LoRaWAN from classic elliptic-curve primitives (e.g., ECC/AES key distribution) to Post-Quantum Cryptography (PQC). However, NIST-standardized lattice-based key encapsulation mechanisms, such as ML-KEM (Kyber-512) [67], require public keys and ciphertexts of 800 and 768 bytes, respectively. These sizes drastically exceed LoRaWAN's maximum payload limits, which range between 51 and 222 bytes across Data Rates DR0 - DR5 under regional parameter constraints [68]. Transmitting PQC ciphertexts over pure ALOHA channels forces multi-frame protocol fragmentation. This fragmentation exponentially increases Time-on-Air (ToA), elevates packet collision probability, and rapidly exhausts the 1% or 0.1% sub-GHz regional duty-cycle limits enforced by regulatory bodies like ETSI [68], [69]. To address these constraints, future research must focus on duty-cycle and MAC-aware PQC adaptation layers tailored for LPWANs. Priorities include state compression algorithms, hybrid implicit-certificates, and stateful hash-based or lightweight code-based cryptography capable of reducing public key transport overhead. Furthermore, research should explore cross-layer optimization strategies where PQC handshakes dynamically adapt payload size and fragmentation rates based on real-time Channel State Information (CSI) and local duty-cycle energy budgets [69], [70].

As AI-based security mechanisms become increasingly integrated into LoRaWAN systems, Model Extraction Attacks (MEAs) constitute another emerging research challenge. In these attacks, adversaries attempt to reconstruct or approximate a machine learning model by repeatedly querying it, thereby compromising the confidentiality of model parameters and facilitating subsequent attacks such as evasion or poisoning attacks. Despite their growing importance in AI-enabled IoT systems, model extraction attacks have received little attention in the context of LoRaWAN. Future studies should investigate appropriate mitigation techniques, including secure federated learning, differential privacy, query-rate limitation, output perturbation, watermarking, and anomaly detection mechanisms to protect deployed machine learning models.

Furthermore, greater attention should be devoted to the protection of metadata and communication patterns, which remain insufficiently addressed in current LoRaWAN security solutions. Even when payloads are encrypted, traffic analysis can reveal sensitive information about users, devices, or network activities. Future research should therefore explore privacy-enhancing techniques such as pseudonymization, traffic obfuscation, dummy traffic generation, and differential privacy to reduce information leakage through network metadata.

Implementing dynamic pseudonym rotation and automated session re-keying over lossy, unacknowledged Class A uplinks introduces a fundamental mathematical trade-off between privacy preservation and state synchronization [30]. When an end device locally updates its device address or derives new session keys via pseudo-random functions or hash chains, the Network/Join Server must match the device's state using a bounded sliding look-ahead window. In real-world environments characterized by severe shadowing or channel fading, consecutive uplink packet drops cause the device's state counter to advance beyond the server's look-ahead window [30], [71]. Expanding this window on the server side mitigates packet loss but exponentially increases cryptographic search space complexity, opening the server to Denial-of-Service (DoS) and exhaustion attacks [71]. Conversely, keeping the window narrow reduces this attack surface but increases the risk of permanent desynchronization, isolating the node until a costly Over-The-Air Activation (OTAA) re-join is manually triggered. Resolving this open challenge requires mathematically rigorous, loss-tolerant synchronization protocols that operate without explicit downlink acknowledgments (ACKs). Future directions should investigate rateless state-synchronization codes, implicit counter alignment via cryptographic headers, and multi-hypothesis look-ahead verification models. Formalizing these synchronization dynamics as Markov decision processes or rateless state-recovery problems will allow researchers to mathematically prove forward secrecy and desynchronization bounds under probabilistic packet erasure channels [30].

Finally, future studies should emphasize large-scale experimental validation and standardized benchmarking methodologies. The lack of common evaluation frameworks makes it difficult to compare existing security solutions objectively. Establishing standardized performance metrics that jointly evaluate security strength, privacy preservation, energy consumption, latency, computational complexity, and communication overhead would facilitate fair comparisons and accelerate the development of practical, efficient, and secure LoRaWAN security architectures.

9. Challenges and Best Practices for LoRaWAN Security Deployment

Despite the growing adoption of LoRaWAN in IoT applications, achieving secure and reliable deployments remains challenging due to resource limitations, evolving cyber threats, and diverse operational requirements. This section highlights the key security challenges and summarizes best practices to improve the protection, privacy, and resilience of LoRaWAN networks.

9.1. Deployment Challenges

Despite significant advances in LoRaWAN security research, several challenges continue to hinder the deployment of robust and comprehensive security mechanisms in real-world IoT applications.

The first challenge concerns the trade-off between security, energy consumption, computational complexity, and communication overhead. LoRaWAN end devices are typically characterized by limited battery capacity, low processing power, and constrained memory resources. Consequently, implementing advanced cryptographic algorithms, continuous authentication mechanisms, or intelligent intrusion detection systems may significantly increase energy consumption, processing latency, and memory usage, thereby reducing device lifetime. Designing lightweight security mechanisms that achieve an appropriate balance between protection and resource efficiency remains one of the most important research challenges.

The second challenge relates to the heterogeneity of LoRaWAN deployments and protocol versions. Although LoRaWAN v1.1 introduced several security improvements, including separate network and application session keys, enhanced join procedures, and stronger key management mechanisms, a considerable number of commercial deployments continue to operate using LoRaWAN v1.0.x due to compatibility constraints and deployment costs. As a result, many operational

networks remain vulnerable to replay attacks, key compromise, session hijacking, and weaknesses in the activation procedure.

Another significant challenge is the limited protection of user privacy and communication metadata. While LoRaWAN encrypts application payloads using AES-128, metadata such as packet timing, transmission frequency, gateway association, frame counters, and communication patterns remain observable. Adversaries can exploit such information through traffic analysis to infer sensitive information about device behavior, user activities, or deployment characteristics, even without decrypting packet contents.

The emergence of Artificial Intelligence (AI)-based security mechanisms, including TinyML and Federated Learning, introduces additional security challenges. Although these approaches improve intrusion detection and anomaly detection capabilities, they also expose LoRaWAN systems to new threats such as model extraction attacks, model inversion attacks, poisoning attacks, and adversarial examples. Protecting machine learning models deployed on resource-constrained devices while preserving their efficiency remains largely unexplored.

Another emerging challenge concerns the future threat posed by quantum computing. Current LoRaWAN security relies primarily on AES-128 symmetric cryptography, which remains relatively resistant to quantum attacks, but several supporting cryptographic mechanisms used in IoT ecosystems may eventually require migration toward Post-Quantum Cryptography (PQC). However, most PQC algorithms introduce larger key sizes, higher computational complexity, and increased communication overhead, making their integration into constrained LoRaWAN devices particularly challenging.

Finally, the literature highlights the absence of standardized benchmarking frameworks capable of objectively evaluating and comparing LoRaWAN security solutions. Existing studies often employ different datasets, experimental platforms, attack models, and evaluation metrics, making direct comparison difficult. The lack of common benchmarks limits reproducibility and slows the adoption of practical security solutions.

9.2. Best Practice Recommendations

Based on the findings of the reviewed studies, several best practices can be recommended to improve the security, privacy, and resilience of LoRaWAN deployments.

First, organizations should adopt LoRaWAN v1.1 (or later versions) whenever possible and prioritize Over-the-Air Activation (OTAA) instead of Activation by Personalization (ABP). OTAA enables dynamic generation of session keys during the join procedure, thereby reducing the risk associated with long-term static keys and improving resistance to replay and key compromise attacks. Strong cryptographic key management should also be considered a fundamental security requirement. Session keys should be periodically renewed, key expiration policies should be enforced, and secure key storage mechanisms such as hardware secure elements should be employed whenever feasible. In addition, secure random number generation is essential for preventing predictable key generation. To improve device authentication while maintaining low computational overhead, lightweight physical-layer security techniques, such as RF fingerprinting, can be deployed at gateways or network servers. These techniques exploit the unique radio-frequency characteristics of transmitting devices to identify legitimate nodes without requiring additional cryptographic operations.

The deployment of lightweight intrusion detection systems (IDS) and AI-based anomaly detection mechanisms at gateways or edge computing nodes can significantly improve the detection of malicious activities, including jamming attacks, replay attacks, rogue gateways, and abnormal traffic behavior. Edge-based detection also reduces communication latency and preserves network scalability. To strengthen privacy protection, dynamic device pseudonymization, periodic DevAddr rotation, and temporary device identifiers should be implemented whenever possible. These techniques reduce the possibility of long-term device tracking and mitigate traffic correlation attacks. Similarly, traffic obfuscation techniques, including dummy packet generation, randomized transmission scheduling, adaptive packet padding, and transmission delay randomization, can effectively reduce the amount of exploitable metadata available to attackers performing traffic analysis.

Considering the increasing integration of Artificial Intelligence into IoT security, future deployments should incorporate protection mechanisms against machine learning attacks, including secure federated learning protocols, differential privacy,

model watermarking, secure aggregation, query-rate limitation, and model integrity verification to mitigate model extraction and poisoning attacks. From a long-term perspective, researchers and system designers should also begin evaluating the feasibility of integrating lightweight Post-Quantum Cryptography (PQC) into LoRaWAN architectures. Hybrid cryptographic approaches combining conventional cryptography with lightweight post-quantum algorithms may provide a practical migration path toward quantum-resistant IoT infrastructures.

Finally, security validation should rely on standardized benchmarking methodologies that jointly evaluate security effectiveness, energy consumption, latency, memory footprint, computational complexity, scalability, and privacy preservation under realistic deployment scenarios. Such evaluation frameworks would facilitate objective comparison between different security solutions and accelerate their adoption in industrial LoRaWAN applications.

10. Conclusion

This systematic literature review analyzed 50 studies selected from 550 records using the PRISMA 2020 methodology and provides five main contributions.

First, it proposes a five-category taxonomy (C1–C5) covering cryptographic key management, privacy and pseudonymization, machine learning-based detection, physical layer security, and emerging architectural approaches, offering a structured framework for LoRaWAN security research.

Second, a comparative evaluation of 10 representative solutions was conducted across five dimensions: security, privacy, energy efficiency, scalability, and validation rigor. The results reveal a fundamental trade-off between cryptographic strength, privacy preservation, and energy efficiency, with no existing solution excelling in all dimensions simultaneously.

Third, five major research gaps were identified: the lack of lightweight dynamic pseudonymization (G1), automatic re-keying with forward/backward secrecy (G2), protection of LoRaWAN-specific metadata (G3), large-scale real-world validation (G4), and explainable lightweight ML-based detection mechanisms (G5). Each gap is associated with potential research directions.

Fourth, several promising future research areas were highlighted, including hybrid multi-layer security architectures, TinyML and federated learning, lightweight post-quantum cryptography, differential privacy for metadata protection, and LoRaWAN security for 6G and non-terrestrial networks.

Finally, the review formulates several best-practice recommendations for secure LoRaWAN deployment based on evidence from the 50 analyzed studies.

Overall, the review concludes that current solutions remain fragmented and address security challenges separately. The growing use of LoRaWAN in critical applications emphasizes the need for integrated, multi-layer, and energy-efficient security frameworks capable of simultaneously addressing security, privacy, and performance requirements.

Declarations

Funding

The authors received no funding for this research.

Clinical Trial Registration

Not applicable. This study is a systematic literature review and does not involve a clinical trial.

Consent to Publish declaration

Not applicable.

Ethics and Consent to Participate declarations

Not applicable.

References

1. Palattella, M. R.; Dohler, M.; Grieco, A.; Rizzo, G.; Torsner, J.; Engel, T., & Ladid, L. Internet of Things in the 5G Era: Enablers, Architecture, and Business Models. *IEEE J. Sel. Areas Commun.* 2016, *34*, 510–527. <https://doi.org/10.1109/JSAC.2016.2525418>.
2. Pan, Q.; Wu, J.; Zheng, X.; Li, J.; Li, S.; Vasilakos, A. Leveraging AI and Intelligent Reflecting Surface for Energy-Efficient Communication in 6G IoT. *arXiv* 2020, *arXiv:2012.14716*. <https://doi.org/10.48550/arXiv.2012.14716>.
3. Sun, Z.; Yang, H.; Liu, K.; Yin, Z.; Li, Z., & Xu, W. Recent Advances in LoRa: A Comprehensive Survey. *ACM Trans. Sensor Netw.* 2022, *18*, 1–73. <https://doi.org/10.1145/3543856>.
4. Osuorah, J.C.; Ahmed, S.T.; Annamalai, A.; Chouikha, M.F. Vulnerabilities and Layered Security Threats in LoRaWAN Systems: A Comprehensive Survey on Physical, MAC, and Application Layer Weaknesses. *IEEE Access* 2025, *13*, 217939–217953. <https://doi.org/10.1109/ACCESS.2025.3647086>.
5. Sung, W.-J.; Ahn, H.-G.; Kim, J.-B.; Choi, S.-G. Protecting End-Device from Replay Attack on LoRaWAN. In Proceedings of the 20th International Conference on Advanced Communication Technology (ICACT), Feb. 2018. 167–171. <https://doi.org/10.23919/ICACT.2018.8323684>.
6. Spadaccino, P.; Garlisi, D.; Cuomo, F.; Pillon, G.; Pisani, P. Discovery Privacy Threats via Device De-Anonymization in LoRaWAN. *Comput. Commun.* 2022, *189*, 1–10. <https://doi.org/10.1016/j.comcom.2022.02.017>.
7. Qadir, J.; Butun, I.; Gastaldo, P.; Aiello, O.; Caviglia, D.D. Mitigating Cyber Attacks in LoRaWAN via Lightweight Secure Key Management Scheme. *IEEE Access* 2023, *11*, 68301–68315. <https://doi.org/10.1109/ACCESS.2023.3291420>.
8. Hessel, F.; Almon, L.; Hollick, M. LoRaWAN Security: An Evolvable Survey on Vulnerabilities, Attacks and Their Systematic Mitigation. *ACM Trans. Sens. Netw.* 2023, *18*, 1–55. <https://doi.org/10.1145/3561973>.
9. Abboud, S.; Abdoun, N. Enhancing LoRaWAN Security: An Advanced AES-Based Cryptographic Approach. *IEEE Access* 2024, *12*, 2589–2606. <https://doi.org/10.1109/ACCESS.2023.3348416>.
10. Thakor, V.A.; Razzaque, M.A.; Khandaker, M.R.A. Lightweight Cryptography Algorithms for Resource-Constrained IoT Devices: A Review, Comparison and Research Opportunities. *IEEE Access* 2021, *9*, 28177–28193. <https://doi.org/10.1109/ACCESS.2021.3052867>.
11. Majeed, A.; Lee, S. Anonymization Techniques for Privacy Preserving Data Publishing: A Comprehensive Survey. *IEEE Access* 2021, *9*, 8512–8545. <https://doi.org/10.1109/ACCESS.2020.3045700>.

12. Akil, M.; Islami, L.; Fischer-Hübner, S.; Martucci, L.A.; Zuccato, A. Privacy-Preserving Identifiers for IoT: A Systematic Literature Review. *IEEE Access* 2020, 8, 168470–168485. <https://doi.org/10.1109/ACCESS.2020.3023659>.
13. Pourghasem, A.; Kirner, R.; Tsokanos, A.; Mporas, I.; Mylonas, A. Machine Learning-Based Multi-Attribute Physical-Layer Authentication for Spoofing Detection in LoRaWAN. *Future Internet* 2025, 17, 68. <https://doi.org/10.3390/fi17020068>.
14. Rafique, S.H.; Abdallah, A.; Musa, N.S.; Murugan, T. Machine Learning and Deep Learning Techniques for Internet of Things Network Anomaly Detection: Current Research Trends. *Sensors* 2024, 24, 1968. <https://doi.org/10.3390/s24061968>.
15. Xu, J.; Wei, D. Polarization Fingerprint-Based LoRaWAN Physical Layer Authentication. *IEEE Trans. Inf. Forensics Secur.* 2023, 18, 4593–4608. <https://doi.org/10.1109/TIFS.2023.3295615>.
16. Almarri, S.; Aljughaiman, A. Blockchain Technology for IoT Security and Trust: A Comprehensive SLR. *Sustainability* 2024, 16, 10177. <https://doi.org/10.3390/su162310177>.
17. Dastjerdi, A.V.; Buyya, R. Fog Computing: Helping the Internet of Things Realize Its Potential. *Computer* 2016, 49, 112–116. <https://doi.org/10.1109/MC.2016.245>.
18. Goulart, A.; Chennamaneni, A.; Torre, D.; Hur, B.; Al-Aboosi, F.Y. On Wide-Area IoT Networks, Lightweight Security and Their Applications—A Practical Review. *Electronics* 2022, 11, 1762. <https://doi.org/10.3390/electronics11111762>.
19. Radhakrishnan, I.; Jadon, S.; Honnavalli, P.B. Efficiency and Security Evaluation of Lightweight Cryptographic Algorithms for Resource-Constrained IoT Devices. *Sensors* 2024, 24, 4008. <https://doi.org/10.3390/s24124008>.
20. Mosenia, A.; Jha, N.K. A Comprehensive Study of Security of Internet-of-Things. *IEEE Trans. Emerg. Top. Comput.* 2017, 5, 586–602. <https://doi.org/10.1109/TETC.2016.2606384>.
21. Halbouni, A.; Gunawan, T.S.; Habaebi, M.H.; Halbouni, M.; Kartiwi, M.; Ahmad, R. Machine Learning and Deep Learning Approaches for Cybersecurity: A Review. *IEEE Access* 2022, 10, 19572–19585. <https://doi.org/10.1109/ACCESS.2022.3151248>.
22. Saleem, A.; Shah, S.; Iftikhar, H.; Zywiółek, J.; Albalawi, O. A Comprehensive Systematic Survey of IoT Protocols: Implications for Data Quality and Performance. *IEEE Access* 2025, 13, 196206–196235. <https://doi.org/10.1109/ACCESS.2024.3486927>.
23. Ashraf, Q.M.; Tahir, M.; Habaebi, M.H.; Isoaho, J. Toward Autonomic Internet of Things: Recent Advances, Evaluation Criteria, and Future Research Directions. *IEEE Internet Things J.* 2023, 10, 14725–14748. <https://doi.org/10.1109/JIOT.2023.3285359>.
24. Ahmed, K.I.; Tahir, M.; Jiangbin, Z.; Lau, S.L.; Habaebi, M.H.; Ahad, A. Optimizing Internet of Things security: Artificial neural networks algorithms performance in authentication and authorization via physical layer features. *Eng. Appl. Artif. Intell.* 2026, 181, 115408. <https://doi.org/10.1016/j.engappai.2026.115408>.

25. Chaudhari, B.S.; Zennaro, M.; Borkar, S. LPWAN Technologies: Emerging Application Characteristics, Requirements, and Design Considerations. *Future Internet* 2020, 12, 46. <https://doi.org/10.3390/fi12030046>.
26. Mekki, K.; Bajic, E.; Chaxel, F.; Meyer, F. A comparative study of LPWAN technologies for large-scale IoT deployment. *ICT Express* 2019, 5, 1–7. <https://doi.org/10.1016/j.icte.2017.12.005>.
27. Ertürk, M.A.; Aydın, M.A.; Büyükakkaşlar, M.T.; Evirgen, H. A Survey on LoRaWAN Architecture, Protocol and Technologies. *Future Internet* 2019, 11, 216. <https://doi.org/10.3390/fi11100216>.
28. Tsai, K.-L.; Leu, F.-Y.; Hung, L.-L.; Ko, C.-Y. Secure Session Key Generation Method for LoRaWAN Servers. *IEEE Access* 2020, 8, 54631–54640. <https://doi.org/10.1109/ACCESS.2020.2978100>.
29. Simin, Z.A.; Aslan, S.; Carvalho, M.M.; Valles, D. Enhanced Security of Bidirectional Communication in IoT-Driven Utility Networks Using Sertainty UXP and LoRaWAN. *Sensors* 2026, 26, 1752. <https://doi.org/10.3390/s26061752>.
30. Loukil, S.; Fourati, L.C.; Nayyar, A.; Chee, K.-W.-A. Analysis of LoRaWAN 1.0 and 1.1 Protocols Security Mechanisms. *Sensors* 2022, 22, 3717. <https://doi.org/10.3390/s22103717>.
31. Pathak, G.; Gutierrez, J.; Ghobakhlou, A.; Rehman, S.U. LPWAN Key Exchange: A Centralised Lightweight Approach. *Sensors* 2022, 22, 5065. <https://doi.org/10.3390/s22135065>.
32. Chen, X.; Lech, M.; Wang, L. A Complete Key Management Scheme for LoRaWAN v1.1. *Sensors* 2021, 21, 2962. <https://doi.org/10.3390/s21092962>.
33. Tsai, K.-L.; Leu, F.-Y.; You, I.; Chang, S.-W.; Hu, S.-J.; Park, H. Low-Power AES Data Encryption Architecture for a LoRaWAN. *IEEE Access* 2019, 7, 146348–146357. <https://doi.org/10.1109/ACCESS.2019.2941972>.
34. Zoli, M.; Barreto, A.N.; Köpsell, S.; Sen, P.; Fettweis, G. Physical-Layer-Security Box: a concept for time-frequency channel-reciprocity key generation. *EURASIP J. Wirel. Commun. Netw.* 2020, 2020. <https://doi.org/10.1186/s13638-020-01712-6>.
35. Ahmed, S.F.; Alam, M.S.B.; Afrin, S.; Rafa, S.J.; Taher, S.B.; Kabir, M.; Mueen, S.M.; Gandomi, A.H. Toward a Secure 5G-Enabled Internet of Things: A Survey on Requirements, Privacy, Security Challenges, and Opportunities. *IEEE Access* 2024, 12, 13125–13145. <https://doi.org/10.1109/ACCESS.2024.3352508>.
36. Péliissier, S.; Cunche, M.; Roca, V.; Donsez, D. Device Re-Identification in LoRaWAN Through Messages Linkage. In *Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)*, 2022. 1–11. <https://doi.org/10.1145/3507657.3528556>.
37. Đujić Rodić, L.; Perković, T.; Škiljo, M.; Šolić, P. Privacy leakage of LoRaWAN smart parking occupancy sensors. *Future Gener. Comput. Syst.* 2023, 138, 142–159. <https://doi.org/10.1016/j.future.2022.08.007>.

38. Menon U, V.; Kumaravelu, B.; Vinoth, C.; Vinoth Kumar, A.; Rammohan; Chinnadurai, S.; Venkatesan, R.; Hai, H.; Selvaprabhu; Poongundran. AI-Powered IoT: A Survey on Integrating Artificial Intelligence With IoT for Enhanced Security, Efficiency, and Smart Applications. *IEEE Access* 2025, 13, 50296–50339. <https://doi.org/10.1109/ACCESS.2025.3551750>.
39. Tsai, K.-L.; Chen, L.-W.; Leu, F.-Y.; Hsu, H.-C.; Wu, C.-T. Secure LoRaWAN Root Key Update Scheme for IoT Environment. *IEEE Internet Things J.* 2022, 9, 2284–2296. <https://doi.org/10.1109/JIOT.2021.3087898>.
40. Cevallos-Salas, D.; Estrada-Jiménez, J.; Guamán, D.S. Enhanced Reconnaissance Attacks Detection for IoT Privacy Protection. In *Proceedings of the 2025 5th International Conference on Information Systems and Software Technologies (ICI2ST)*, Quito, Ecuador, 2025. 34–41. <https://doi.org/10.1109/ICI2ST68465.2025.00014>.
41. Sagduyu, Y.E.; Erpek, T. Adversarial Attacks on LoRa Device Identification and Rogue Signal Detection with Deep Learning. In *Proceedings of the IEEE Military Communications Conference (MILCOM)*, Boston, MA, USA, 2023. 385–390. <https://doi.org/10.1109/MILCOM58377.2023.10356224>.
42. Senol, N.S.; Rasheed, A.; Baza, M.; Alsabaan, M. Identifying Tampered Radio-Frequency Transmissions in LoRa Networks Using Machine Learning. *Sensors* 2024, 24, 6611. <https://doi.org/10.3390/s24206611>.
43. Islam, M.; Abdullah, W.M.; Saha, B.N. Privacy-Preserving Hierarchical Fog Federated Learning for IoT Intrusion Detection. *Sensors* 2025, 25, 7296. <https://doi.org/10.3390/s25237296>.
44. Alanazi, F. Lightweight deep learning models for real-time IoT data analysis in resource-constrained environments. *Sci. Rep.* 2026, 16, 20861. <https://doi.org/10.1038/s41598-026-49314-4>.
45. Raza, M.; Saeed, M.J.; Riaz, M.B.; Sattar, M.A. Federated Learning for Privacy-Preserving Intrusion Detection in Software-Defined Networks. *IEEE Access* 2024, 12, 69551–69567. <https://doi.org/10.1109/ACCESS.2024.3395997>.
46. Meurisch, C.; Mühlhäuser, M. Data Protection in AI Services: A Survey. *ACM Comput. Surv.* 2021, 54, 1–38. <https://doi.org/10.1145/3440754>.
47. Sanchez-Iborra, R.; Skarmeta, A. TinyML-Enabled Frugal Smart Objects: Challenges and Opportunities. *IEEE Circuits Syst. Mag.* 2021, 20, 4–18. <https://doi.org/10.1109/MCAS.2020.3005467>.
48. Ruotsalainen, H.; Shen, G.; Zhang, J.; Fujdiak, R. LoRaWAN Physical Layer-Based Attacks and Countermeasures, A Review. *Sensors* 2022, 22, 3127. <https://doi.org/10.3390/s22093127>.
49. Anisah, I.; Suwadi; Wirawan; Yuliana, M. LoRa-PRIME: A Novel Secret Key Generation Framework Based on Periodic Bit Reversal and Modified Adaptive Quantization for Robust Cooperative Jamming LoRa Relay Networks. *IEEE Open J. Commun. Soc.* 2026, 7, 2664–2683. <https://doi.org/10.1109/OJCOMS.2026.3672889>.

50. Jouhari, M.; Saeed, N.; Alouini, M.-S.; Amhoud, E.M. A Survey on Scalable LoRaWAN for Massive IoT: Recent Advances, Potentials, and Challenges. *IEEE Commun. Surv. Tutorials* 2023, 25, 1841–1876. <https://doi.org/10.1109/COMST.2023.3274934>.
51. Gallardo, J.L.; Ahmed, M.A.; Jara, N. LoRa IoT-Based Architecture for Advanced Metering Infrastructure in Residential Smart Grid. *IEEE Access* 2021, 9, 124295–124312. <https://doi.org/10.1109/ACCESS.2021.3110873>.
52. Lin, C.; Khazaei, H.; Walenstein, A.; Malton, A. Autonomic Security Management for IoT Smart Spaces. *ACM Trans. Internet Things* 2021, 2, 27. <https://doi.org/10.1145/3466696>.
53. Abdel Hakeem, S.A.; Abd El-Kader, S.M.; Kim, H. A Key Management Protocol Based on the Hash Chain Key Generation for Securing LoRaWAN Networks. *Sensors* 2021, 21, 5838. <https://doi.org/10.3390/s21175838>.
54. Mousavi, S.M.; Khademzadeh, A.; Rahmani, A.M. The Role of Low-Power Wide-Area Network Technologies in Internet of Things: A Systematic and Comprehensive Review. *Int. J. Commun. Syst.* 2022, 35, e5036. <https://doi.org/10.1002/dac.5036>.
55. Liwen, Z.; Qamar, F.; Liaqat, M.; Hindia, M.; Zainol Ariffin, K.A. Toward Efficient 6G IoT Networks: A Perspective on Resource Optimization Strategies, Challenges, and Future Directions. *IEEE Access* 2024, 12, 76606–76633. <https://doi.org/10.1109/ACCESS.2024.3405487>.
56. Althobaiti, F.A. Lightweight cryptography for IoT: A comprehensive survey of algorithms, implementations, and standardization. *World J. Adv. Eng. Technol. Sci.* 2025, 15, 516–525. <https://doi.org/10.30574/wjaets.2025.15.3.0967>.
57. Bezerra, W.R.; Bezerra, L.M.; Westphall, C.B. Qualitative assessment of low power wide area network protocols and their security aspects: A umbrella review. *Meas. Digit.* 2026, 6, 100031. <https://doi.org/10.1016/j.meadig.2026.100031>.
58. Li, K.; Li, C.; Yuan, X.; Li, S.; Zou, S.; Ahmed, S.S.; Akan, Ö.B. Zero-trust foundation models: A new paradigm for secure and collaborative artificial intelligence for internet of things. *IEEE Internet Things J.* 2025, 12, 46269–46293. <https://doi.org/10.1109/JIOT.2025.3603957>.
59. Nabeel, N.; Habaebi, M.H.; Islam, M.D.R. Security Analysis of LNMNT-LightWeight Crypto Hash Function for IoT. *IEEE Access* 2021, 9, 165754–165765. <https://doi.org/10.1109/ACCESS.2021.3133097>.
60. Akram, M.A.; Mian, A.N.; Biswas, A.K.; Kumari, S.; Chen, C.-M. Privacy-Preserving Lightweight LoRaWAN Authentication Protocol for IoT Applications. *IEEE Internet Things J.* 2025, 12, 42790–42802. <https://doi.org/10.1109/JIOT.2025.3593886>.
61. Ahmed, K.I.; Tahir, M.; Lau, S.L.; Habaebi, M.H.; Ahad, A.; Mughees, A. Trust-Aware Authentication and Authorization for IoT: A Federated Machine Learning Approach. *IEEE Internet Things J.* 2025, 12, 9889–9904. <https://doi.org/10.1109/JIOT.2024.3512657>.
62. Merrad, Y.; Habaebi, M.H.; Elsheikh, E.A.A.; Suliman, F.E.M.; Islam, M.R.; Gunawan, T.S.; Mesri, M. Blockchain: Consensus Algorithm Key Performance Indicators, Trade-Offs, Current

Trends, Common Drawbacks, and Novel Solution Proposals. *Mathematics* 2022, 10, 2754. <https://doi.org/10.3390/math10152754>.

63. You, I.; Kwon, S.; Choudhary, G.; Sharma, V.; Seo, J.T. An Enhanced LoRaWAN Security Protocol for Privacy Preservation in IoT with a Case Study on a Smart Factory-Enabled Parking System. *Sensors* 2018, 18, 1888. <https://doi.org/10.3390/s18061888>.

64. Alajmi, A.; Ghandoura, A.; Motwakel, A.; Abdelhady, G. Game-Theoretic Adaptive Routing and Integrated Security Framework for Multi-Hop LoRaWAN Networks. *IEEE Internet Things J.* 2026, early access. <https://doi.org/10.1109/JIOT.2026.3675915>.

65. Ray, P.P. A review on TinyML: State-of-the-art and prospects. *J. King Saud Univ. Comput. Inf. Sci.* 2022, 34, 1595–1623. <https://doi.org/10.1016/j.jksuci.2021.11.019>.

66. Khan, N.; Ahmad, K.; Al Tamimi, A.; Alani, M.M.; Bermak, A.; Khalil, I. Explainable AI-Based Intrusion Detection Systems for Industry 5.0 and Adversarial XAI: A Systematic Review. *Information* 2025, 16, 1036. <https://doi.org/10.3390/info16121036>.

67. National Institute of Standards and Technology (NIST). Module-Lattice-Based Key-Encapsulation Mechanism Standard; Federal Information Processing Standards Publication (FIPS PUB 203); NIST: Gaithersburg, MD, USA, 2024.

68. LoRa Alliance Technical Committee. LoRaWAN Regional Parameters v1.0.3; Technical Report; LoRa Alliance: Fremont, CA, USA, 2021.

69. Sakk, E.; Xu, G.; Mao, J.; Wang, S. Evaluating Post-Quantum Cryptography in IoT Networks: Communication, Fragmentation, and Reliability. *Future Internet* 2026, 18, 316. <https://doi.org/10.3390/fi18060316>.

70. Liu, T.; Ramachandran, G.; Jurdak, R. On the Energy Cost of Post-Quantum Key Establishment in Wireless Low-Power Personal Area Networks. In *Proceedings of the 2026 ACM/IEEE International Conference on Embedded Artificial Intelligence and Sensing Systems (SenSys '26)*, 2026. 1137–1143. <https://doi.org/10.1145/3774906.3802784>.

71. Butun, I.; Pereira, N.; Gidlund, M. Analysis of LoRaWAN v1.1 security: research paper. In *Proceedings of the 4th ACM MobiHoc Workshop on Experiences with the Design and Implementation of Smart Objects (SMARTOBJECTS '18)*, 2018. 1–6. <https://doi.org/10.1145/3213299.3213304>.