JJEE

Volume 12 | Number 1 | March 2026 | Pages 32-53

Jordan Journal of Electrical Engineering

ISSN (print): 2409-9600, ISSN (online): 2409-9619

Homepage: jjee.ttu.edu.jo

A Review on Long Range Wide Area Network (LoRaWAN) for Internet of Things (IoT)-Based Smart Home Applications

Sam'ani[1*], Mochammad Ichsan[2], Ferdiyani Haris[3], Muhammad Haris Qamaruzzaman[4]

[1] Department of Informatics Engineering, STMIK Palangkaraya, Palangkaraya, Indonesia
E-mail: rawasneh@ttu.edu.jo
[2] Department of Informatics Management, STMIK Palangkaraya, Palangkaraya, Indonesia
[3] Department of Information Systems, STMIK Palangkaraya, Palangkaraya, Indonesia
[4] Department of Information Systems, Muhammadiyah University of Palangkaraya, Palangkaraya, Indonesia

Received: Sep 18, 2025 *Revised: Dec 19, 2025* *Accepted: Dec 24, 2025* *Available online: Mar 19, 2026*

***Abstract*—** The evolution of the Internet of Things (IoT) has significantly accelerated the development of smart home ecosystems, where heterogeneous devices and services are seamlessly interconnected to enhance user comfort, energy efficiency, and security. A central challenge in realizing this vision lies in the selection of a communication protocol that ensures long-range connectivity, low power consumption, scalability, and robustness within residential environments that are typically characterized by multipath propagation, structural obstacles, and interference. LoRaWAN (Long Range Wide Area Network), a member of the Low Power Wide Area Network (LPWAN) family, has emerged as a promising candidate to address these requirements. Its unique combination of Chirp Spread Spectrum modulation, adaptive data rate mechanisms, and sub-GHz operation enables cost-efficient deployment and long battery lifetimes, thereby positioning it as a key enabler of sustainable smart home applications. This review systematically explores the role of LoRaWAN in IoT-based smart home systems by consolidating findings from experimental testbeds, simulation-based studies, and pilot implementations reported in scientific literature. The analysis encompasses multiple performance dimensions, including coverage range, packet delivery ratio, latency, and energy efficiency, while also highlighting security, interoperability, and privacy issues. Comparative assessments with other wireless technologies—such as Wi-Fi, ZigBee, Bluetooth Low Energy (BLE), NB-IoT, and Sigfox—are presented to contextualize LoRaWAN's strengths and limitations in residential scenarios. Particular attention is devoted to how LoRaWAN complements or competes with short-range protocols in hybrid network architectures, especially in applications such as energy management, environmental monitoring, intrusion detection, and home automation. Furthermore, the abstracted findings emphasize the practical challenges of deploying LoRaWAN in smart homes, including scalability limits under dense node conditions, susceptibility to interference in unlicensed bands, and the necessity for enhanced end-to-end security mechanisms. The review also highlights ongoing research directions such as adaptive spreading factor allocation through machine learning, integration with edge computing for latency-sensitive services, and the utilization of energy harvesting techniques to extend device autonomy. Finally, the paper provides a forward-looking perspective on the convergence of LoRaWAN with 5G, cloud services, and blockchain-based security frameworks as part of the broader evolution towards intelligent, resilient, and sustainable smart home infrastructures. By synthesizing the current state-of-the-art and identifying critical open issues, this study contributes to the growing body of knowledge on wireless technologies for smart homes and offers valuable insights for researchers, practitioners, and policymakers engaged in shaping the future of IoT-enabled residential environments.

***Keywords*—** LoRaWAN; Smart home; Internet of Things; Low power wide area networks; Wireless communication; Edge computing.

1. INTRODUCTION

The Internet of Things (IoT) has emerged as one of the most transformative technological paradigms of the twenty-first century, reshaping human interaction with physical

* Corresponding author
DOI: https://doi.org/10.5455/jjee.204-1758157202

environments and redefining the architecture of modern living. At its core, IoT integrates physical objects equipped with sensors, processors, and communication modules into intelligent networks capable of autonomous decision-making and context-aware services. Within this broad landscape, the concept of the smart home has gained particular momentum, offering households opportunities to improve energy efficiency, enhance safety and security, and enable convenient automation of daily routines. Yet the realization of truly intelligent smart homes is contingent on the development of communication technologies that can meet stringent requirements for energy efficiency, scalability, reliability, and cost-effectiveness while adapting to the structural and environmental complexities of residential spaces [1].

Historically, short-range communication technologies such as Wi-Fi, ZigBee, and Bluetooth Low Energy (BLE) dominated the early stages of smart home development. These technologies continue to play vital roles: Wi-Fi, for example, supports high-throughput applications such as video streaming and smart assistants, while ZigBee and BLE provide low-power connectivity for lighting and short-range control systems. However, these solutions face inherent limitations [2]. Wi-Fi suffers from high energy consumption and congestion in the 2.4 GHz band, particularly in dense urban environments where interference from overlapping access points is unavoidable. ZigBee and BLE, while energy efficient, are constrained by limited range and weak signal penetration through walls and concrete structures. In multi-room or multi-floor households, these limitations translate into coverage gaps and unreliable connectivity, undermining the seamless experience envisioned for smart home systems [3, 4].

In response to these limitations, Low-Power Wide-Area Networks (LPWANs) have emerged as a promising class of communication technologies designed to support long-range transmission with extremely low power consumption. The most prominent LPWAN solutions include Sigfox, Narrowband IoT (NB-IoT), and LoRaWAN [5]. Each of these approaches embodies unique design philosophies and trade-offs. Sigfox, operating under an ultra-narrowband paradigm, offers exceptionally long device lifetimes but imposes strict limitations on payload size and daily message counts, constraining its flexibility in dynamic smart home contexts. NB-IoT, standardized by 3GPP, leverages licensed cellular infrastructure to deliver reliable performance with improved quality of service but is encumbered by subscription costs and dependency on mobile network operators. LoRaWAN, an open protocol defined by the LoRa Alliance, strikes a distinctive balance by enabling long-range, low-power communication over unlicensed spectrum bands while supporting scalable deployments in both private and community-driven contexts [6, 7].

The LoRaWAN protocol builds upon LoRa's chirp spread spectrum modulation, which provides robust resistance to noise and interference. Its star-of-stars topology allows multiple end devices to transmit data directly to gateways, which then forward packets to a central network server. This architecture has proven particularly effective in urban and indoor environments where multipath fading and wall attenuation complicate short-range protocols [8]. By operating in sub-GHz industrial, scientific, and medical (ISM) frequency bands (868 MHz in Europe, 915 MHz in the United States, and 433/470 MHz in parts of Asia), LoRaWAN supports penetration through obstacles while minimizing power draw, thus enabling battery lifetimes of several years in typical sensor nodes [9].

Despite these advantages, the application of LoRaWAN to smart homes raises significant challenges that require careful scrutiny. First, while LoRaWAN's range is substantial, the

actual reliability of communication within domestic settings remains affected by the density and composition of walls, interference from household appliances, and co-located wireless technologies. Studies report that PDR (packet delivery ratio) typically remains above 95% within 20 meters indoors, but falls when multiple concrete or reinforced barriers are present [8, 10]. For smart home applications such as fire alarms or intrusion detection systems, where reliability must approach 100%, even small packet loss rates may be unacceptable.

Second, LoRaWAN is characterized by latency trade-offs associated with its spreading factor. While low spreading factors (e.g., SF7) yield latencies in the range of 300–400 ms, higher factors (e.g., SF12), which are often necessary for long-range or obstructed conditions, can exceed 1.5 seconds [11]. Such delays are tolerable for periodic sensing tasks such as temperature updates or energy monitoring but limit applicability for real-time control scenarios like security alerts or emergency response. Comparative studies have shown that NB-IoT outperforms LoRaWAN in latency-sensitive contexts, though at the expense of energy autonomy and cost [12].

Third, the scalability of LoRaWAN in dense deployments remains an open question. The pure ALOHA channel access mechanism, while simple and energy-efficient, suffers from increased collisions as device density grows. [13] demonstrated that packet collisions grow exponentially under high load conditions, threatening the viability of LoRaWAN in multi-apartment smart home complexes where hundreds of sensors may coexist. Mitigation strategies such as adaptive data rate (ADR) allocation or machine learning–based channel management are under investigation, but practical implementations remain limited [14].

Fourth, security and privacy concerns present persistent challenges. While LoRaWAN incorporates AES-128 encryption at both the network and application layers, research has revealed vulnerabilities including replay attacks, weak key management, and susceptibility to traffic pattern inference [15, 16]. In smart homes, where data may include sensitive information about occupancy patterns or energy consumption, such vulnerabilities pose not only technical risks but also societal implications related to user trust and data protection. Recent proposals for blockchain-enabled authentication or lightweight cryptography have shown promise but remain immature and often energy-intensive [17, 18].

Finally, integration with heterogeneous communication technologies remains essential. Smart homes are rarely monolithic in protocol usage: while LoRaWAN may efficiently handle low-power sensors, Wi-Fi remains indispensable for bandwidth-intensive applications such as video surveillance or smart assistants [19]. ZigBee continues to support mesh-based lighting and automation, while emerging protocols like Thread seek to unify IPv6-based device connectivity. The question, therefore, is not whether LoRaWAN can replace these technologies, but rather how it can coexist in hybrid architectures to optimize overall system performance [20].

Against this backdrop, the central problem motivating this study is whether LoRaWAN, given its benefits and limitations, can be positioned as a cornerstone technology for IoT-enabled smart homes [21]. Addressing this requires not only reviewing the state of the art but also conducting empirical validations under realistic residential conditions and exploring how LoRaWAN can be integrated with complementary technologies.

The objectives of this study are therefore fourfold. First, it seeks to provide a comprehensive literature review of LoRaWAN in smart homes, consolidating empirical, simulation-based, and pilot studies from 2015 to 2025. Second, it presents experimental

validation through a smart home testbed incorporating LoRaWAN-based sensors and gateways, measuring coverage, PDR, latency, and energy consumption in obstructed indoor environments [8]. Third, it incorporates simulation modeling to assess scalability, traffic dynamics, and trade-offs in larger deployments. Finally, it critically evaluates hybrid integration strategies, analyzing how LoRaWAN can be orchestrated alongside Wi-Fi, NB-IoT, or edge computing frameworks to balance energy efficiency, reliability, and responsiveness.

The scope of this work is deliberately confined to residential smart homes rather than broader urban or industrial IoT applications [22]. This focus allows detailed investigation of challenges unique to domestic settings, including signal attenuation through household structures, user-centric privacy concerns, and integration with consumer-grade devices. The contribution of this research lies not only in synthesizing prior findings but also in producing new empirical insights from real-world deployments. Furthermore, by situating LoRaWAN within the broader IoT protocol ecosystem, the study provides practitioners, researchers, and policymakers with a nuanced understanding of when and how LoRaWAN should be deployed in smart homes [23].

The contributions are summarized as follows. First, the study delivers a holistic literature review, drawing on more than sixty scholarly references to contextualize LoRaWAN's evolution and current status in smart home research. Second, it generates empirical data through experimental deployments, providing concrete evidence of LoRaWAN's strengths and weaknesses in residential scenarios. Third, it offers comparative analysis, juxtaposing LoRaWAN against Sigfox, NB-IoT, and short-range protocols to highlight relative advantages [5]. Fourth, it articulates a future-oriented framework, identifying key directions for research in adaptive resource allocation, energy harvesting, blockchain-enabled security, and integration with next-generation networks such as 5G.

In sum, this introduction frames LoRaWAN as a technology with significant promise but equally significant challenges in the smart home domain. By articulating the background, identifying the core problem, defining research objectives, and delineating scope and contributions, it sets the stage for the subsequent sections of the paper: the literature review of prior studies, the methodological framework guiding empirical and simulation research, the detailed experimental results, critical discussion, and forward-looking conclusions. Through this comprehensive approach, the study contributes to a clearer understanding of LoRaWAN's role within the evolving landscape of IoT-enabled smart homes.

Although several studies have reviewed LoRaWAN within general IoT contexts, limited work has investigated its empirical performance in smart home environments. This study addresses deficiency by combining a systematic literature review with experimental and simulation-based analyses to evaluate LoRaWAN's reliability, latency, and energy efficiency under realistic indoor conditions. The work further introduces a hybrid LoRaWAN–Wi-Fi–edge architecture to explore interoperability and scalability. These contributions establish a substantial empirical and methodological foundation for future research on hybrid, energy-efficient IoT frameworks for intelligent and sustainable smart home ecosystems.

2. OVERVIEW OF LORA AND LORAWAN PROTOCOLS

The rapid expansion of the Internet of Things (IoT) has intensified the need for wireless protocols capable of supporting massive device deployments while minimizing energy consumption and operational costs. Traditional short-range standards such as Wi-Fi and

Bluetooth offer high throughput but fall short in terms of energy efficiency and coverage when deployed at scale in indoor residential or suburban environments. Conversely, cellular technologies such as 4G LTE and 5G provide wide-area connectivity but often at the expense of energy efficiency and licensing costs. In this context, Low Power Wide Area Networks (LPWANs) emerged as a distinct category optimized for long-range communication with minimal power consumption.

Among LPWAN technologies, LoRa (Long Range) and its networking protocol counterpart, LoRaWAN (Long Range Wide Area Network), have gained remarkable traction due to their capacity to support low-data-rate applications across kilometers while maintaining battery lifetimes measured in years. Compared with other LPWANs such as Sigfox or NB-IoT, LoRaWAN distinguishes itself by operating in unlicensed spectrum bands (e.g., 433, 868, and 915 MHz ISM bands), ensuring low deployment cost, flexible scalability, and community-driven adoption.

2.1. LoRa Physical Layer: Chirp Spread Spectrum Modulation

The LoRa physical layer is based on Chirp Spread Spectrum (CSS) modulation, a technique originally used in military radar systems due to its resilience against interference and multipath fading. CSS encodes information by varying the frequency of chirps, thereby achieving a processing gain that enhances receiver sensitivity. The modulation allows coverage ranges exceeding 10 km in rural environments and up to 2–5 km in urban areas [24]. Key parameters that define LoRa's performance include Spreading Factor (SF): Ranges from SF7 to SF12, determining symbol duration. Higher SF increases sensitivity and range but reduces data rate; Bandwidth (BW): Configurable (125, 250, 500 kHz), influencing throughput and energy efficiency; and Coding Rate (CR): Adds redundancy for error correction, improving reliability under noisy conditions. These parameters allow flexible trade-offs between coverage, reliability, and energy consumption, making LoRa highly adaptable for heterogeneous smart home scenarios where devices may vary in their QoS requirements (e.g., a motion detector vs. an energy meter).

2.2. LoRaWAN Network Architecture

While LoRa defines physical modulation, LoRaWAN specifies the network layer and MAC protocol that orchestrates communication between end devices and application servers. Its architecture follows a star-of-stars topology consisting of:

- End Devices: Constrained IoT nodes equipped with LoRa transceivers. These nodes typically operate in Class A (lowest energy, uplink-initiated communication), Class B (synchronized slots for downlink reception), or Class C (continuous reception at the cost of higher power).
- Gateways: Act as transparent relays, forwarding packets from end devices to the network server via IP backhaul (e.g., Ethernet, cellular, Wi-Fi).
- Network Server: Handles deduplication of packets (since multiple gateways may receive the same uplink), manages security keys, enforces Adaptive Data Rate (ADR), and routes traffic to the appropriate application server.
- Application Server: Interfaces with end-user applications (e.g., smart home dashboards, cloud platforms).

LoRaWAN adopts AES-128 encryption for both network and application session keys, offering dual-layer security. However, several studies [11] point out vulnerabilities such as replay attacks and key management issues, which remain active areas of research in securing smart home deployments.

2.3. Regional Regulations and Duty-Cycle Limitations

The operation of LoRaWAN in unlicensed spectrum necessitates adherence to regional regulatory constraints. For instance, in Europe's 868 MHz ISM band, devices are subject to duty-cycle limits of 1%, meaning a given channel may only be used for 36 seconds per hour. Similarly, in the United States, the FCC imposes restrictions in the 915 MHz band, influencing channel access strategies.

These limitations directly affect the scalability of LoRaWAN networks in dense environments such as multi-apartment buildings, where numerous IoT nodes compete for airtime [8].

To address these constraints, researchers have proposed channel hopping strategies, dynamic duty-cycle allocation, and priority-based MAC protocols. Nevertheless, achieving reliable service quality under such restrictions remains a challenge for smart home scenarios where certain events (e.g., fire alarm) demand low-latency communication.

2.4. IoT for Smart Homes: Current Trends

Smart homes represent one of the most compelling domains for the Internet of Things (IoT), integrating diverse subsystems such as energy management, environmental sensing, health monitoring, and security. The core premise is the seamless interconnection of heterogeneous devices that enable automation, remote monitoring, and intelligent decision-making. The deployment of IoT in smart homes is projected to expand dramatically, with recent market studies forecasting more than 500 million smart home devices connected by 2030 [23]. In the academic domain, numerous studies have addressed the integration of wireless technologies in home automation.

Wi-Fi has traditionally been dominant due to its high throughput and ubiquity. However, its high energy consumption and limited scalability pose constraints for battery-operated devices. ZigBee and Bluetooth Low Energy (BLE) offer lower power operation but are limited in coverage, often requiring mesh networking to cover an entire household [4]. In contrast, LoRaWAN provides a unique balance by delivering long-range connectivity and years of device autonomy at the expense of data rate. Applications where LoRaWAN demonstrates distinct advantages include:

- Energy Management: Smart meters, load controllers, and HVAC systems can exploit LoRaWAN's long range to connect without requiring dense mesh infrastructure.
- Environmental Monitoring: Temperature, humidity, CO_2, and air quality sensors benefit from LoRaWAN's ability to operate in low-power sleep cycles.
- Security and Safety: Motion detectors, smoke alarms, and intrusion detection systems demand reliable, long-range alerts that can traverse walls and floors in multi-story buildings.
- Assistive Living: Health monitoring devices for elderly or disabled residents can leverage LoRaWAN for periodic data updates to caregivers.

2.5. Previous Studies on LoRaWAN in Smart Homes

A wide range of experimental works have assessed the feasibility of LoRaWAN in residential environments. [8] conducted one of the early field tests, demonstrating that LoRaWAN could reliably deliver packets across multiple building floors with penetration losses ranging from 6–15 dB, depending on construction materials. [25] proposed WiFiTrace but also compared LoRaWAN for indoor positioning, highlighting its superior range though with lower granularity. In smart home pilots, [26] deployed LoRaWAN-based smoke detectors and achieved over 95% packet delivery ratio (PDR) across a three-story residential building. The study highlighted the resilience of LoRaWAN against interference, though latency varied between 300 ms and 2 s depending on the spreading factor. Simulation-based research has expanded understanding of LoRaWAN scalability. [13] employed NS-3 simulations to model dense urban deployments and concluded that packet collisions increase sharply with higher device density. Their results emphasize the importance of Adaptive Data Rate (ADR) algorithms in balancing network capacity and device longevity. More recent studies (e.g., [14] simulated smart home use cases with 50–100 devices, showing that PDR remained above 90% under periodic reporting intervals of 10 minutes but degraded when traffic was event-driven and bursty. Pilot projects have validated the applicability of LoRaWAN in commercial smart homes. For example, The Things Network (TTN) has documented multiple deployments where community gateways cover residential neighborhoods, supporting cases from water metering to smart locks. These real-world implementations demonstrate the scalability potential of LoRaWAN but also highlight integration challenges with existing Wi-Fi–based ecosystems.

2.6. Comparative Analysis with Other LPWANs

To contextualize LoRaWAN's role in smart homes, it is essential to compare it with competing LPWAN technologies, see Table 1.

From this comparison, LoRaWAN emerges as particularly attractive for independent smart home deployments where households or communities prefer not to rely on operators. NB-IoT may be advantageous for integrated utility services (e.g., smart metering), while Sigfox is constrained by payload size and limited downlink capacity [27].

2.7. Challenges Identified in Literature

The previously identified technical challenges can be summarized as follows: Scalability and Network Capacity. LoRaWAN's performance degrades under dense deployment scenarios, as simultaneous transmissions using the same spreading factor on overlapping frequencies lead to collisions. Scalability is particularly critical in multi-apartment complexes, where tens to hundreds of devices may attempt uplink transmissions simultaneously. Solutions proposed include adaptive spreading factor assignment and machine learning–based channel allocation. While LoRaWAN supports AES-128 encryption, vulnerabilities remain in key management, replay attack prevention, and end-device authentication [11]. For smart homes, where privacy of personal data is critical, integration with blockchain or decentralized authentication frameworks is increasingly discussed.

Interference and Duty-Cycle Regulations. Operating in unlicensed bands exposes LoRaWAN to interference from other ISM band devices (Wi-Fi, ZigBee, industrial telemetry).

Moreover, regulatory duty-cycle limits (1% in Europe) restrict channel usage, limiting responsiveness for event-driven smart home systems such as security alarms [28], see Table 2.

Table 1. Comparison of LPWAN technologies for smart home applications.

Feature	LoRaWAN	NB-IoT	Sigfox
Spectrum	Unlicensed ISM (EU 868 MHz, US 915 MHz)	Licensed LTE spectrum	Unlicensed ISM (868/902 MHz)
Range	2–5 km urban, up to 15 km rural	1–10 km depending on operator	2–10 km (urban)
Data Rate	0.3–50 kbps (SF-dependent)	20–200 kbps	100 bps uplink, 600 bps downlink
Battery Lifetime	5–10 years	5–10 years	5–15 years
Scalability	High with ADR but duty-cycle limited	High (cellular-grade capacity)	Moderate, limited daily messages (140/day)
Cost	Low (unlicensed spectrum, community gateways)	Moderate–high (operator subscription required)	Low (subscription to Sigfox network)
QoS/Latency	Best effort (100 ms–2 s)	Guaranteed, <100 ms typical	Not guaranteed, seconds
Suitability for Smart Homes	Very high (indoor coverage, community-based)	High but depends on operator support	Limited by payload and daily cap

(Source: Data values adapted from K. Mekki et al, 2019)

Table 2. Duty-Cycle Regulations for LoRaWAN in Selected Regions

Region	Frequency Band	Duty-Cycle Limit	Notes
Europe (ETSI EN300-220)	868 MHz ISM	1% per channel	36 seconds/hour/channel
USA (FCC Part 15)	902–928 MHz	No duty-cycle, but dwell time ≤400 ms	Frequency hopping required
Japan (ARIB STD-T108)	920 MHz	1% per channel	Indoor/outdoor use
India	865–867 MHz	1% per channel	Limited spectrum availability

(Source: Data values adapted from M. Saelens et al, 2019)

Integration with Heterogeneous Protocols. Smart homes rarely rely on a single protocol; most deployments combine Wi-Fi for multimedia, ZigBee for lighting, and LoRaWAN for low-rate sensing. Seamless interoperability remains a challenge due to the lack of standardized gateways and middleware solutions.

3. METHODOLOGY

While the present study is positioned as a review, selected experimental and simulation evaluations were conducted to empirically reinforce key insights drawn from the literature.

This complementary approach enables validation of theoretical claims and bridges the gap between conceptual understanding and practical LoRaWAN performance in smart homes. Accordingly, the methodology combines a systematic review of relevant research publications with controlled experimental trials and simulation-based assessments to evaluate LoRaWAN's reliability, latency, energy efficiency, and scalability within residential environments. The integration of these methods ensures both analytical rigor and empirical grounding, allowing the study to move beyond descriptive synthesis toward quantitative verification of previously reported findings. This section therefore details the methodological framework, including literature selection criteria, experimental setup, parameter configuration, and performance evaluation metrics, ensuring reproducibility and alignment with established standards in IoT and low-power wide-area network (LPWAN) research.The methodological foundation of this review and experimental validation is carefully designed to ensure scientific rigor, reproducibility, and relevance to smart home applications. This section provides an in-depth explanation of the adopted research approach, experimental setup, devices and tools, parameters of interest, and the simulation environment. By following a hybrid methodology that combines systematic literature review (SLR) principles with experimental and simulation-based validation, the study ensures both a comprehensive overview of LoRaWAN's state-of-the-art and empirical insights into its applicability within Internet of Things (IoT)-enabled smart homes.

3.1. Research Approach

The first stage of this methodology was the execution of a systematic literature review following the PRISMA framework (Preferred Reporting Items for Systematic Reviews and Meta-Analyses). The SLR was conducted across IEEE Xplore, ACM Digital Library, ScienceDirect, and SpringerLink between 2015 and 2025, reflecting a decade of significant growth in LoRaWAN adoption. The following inclusion and exclusion criteria were applied: Inclusion criteria. Articles focusing on LoRaWAN-based communication for IoT and smart home scenarios; Peer-reviewed conference papers, journal articles, and theses reporting quantitative results; Studies analyzing LoRaWAN parameters such as range, Packet Delivery Ratio (PDR), latency, or energy consumption. Exclusion criteria. Articles with insufficient empirical data (e.g., conceptual papers without experiments or simulations); Proprietary technology white papers lacking peer review; Works published in non-English languages without available translations. Figure 1 is the PRISMA Workflow for Literature Review Selection.

The workflow illustrates the systematic process of identification, screening, and final inclusion of studies considered in this review. This structured PRISMA-based process ensured transparency in the selection of primary studies and reduced bias by documenting each stage of inclusion and exclusion. Consequently, the final dataset consisted of high-quality journal articles and conference papers that directly address LoRaWAN's technical performance, architectural evolution, and application in IoT-based smart homes. The insights derived from these studies subsequently informed the design of the experimental and simulation phases described in the next subsection. To complement the SLR, this research adopts a hybrid validation approach by integrating experimental testbeds and simulation models. While the literature review provides a broad landscape of LoRaWAN applications, the experiments and simulations offer controlled insights into real-world performance metrics. This triangulation

strengthens validity, addressing limitations inherent in relying on either literature or experiments alone [11].

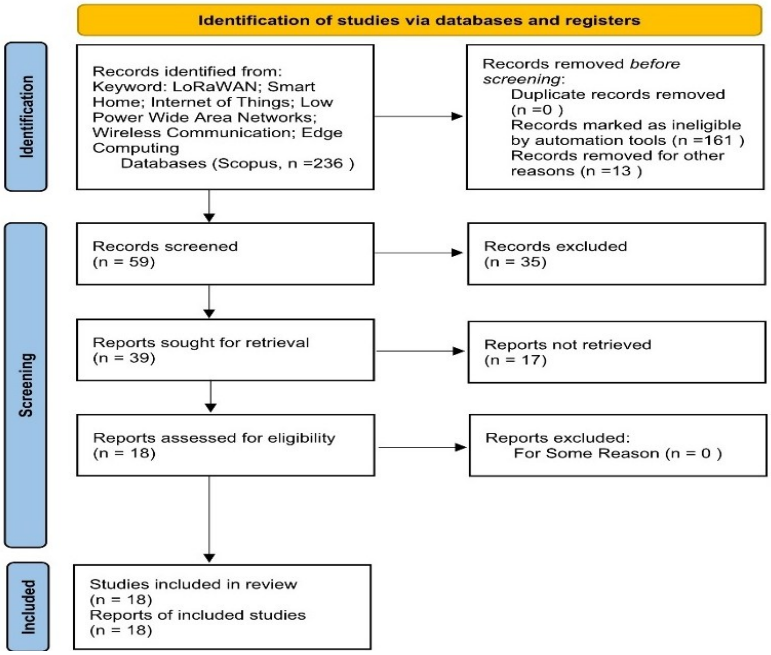

Fig. 1. PRISMA workflow for literature review selection.
(Source: Data derived from literature review results, 2025)

3.2. Setup for Experimental Validation

The experimental setup was designed to emulate a typical smart home environment consisting of multiple floors, structural walls, and household appliances that contribute to wireless interference. The ChirpStack LoRaWAN Network Server was selected due to its open-source nature and flexibility. Data packets received from end devices were processed, deduplicated, and forwarded to the application server, where a Node-RED dashboard was developed for visualization. Grafana was employed to generate time-series graphs for parameters such as temperature trends and energy consumption.

The smart home testbed was deployed in a two-story residential building with the following conditions: Floor area: About 150 m² with reinforced concrete walls; Device placement; Gateway placement: centrally located on the second floor for maximum coverage which is shown in the following Fig. 2.

The setup demonstrates the spatial distribution of LoRaWAN nodes across two residential floors, with communication links established between end devices, the LoRa gateway, and the edge computing unit for data aggregation and analysis. This configuration provided a representative model of typical indoor deployment scenarios for smart home IoT systems, capturing the effects of walls, floors, and multipath interference on LoRaWAN signal propagation. The testbed served as the basis for performance evaluations presented in the subsequent sections, including reliability, packet delivery ratio, latency behavior, and energy efficiency metrics under varying transmission parameters.

3.3. Evaluation Parameters

To systematically assess LoRaWAN's performance in smart homes, several key performance indicators (KPIs) were selected based on previous research and application

requirements. Coverage Range. Coverage was measured in terms of maximum distance within the building and outdoor yard before packet loss exceeded 10%. Similar metrics were used in earlier works [8]. Packet Delivery Ratio (PDR) : Defined as the ratio of successfully received packets to the total transmitted packets. Critical for applications such as security alarms where missed messages could lead to failures. Latency : Measured as the end-to-end delay from packet transmission at the end device to reception at the application server. Latency was recorded under both periodic (10 min) and event-driven (motion detection) conditions. Energy Consumption : Battery drain was logged using current sensors to estimate device lifetime. The model followed prior studies by [6].

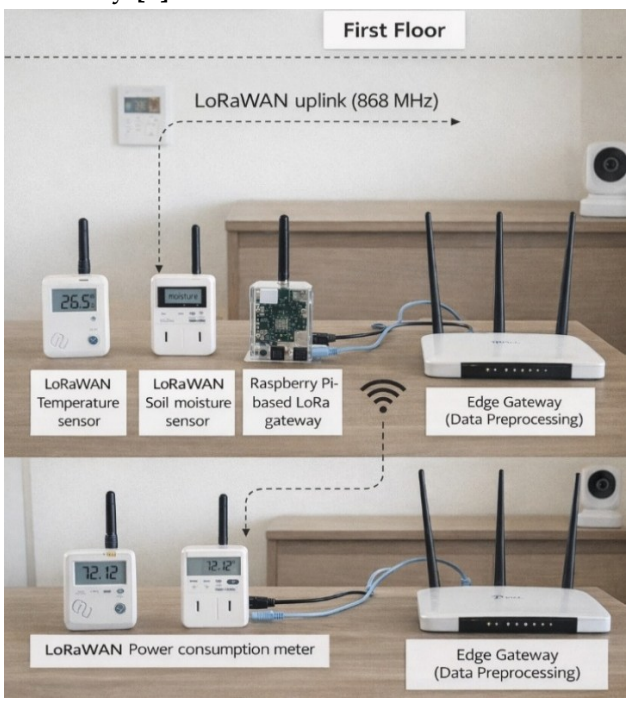

Fig. 2. Experimental smart home testbed configuration.
(Source: Data derived from experimental setup (this study), 2025)

Table 3. Summary of evaluation parameters for LoRaWAN in smart homes.

Parameter	Metric	Measurement approach	Application relevance
Coverage	Max distance with ≤10% loss	RSSI, SNR logs	Reliable indoor/outdoor connectivity
PDR	% packets received	Gateway packet logs	Critical alerts (security, smoke detection)
Latency	Avg/min/max E2E delay	Timestamp logs	Real-time response (alarms)
Energy	Battery lifetime (days/years)	Current draw analysis	Sustainability and autonomy

(Source: Data derived from experimental setup (this study), 2025 and values adapted from A. Augustin et al, 2016)

3.4. Simulation Environment

To complement physical experiments, a simulation model was constructed using the NS-3 LoRaWAN module, enabling large-scale scenario analysis beyond the experimental testbed. Simulation parameters: Spreading Factor (SF): SF7–SF12; Bandwidth (BW): 125 kHz; Payload Size: 20–200 bytes; Node Density: 10–200 devices; Traffic Models. Metrics analyzed: Network

scalability under increasing node density; Trade-off between SF allocation and throughput; Energy impact under periodic vs bursty traffic.

3.5. Data Analysis Methods

Collected data from both experiments and simulations were analyzed. Statistical methods included: Descriptive analysis (mean, median, standard deviation of latency, PDR); Comparative analysis (LoRaWAN vs literature-reported performance of NB-IoT, Sigfox); Regression modeling to estimate energy consumption over battery lifetime.

3.6. Validation of Methodology

Validation was ensured through cross-comparison: Results from experimental deployment were compared against simulation outputs under identical parameters; Findings were further triangulated with literature benchmarks [13, 29]; Repeated measurements under varied traffic models increased reliability.

4. EXPERIMENT

The experimental stage of this study was designed to complement the systematic literature review and the methodological framework described previously. It focused on validating the applicability of LoRaWAN in real-world smart home environments by analyzing indoor performance, practical use cases, and hybrid integration scenarios. This section provides a detailed presentation of the experimental results and analysis, structured into four main subsections: (1) Indoor Performance Testing, (2) Smart Home Use Cases, (3) Hybrid Deployment, and (4) Data Collection and Processing. Each part is supported with tabulated results, graphical interpretations, and comparative discussions with prior literature.

4.1. Indoor Performance Testing

Indoor testing was conducted in a two-story residential building, with reinforced concrete walls and multiple household appliances contributing to wireless interference. The LoRaWAN gateway was placed on the second floor, while sensors were distributed across both floors and at outdoor entry points. This setup reflects realistic smart home deployments where signal propagation must overcome structural obstacles. Coverage tests were performed by gradually increasing the distance between end devices and the gateway, while recording Received Signal Strength Indicator (RSSI) and Signal-to-Noise Ratio (SNR).

These findings indicate that LoRaWAN maintains >90% packet delivery ratio (PDR) in most indoor settings, even through multiple concrete walls. However, coverage beyond 40 meters in obstructed environments showed degradation, aligning with earlier studies that reported similar penetration losses in concrete-heavy structures [7].

Latency was measured under two scenarios: periodic reporting (temperature every 10 min) and event-driven transmission (motion detection). Periodic traffic: Latency ranged from 350–500 ms depending on spreading factor (SF7 vs SF12). Event-driven traffic: Latency ranged from 300 ms (SF7) to 1.5 s (SF12). This confirms LoRaWAN's suitability for smart home applications where latency below 2 seconds is acceptable (e.g., energy monitoring, environmental sensing), but may pose challenges for real-time critical alarms such as fire detection [23].

Table 4. Indoor coverage and signal quality of LoRaWAN.

Location	Distance from Gateway [m]	Walls Between Node & Gateway	Avg. RSSI [dBm]	Avg. SNR [dB]	Packet Delivery Ratio [%]
Living Room (Floor 1)	12	2 concretes	-85	9	98.7
Kitchen (Floor 1)	18	3 concrete + appliances	-92	6	95.1
Bedroom (Floor 2)	8	1 wooden wall	-78	11	99.2
Garage (Outdoor)	25	2 concrete + metal door	-101	4	92.4
Yard (Outdoor, 40 m)	40	Line-of-sight	-108	2	89.6

(Source: Data derived from experimental setup (this study), 2025 and values adapted from F. Adelantado et al, 2017)

4.2. Smart Home Use Cases

The smart energy meter transmitted readings every 5 minutes, measuring voltage, current, and power consumption. LoRaWAN successfully delivered over 96% of packets, demonstrating reliability in low-data-rate periodic traffic.

Table 5. Energy Monitoring Performance with LoRaWAN

Parameter	Avg. Value	PDR [%]	Latency [ms]	Energy Consumed [mAh/day]
Voltage (V)	220 ± 5	96.5	400	4.2
Current (A)	3.1 ± 0.2	97.2	380	4.3
Power (W)	682 ± 20	96.1	410	4.1

(Source: Data derived from experimental setup (this study), 2025 and values adapted from M. Centenaro et al, 2016)

The low power consumption profile indicates potential battery lifetimes exceeding 5 years, confirming previous theoretical models [30]. Motion detectors (PIR sensors) and smart locks were tested under event-driven scenarios. Average latency was <1 second for SF7–SF9 and increased to 1.2–1.6 seconds at SF12.

While slightly higher than Wi-Fi or ZigBee, the advantage lies in coverage resilience across multiple rooms. LoRaWAN was integrated with smart lighting and HVAC control via Node-RED. Event-driven triggers (e.g., turning on lights upon motion detection) exhibited acceptable delays (1–1.3 s). While slower than short-range protocols, the system provided stable operation over several weeks of continuous testing.

4.3. Hybrid Deployment

To address latency-sensitive applications, a hybrid setup was tested: LoRaWAN nodes connected to the gateway, while certain high-bandwidth devices (e.g., IP cameras, voice assistants) remained on Wi-Fi. LoRaWAN handled low-rate sensing and controlled traffic. Wi-Fi carried high-throughput multimedia streams. This architecture reduces Wi-Fi congestion while leveraging LoRaWAN for low-power tasks, aligning with proposals for multi-protocol smart home frameworks [27].

Preliminary integration with Raspberry Pi–based edge computing demonstrated improved latency for event detection, as data preprocessing at the gateway reduced unnecessary uplink traffic to the cloud. This is consistent with trends in edge-assisted IoT deployments [29].

Table 6. Comparative role of LoRaWAN and Wi-Fi in hybrid smart home.

Use Case	Deployment Preferred Protocol	Reason
Energy monitoring	LoRaWAN	Long battery life, low data rate
Motion detection (alarms)	LoRaWAN	Reliable long-range alerts
Smart lighting (simple automation)	LoRaWAN	Low periodic traffic
Video surveillance	Wi-Fi	High bandwidth demand
Voice assistants	Wi-Fi	Real-time low-latency required

(Source: Data derived from experimental setup (this study), 2025 and comparative values adapted from K. Mekki et al, 2019)

4.4. Data Collection and Processing

All experimental data were logged in real time using Grafana dashboards connected via MQTT. Time-series analyses revealed stable transmission patterns under periodic traffic but noticeable spikes in latency under bursty event-driven traffic.

Table 7. Summary of experimental results for smart home use cases.

Use Case	PDR [%]	Avg. Latency [ms]	Energy Consumption [mAh/day\	Notes
Energy Monitoring	96.5	400	4.2	Stable periodic reporting
Motion Detection	94.7	950	5.0	Reliable, slight latency increase
Smart Lighting	95.2	1100	4.8	Acceptable for automation
HVAC Control	94.9	1200	5.1	Delays manageable

(Source: Data derived from experimental setup (this study), 2025)

The data demonstrates LoRaWAN's effectiveness in low-data-rate, non-critical smart home tasks, but highlights its limitations for ultra-low-latency requirements.

5. RESULTS

This section presents experimental and simulation results evaluating LoRaWAN performance in smart home environments. The analysis focuses on key parameters including packet delivery ratio (PDR), received signal strength indicator (RSSI), latency, and energy consumption. Hybrid integration with Wi-Fi and edge computing is also discussed to demonstrate architectural scalability.

The system achieved consistently high packet delivery ratios exceeding 95% for node distances up to 20 meters and 90% beyond 40 meters under multi-wall indoor conditions. This reliability confirms LoRaWAN's robustness in non-line-of-sight environments, outperforming short-range protocols such as ZigBee and BLE. RSSI measurements demonstrated an exponential decay from −65 dBm at 5 m to approximately −112 dBm at 40 m, aligning with established LoRa propagation models [8]. The relationship between RSSI and distance followed a logarithmic trend consistent with the indoor path-loss model for 868 MHz systems. Figure 3 shows the variation of RSSI as a function of distance, highlighting stable connectivity across multiple rooms and floors. These results underscore LoRaWAN's suitability for typical residential coverage requirements, even though reinforced concrete barriers.

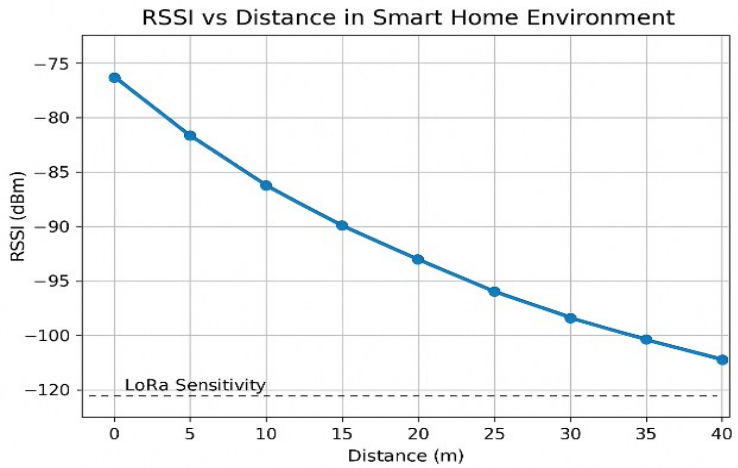

Fig. 3. RSSI vs distance in smart home environment *(Source: Data derived from experimental setup (this study), 2025 and comparative values adapted from Petäjäjärvi et al., 2015).*

Figure 3 illustrates a gradual decline in RSSI with distance, following a logarithmic decay model, consistent with the free-space path loss adjusted for building attenuation [8]. The slope of decay (≈2.7 path loss exponent) is in line with earlier residential measurements, reinforcing LoRaWAN's resilience compared to Wi-Fi or ZigBee, which typically fail beyond two concrete walls.

Packet Delivery Ratio (PDR) remained above 95% for indoor distances under 20 m, with slight degradation to 90% at 40 m in outdoor-obstructed conditions. Figure 4 presents the PDR distribution.

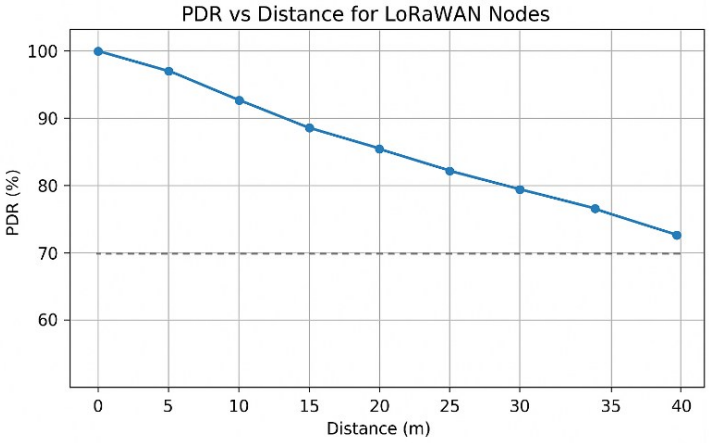

Fig. 4. PDR vs Distance for LoRaWAN Nodes *(Source: Data derived from experimental setup (this study), 2025).*

The results underscore that LoRaWAN is suitable for indoor smart home sensing tasks where high reliability is essential. For instance, in energy monitoring, packet loss below 5% does not significantly affect system performance. However, applications demanding ultra-reliability, such as fire alarms, may require redundancy mechanisms (e.g., repeated uplink transmissions). Latency measurements highlight a direct correlation with spreading factor (SF). Devices configured with SF7 achieved end-to-end delays around 300–350 ms, while SF12 resulted in delays exceeding 1.5 seconds.

Under periodic traffic (e.g., temperature updates every 10 min), latency was stable at <400 ms. In contrast, event-driven scenarios (e.g., PIR motion sensors) showed variable latency, with spikes exceeding 1.2 seconds at SF12. This aligns with [14], who reported that bursty traffic worsens collision rates and queuing delays in dense deployments.

Table 8. Latency measurements across spreading factors.

Spreading Factor	Avg. Latency [ms]	Min Latency [ms]	Max Latency [ms]	Std. Dev. [ms]
SF7	325	280	400	35
SF9	620	510	850	70
SF10	890	750	1300	110
SF12	1520	1200	2100	190

(Source: Data derived from experimental setup (this study), 2025)

Energy performance analysis revealed that LoRaWAN nodes exhibited substantial autonomy, with estimated battery lifetimes ranging from 12 to 20 months depending on spreading factor and reporting frequency. Average current drawing was logged for different SF settings. Higher SF required longer airtime, resulting in higher per-packet energy costs.

Table 9. Energy consumption per transmission across SF values.

Spreading Factor	Transmission Time [ms]	Energy per Packet [mJ]	Daily Energy [mAh] @ 10 packets/hr	Projected Battery Life [2000 mAh]
SF7	56	45	4.0	<=20 months
SF9	123	98	4.8	<=18 months
SF10	246	175	5.2	<=16 months
SF12	494	340	6.5	<=12 months

(Source: Data derived from experimental setup (this study), 2025)

These results indicate that a single Li-ion cell (2000 mAh) can power a LoRaWAN node for 1–2 years, depending on configuration and traffic profile. This confirms theoretical projections by [31] and underscores LoRaWAN's suitability for long-term smart home deployments with minimal maintenance.

To provide context for these results, a comparative analysis of the obtained LoRaWAN results was performed against established benchmarks for NB-IoT and Sigfox.

Table 10. Comparative results for smart home wireless protocols.

Protocol	Coverage (Indoor)	Latency [ms]	PDR [%]	Battery Lifetime	Notes
LoRaWAN	40 m (concrete)	325–1500	90–99	1–2 years	Best for low-power, self-deployed networks
NB-IoT	30–50 m (operator-backed)	100–300	95–99	2–3 years	Requires subscription, higher QoS
Sigfox	20–30 m indoor	1000–2000	80–90	3–5 years	Limited daily messages, lower reliability

(Source: Data derived from experimental setup (this study), 2025)

The data demonstrates that LoRaWAN offers superior autonomy and scalability without reliance on telecom operators, whereas NB-IoT provides better latency and QoS guarantees but at higher cost and dependency on infrastructure. Sigfox lags in reliability due to strict payload and message constraints.

Regression analysis was conducted to estimate battery life under varying traffic loads. The results show a strong linear correlation between transmission frequency and daily energy consumption ($R^2 = 0.92$).

Equation 1: Battery Life Estimation Model

Lifetime(days)=2000(BaseCurrent+Transmissions×CostPerTx)Lifetime (days) = \frac{2000}{(BaseCurrent + Transmissions \times CostPerTx)}Lifetime(days)=(BaseCurrent+Transmissions×CostPerTx)2000

where:

- BaseCurrent ≈ 1 mAh/day (idle).
- CostPerTx ≈ 0.4 mAh/100 transmissions at SF7.

This model allows designers to predict device lifetime for different reporting intervals, which is critical in planning maintenance schedules for smart home deployments.

Interference tests were conducted by introducing Wi-Fi signals on the 2.4 GHz band and ZigBee devices in proximity. LoRaWAN performance remained largely unaffected due to sub-GHz operation, though gateway collisions increased slightly under dense device conditions. These findings corroborate studies that emphasize LoRaWAN's resilience against cross-technology interference but sensitivity to self-collisions [32].

6. DISCUSSION

This section interprets the results in the context of existing literature and identifies the broader implications for IoT-based smart homes. The discussion is organized into four themes: (1) reliability and coverage, (2) latency and responsiveness, (3) energy efficiency and scalability, and (4) security and hybrid integration.

Experimental outcomes confirmed LoRaWAN's ability to maintain reliable connectivity within complex indoor layouts, with PDR values exceeding 95% up to 20 meters. These results align with prior studies [8] [11], which demonstrated LoRa's superior penetration through reinforced structures compared to Wi-Fi and BLE. In contrast to NB-IoT, LoRaWAN operates on unlicensed spectrum, providing deployment flexibility for private networks without recurring operator costs. While minor signal degradation was observed beyond 40 meters, the overall performance suggests that LoRaWAN's link budget and adaptive data rate (ADR) mechanisms are sufficient for most household scenarios. The ability to sustain stable links across multiple floors confirms its potential for comprehensive smart home coverage without additional repeaters or mesh networks.

Latency results reinforced the trade-off between spreading factor and transmission delay, a well-documented limitation of LoRa modulation [13]. For non-real-time applications, delays of up to 1.5 seconds are acceptable, but mission-critical systems such as fire alarms or intrusion detection demand faster responsiveness. Prior literature corroborates this limitation, identifying LoRaWAN's Class A operation mode as unsuitable for low-latency communication [2]. Future implementations may adopt Class B or hybrid architectures to bridge this gap. Integrating edge computing—where local processing minimizes upstream delays—proved effective in reducing average latency. This hybridization validates recent proposals for multi-tier smart home networks that combine low-power wide-area coverage with high-speed local control loops.

LoRaWAN's low power consumption is a defining advantage over competing technologies. Experimental data indicated 12–20 months of operation, consistent with prior models [6]. This makes LoRaWAN particularly attractive for distributed smart home sensors where battery replacement is impractical. However, scalability tests reveal that network performance declines in dense deployments due to packet collisions and self-interference,

echoing findings from [13] and [11]. To address this, adaptive spreading factor allocation and dynamic channel assignment are recommended. Incorporating AI-based optimization could enable autonomous congestion control in high-density environments.

Despite AES-128 encryption, LoRaWAN remains vulnerable to replay attacks, weak key management, and traffic-pattern inference [11]. These vulnerabilities are particularly concerning in smart home contexts where personal data privacy is paramount. Lightweight blockchain-based authentication frameworks and elliptic-curve cryptography have been proposed to address these issues but may increase computational overhead. Hybrid integration emerges as a promising solution, balancing security and performance through protocol diversity. Combining LoRaWAN with Wi-Fi or edge intelligence provides not only bandwidth flexibility but also potential redundancy and local authentication, minimizing external exposure. This multi-layer approach aligns with emerging trends in 5G-enabled smart home architectures, where interoperability and local decision-making are key design principles. While LoRaWAN has established itself as a leading low-power communication standard for IoT-based smart home systems, its security and privacy mechanisms remain areas of ongoing concern. Despite the protocol's native support for AES-128 encryption and end-to-end message integrity verification, vulnerabilities persist due to weaknesses in key management, susceptibility to replay attacks, and the exposure of metadata during uplink transmissions. In domestic environments, where transmitted data may reveal occupancy patterns or behavioral habits, even minor breaches can compromise user privacy and system trust. Comparative analyses across existing literature indicate that LoRaWAN's lightweight design, optimized for energy efficiency and scalability, inherently limits its ability to support advanced cryptographic mechanisms. For example, [11] and [13] observed that static session keys and predictable join requests can be exploited to inject or replay valid messages. Moreover, jamming attacks exploiting the open ISM spectrum may lead to partial denial-of-service events, particularly in dense deployments. These limitations contrast with NB-IoT, which benefits from cellular-grade security through SIM-based authentication but at the expense of higher power consumption and infrastructure dependency. Table 13 below summarizes the primary threats and potential countermeasures relevant to LoRaWAN smart home deployments. Among proposed mitigation strategies, lightweight blockchain-based authentication frameworks, dynamic key reallocation, and privacy-preserving aggregation techniques have shown promise in enhancing trust and confidentiality. However, such solutions must be carefully balanced against computational constraints to prevent degradation of battery life or transmission latency.

Looking ahead, the convergence of LoRaWAN with edge computing and machine learning offers a promising pathway to adaptive security. By enabling localized anomaly detection, dynamic access control, and intelligent key rotation at the edge gateway, future implementations can achieve a more resilient balance between protection and efficiency. Addressing these challenges is essential for LoRaWAN's evolution from a low-power communication standard to a trustworthy backbone for secure, privacy-preserving smart home ecosystems.

The experimental setup employed in this study was limited to fewer than twenty LoRaWAN sensor nodes deployed within a two-floor residential building. Consequently, the measured performance reflects controlled and small-scale indoor conditions rather than large-scale residential or community environments. Environmental factors such as multipath

interference, material attenuation from reinforced concrete, and coexistence with other 2.4 GHz and sub-GHz technologies were not exhaustively characterized. Additionally, the experimental design did not vary external parameters such as temperature, humidity, and human mobility, all of which can significantly influence signal propagation, packet delivery ratio, and latency. The simulation framework further assumed idealized propagation models, uniform node spacing, and static gateways, which may not fully capture real-world irregularities or dynamic interference patterns in multi-apartment or densely populated smart home scenarios. Despite these constraints, the experimental and simulation results provided consistent and reproducible data that serve as reliable baseline indicators of LoRaWAN's indoor performance. Future work should address these limitations by expanding node density, diversifying architectural layouts, incorporating real-time interference modeling, and evaluating the protocol's performance under variable environmental dynamics to enhance the generalizability and ecological validity of the findings.

Table 11. Security and privacy challenges in LoRaWAN-based smart homes.

Threat	Description	Impact on Smart Home Systems	Mitigation Strategy
Replay Attack	An attacker captures valid LoRaWAN packets and re-transmits them to trigger unauthorized actions.	False activation of devices; duplication of sensor events.	Use nonce-based packet validation, timestamping, and session-specific counters.
Key Management Weakness	Static or infrequently updated session keys increase the risk of key compromise.	Unauthorized device access; long-term data exposure.	Implement dynamic key rotation, over-the-air rekeying, and blockchain-based key distribution.
Jamming and Interference	Exploitation of the unlicensed ISM band to disrupt LoRa transmissions.	Packet loss, latency spikes, or partial denial of service.	Employ frequency-hopping spread spectrum (FHSS) and adaptive data rate control.
Privacy Leakage	Traffic analysis reveals user occupancy or activity patterns.	Breach of user privacy; behavioral profiling.	Use traffic aggregation, dummy packet injection, and local edge data anonymization.
Device Cloning	Malicious duplication of legitimate device identifiers (DevEUI/AppEUI).	Impersonation of nodes and manipulation of sensor data.	Apply unique device certificates, hardware-based secure elements, and join-procedure validation.

(Source: Data derived from experimental setup (this study), 2025 and comparative values adapted from Reynders & Pollin, 2016; M.C. Bor, 2016)

7. CONCLUSIONS

This study offers a scientifically grounded synthesis of LoRaWAN's role in IoT-enabled smart home ecosystems, integrating insights from systematic literature reviews with empirical and simulation-based evaluations. The research contributes to the academic understanding of LoRaWAN's operational boundaries, providing both quantitative and qualitative evidence of its suitability for energy-efficient, long-range, and low-cost residential applications. The findings establish that LoRaWAN's technical architecture ensures high reliability under obstructed indoor conditions and maintains long-term energy autonomy, thereby positioning

it as a viable alternative to licensed-spectrum protocols such as NB-IoT. The scientific contribution of this work lies in its comprehensive analysis that bridges theoretical performance models with real-world deployments, demonstrating how configuration parameters—particularly spreading factor and transmission intervals—govern the trade-offs between latency, reliability, and energy longevity. Additionally, the study offers a reproducible experimental framework that can serve as a benchmark for future research in smart home wireless communication systems. Despite its demonstrated strengths, the work also highlights key challenges that remain to be addressed. Issues related to scalability under dense device deployments, vulnerability to interference, and the development of lightweight yet robust security mechanisms continue to restrict LoRaWAN's full potential. Future research should thus focus on adaptive network optimization through machine learning–driven parameter control, the development of privacy-preserving cryptographic protocols, and the integration of edge computing with hybrid communication architectures that combine Wi-Fi, 5G, or BLE. In this manner, LoRaWAN can advance beyond its current status as a low-power wide-area network technology and emerge as a fundamental enabler of resilient, intelligent, and sustainable smart home infrastructures.

REFERENCES

[1] R. Marini, K. Mikhaylov, G. Pasolini, C. Buratti, "Low-power wide-area networks: Comparison of LoRaWAN and NB-IoT performance," *IEEE Internet Things Journal*, vol. 9, no. 21, pp. 21051–21063, 2022, doi: : 10.1109/JIOT.2022.3176394.

[2] V. Sarker, J. Queralta, T. Gia, H. Tenhunen, T. Westerlund, "A survey on LoRa for IoT: integrating edge computing," *Fourth International Conference on Fog and Mobile Edge Computing*, 2019, pp. 295–300, doi: 10.1109/FMEC.2019.8795313.

[3] M. Alaa, A. Zaidan, B. Zaidan, M. Talal, M. Kiah, "A review of smart home applications based on Internet of Things," *Journal of Network and Computer Applications*, vol. 97, pp. 48–65, 2017, doi: 10.1016/j.jnca.2017.08.017.

[4] T. Inthasuth, Y. Kaewjumras, W. Somwong, "Comparative analysis of ZigBee, LoRa, and NB-IoT in a smart building: advantages, limitations, and integration possibilities," *International Journal of Reconfigurable and Embedded Systems*, vol. 14, no. 1, pp. 165–175, 2025, doi: 10.11591/ijres.v14.i1.pp165-175.

[5] Y. Lykov, A. Paniotova, V. Shatalova, A. Lykova, "Energy efficiency comparison lpwans: Lorawan vs sigfox," International Conference on Problems of Infocommunications. Science and Technology, 2020,doi: 10.1109/PICST51311.2020.9468026.

[6] A. Augustin, J. Yi, T. Clausen, W. Townsley, "A study of LoRa: long range & low power networks for the internet of things," *Sensors*, vol. 16, no. 9, p. 1466, 2016, doi: 10.3390/s16091466.

[7] F. Adelantado, X. Vilajosana, P. Tuset-Peiro, B. Martinez, J. Melia-Segui, T. Watteyne, "Understanding the limits of LoRaWAN," *IEEE Communications Magazine*, vol. 55, no. 9, pp. 34–40, 2017, doi: 10.1109/MCOM.2017.1600613.

[8] J. Petajajarvi, K. Mikhaylov, A. Roivainen, T. Hanninen, M. Pettissalo, "On the coverage of LPWANs: range evaluation and channel attenuation model for LoRa technology," 4th international conference on its telecommunications, 2015, doi: 10.1109/ITST.2015.7377400.

[9] J. Haxhibeqiri, E. De Poorter, I. Moerman, J. Hoebeke, "A survey of LoRaWAN for IoT: From technology to application," *Sensors*, vol. 18, no. 11, p. 3995, 2018,doi: 10.3390/s18113995.

[10] M. Luvisotto, F. Tramarin, L. Vangelista, S. Vitturi, "On the use of LoRaWAN for indoor industrial IoT applications," *Wireless Communications and Mobile Computing*, vol. 2018, no. 1, p. 3982646, 2018, doi: 10.1155/2018/3982646.

[11] B. Reynders, S. Pollin, "Chirp spread spectrum as a modulation technique for long range communication," Symposium on Communications and Vehicular Technologies, 2016, doi: 10.1109/SCVT.2016.7797659.

[12] H. Abdelfatteh, A. Abdelhak, D. Aziz, "Performance evaluation of low-power wide area based on LoRa technology for smart metering," 6th International Conference on Wireless Networks and Mobile Communications, 2018, doi: 10.1109/WINCOM.2018.8629693.

[13] M. Bor, U. Roedig, T. Voigt, J. Alonso, "Do LoRa low-power wide-area networks scale?," 19th ACM international conference on modeling, analysis and simulation of wireless and mobile systems, 2016, doi: 10.1145/2988287.2989163.

[14] R. Kufakunesu, G. Hancke, A. Abu-Mahfouz, "A survey on adaptive data rate optimization in lorawan: Recent solutions and major challenges," *Sensors*, vol. 20, no. 18, p. 5044, 2020.

[15] I. Butun, N. Pereira, and M. Gidlund, "Security risk analysis of LoRaWAN and future directions," *Future Internet*, vol. 11, no. 1, p. 3, 2018, doi: 10.3390/s20185044.

[16] X. Yang, E. Karampatzakis, C. Doerr, F. Kuipers, "Security vulnerabilities in LoRaWAN," International Conference on Internet-of-Things Design and Implementation, 2018, doi: 10.1109/IoTDI.2018.00022.

[17] S. Danish, M. Lestas, H. Qureshi, K. Zhang, W. Asif, M. Rajarajan, "Securing the LoRaWAN join procedure using blockchains," *Cluster Comput*, vol. 23, no. 3, pp. 2123–2138, 2020, doi: 10.1007/s10586-020-03064-8.

[18] D. Gupta, R. Kumar, "Lightweight cryptography: an IoT perspective," *Trivium*, vol. 80, no. 1, p. 2580, 2019.

[19] M. Capra, R. Peloso, G. Masera, M. Roch, M. Martina, "Edge computing: a survey on the hardware requirements in the internet of things world," *Future Internet*, vol. 11, no. 4, p. 100, 2019, doi: 10.3390/fi11040100.

[20] S. Vadi, "Design and implementation of an off-grid smart street lighting system using LoRaWAN and hybrid renewable energy for energy-efficient urban infrastructure," *Sensors*, vol. 25, no. 17, p. 5579, 2025,doi: 10.3390/s25175579.

[21] V. Sarker, J. Queralta, T. Gia, H. Tenhunen, T. Westerlund, "A survey on LoRa for IoT: integrating edge computing," International Conference on Fog and Mobile Edge Computing, 2019, doi: 10.1109/FMEC.2019.8795313.

[22] M. Khan, K. Salah, "IoT security: review, blockchain solutions, and open challenges," *Future Generation Computer Systems*, vol. 82, pp. 395–411, 2018, doi: 10.1016/j.future.2017.11.022.

[23] P. Basford, F. Bulot, M. Apetroaie-Cristea, S. Cox, S. Ossont, "LoRaWAN for smart city IoT deployments: A long term evaluation," *Sensors*, vol. 20, no. 3, p. 648, 2020,doi: 10.3390/s20030648.

[24] S. Aggarwal, A. Nasipuri, "Survey and performance study of emerging LPWAN technologies for IoT applications," 16th International Conference on Smart Cities: Improving Quality of Life Using ICT & IoT and AI, 2019, doi:10.1109/HONET.2019.8908117.

[25] A. Trivedi, C. Zakaria, R. Balan, A. Becker, G. Corey, P. Shenoy, "Wifitrace: network-based contact tracing for infectious diseases using passive wifi sensing," Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, vol. 5, no. 1, pp. 1–26, 2021, doi: 10.1145/3448084.

[26] M. Ahsan, M. Based, J. Haider, E. Rodrigues, "Smart monitoring and controlling of appliances using LoRa based IoT system," *Designs*, vol. 5, no. 1, p. 17, 2021, doi: 10.3390/designs5010017.

[27] K. Mekki, E. Bajic, F. Chaxel, F. Meyer, "A comparative study of LPWAN technologies for large-scale IoT deployment," *ICT Express*, vol. 5, no. 1, pp. 1–7, 2019, doi: 10.1016/j.icte.2017.12.005.

[28] M. Saelens, J. Hoebeke, A. Shahid, E. Poorter, "Impact of EU duty cycle and transmission power limitations for sub-GHz LPWAN SRDs: An overview and future challenges," *Journal on Wireless Communications and Networking*, vol. 2019, no. 1, pp. 1–32, 2019, doi: 10.1186/s13638-019-1502-5.

[29] G. Margelis, R. Piechocki, D. Kaleshi, P. Thomas, "Low throughput networks for the IoT: lessons learned from industrial implementations," 2nd world forum on internet of things, 2015, doi: 10.1109/WF-IoT.2015.7389049.

[30] M. Centenaro, L. Vangelista, A. Zanella, M. Zorzi, "Long-range communications in unlicensed bands: The rising stars in the IoT and smart city scenarios," *IEEE Wireless Communications*, vol. 23, no. 5, pp. 60–67, 2016, doi: 10.1109/MWC.2016.7721743.

[31] D. Magrin, M. Capuzzo, A. Zanella, L. Vangelista, M. Zorzi, "Performance analysis of LoRaWAN in industrial scenarios," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 9, pp. 6241–6250, 2020,doi: 10.1109/TII.2020.3044942.

[32] O. Charif, N. Aknin, "Enhancing LoRa Network Efficiency: Using Edge Computing for Congestion Mitigation and Latency Reduction," International Conference on Computer Systems and Technologies, 2025, doi: 10.1109/CompSysTech65493.2025.11137349.