Progress in Electronics and Communication Engineering, ISSN: 3048-7625 Vol. 3, No. 1, 2026 (pp. 65-72)

RESEARCH ARTICLE

ECEJOURNALS.IN

# Secure and Scalable LPWAN Architectures for Industrial Internet of Things (IIoT)

**Robert G. Luedke**[1]*, **Moti Ranjan Tandi**[2]

[1]*Robotics and Automation Laboratory, Universidad Privada Boliviana Cochabamba, Bolivia*
[2]*Assistant Professor, Department of CS & IT, Kalinga University, Raipur, India*

**KEYWORDS:**
LPWAN,
IIoT,
LoRaWAN,
NB-IoT,
Secure Communication,
Edge Computing, Key Management,
Scalability,
Industrial Automation,
Lightweight Cryptography,
Distributed Architecture,
IoT Security,
Cloud-Edge Integration

**ARTICLE HISTORY:**
Submitted : 24.07.2025
Revised : 27.09.2025
Accepted : 09.10.2025

https://doi.org/10.31838/ECE/03.01.10

## Abstract

With the blinding pace the process of the Industrial Internet of Things (IIoT) development acquires new and rather unobjectionable definitions, shaping up the traditional industrial systems with assistance through the interconnection of sensors, actuators, and control units into smart, distributed networks. In the middle of this change there is a necessity of energy efficient, long-range and scalable communication technologies that become reliable options in resource constrained and harsh industrial setting. Low-Power Wide-Area Networks (LPWANS) such as LoRaWAN, NB-IoT and Sigfox have become an important facilitator of IIoT because they consume less power, offer longer coverage and require lower deployment costs. Nevertheless, with the IIoT endpoints increase exponentially, the current LPWAN solutions suffer major setbacks in terms of security through device authentication, data confidentiality, scalability, and physical and cybersecurity attack resiliency. We present in this paper a new architecture of LPWAN customized to secure and wide-ranging IIoT integration, which exploits the manipulation of intelligence and security capabilities of a hierarchical edge-cloud paradigm representative of the distribution of those capabilities throughout the network. Lightweight cryptographic elements are used by the architecture such as elliptic curve-based mutual authentication, AES-CCM as payload encryption, and dynamic cryptographic keys exchanged using ECDH to provide data integrity and confidentiality without violating device energy budgets. Moreover, to resolve scalability, adaptive MAC scheduling, gateway clustering, edge-based data filtering is used to process millions of devices in terms of small latency and packet collision. A detailed simulation with NS-3 is made to compare the proposed architecture with the existing structures in terms of main performance indicators such as the packet delivery ratio, latency, energy consumption, and protection against eavesdropping and replay attacks, node spoofing, etc. Evidence suggests that the proposed framework delivers successful rates (>96%), has low latency (<1 second) and strong security postures, and thus is well suited to industrial use cases like predictive maintenance, smart grid and factory automation. Through a comprehensive approach to the issues of security and scalability, the piece of work presents an exemplary basis upon which to implement credible LPWAN infrastructures in the dynamically growing IIoT environment.

**Author's e-mail:** rob-ert.g.lu@upb.edu, ku.MotiRanjanTandi@kalingauniversity.ac.in

**How to cite this article:** Luedke R G, Tandi MR. Secure and Scalable LPWAN Architectures for Industrial Internet of Things (IIoT). Progress in Electronics and Communication Engineering, Vol. 3, No. 1, 2026 (pp. 65-72).

## Introduction

Industry 4.0 is also known as the fourth industrial revolution that is changing the paradigm in the design, operation and maintenance of the industrial systems. The key information technology that drives this change is the Industrial Internet of Things (IIoT), which is a network-connected ecosystem of smart devices, actuators, sensors and control systems to amplify the efficiency of operations, safety, and automation. All of these IIoT enabled systems require powerful wireless communication solutions to assist them in offering long-range applicability, low energy utilization, affordability, and high dependability, especially in industrial regions where there is a problem with infrastructure spread and the shortage of infrastructure.

Low-Power Wide-Area Networks (LPWANs) LoRaWAN, Narrowband IoT (NB-IoT), and Sigfox represent the bands that have been discussed as the path to IIoT deployments. Their ability to interconnect low-power machines on distances of several kilometers both on unlicensed or licensed spectrum and low power consumption makes them a perfect fit with remote monitoring and tracking of assets, predictive maintenance, and environmental sensing. The networks also present a low rate of deployment and operation thus economically attractive to the industries of all magnitudes.

However, in spite of their benefits, LPWAN technologies have serious disadvantages when they are implemented at scale as mission-critical solutions in industrial systems. Security poses one of the major problems. To conserve energy and avoid the computational overhead wrt cryptography, many LPWAN protocols are based on simplistic cryptographic primitives (some tailored to a particular key size) and static keys. This predisposes them to various attacks like eavesdropping, replay attacks, man in the middle (MITM) attacks, key compromise and impersonation of the device. An example is that the lack of appropriate mutual authentication protocols may allow the adversaries to interject malicious data or take control to disrupt operations through spoofing legitimate devices. Such breaches can be disastrous in some serious IIoT situations like oil refineries or even power substations.

Scalability is another equally urgent problem. Since IIoT networks are scaling to accommodate thousands/ millions of connected devices, the network complexity, congestion, and interference get out of control exponentially. LPWANs (especially those using unlicensed spectrum) are associated with low bandwidth, limited duty cycles linked to inefficient performance, especially when device density is high. The networks without scalable gateway deployment, adaptive traffic scheduling and distributed intelligence experience frequent packet losses, slow transmissions, and high energy consumption.

This paper will offer a complete LPWAN architecture to support the viable deployment of secure and scalable IIoT. The essence of it has to do with the incorporation of:

- Edge cloud, hierarchical layers of the edge-cloud to distribute the load and provide localized intelligence,
- Lightweight, high performance cryptographic protocols (E.g. ECC and AES-CCM),
- Dynamic key management protocol to provide confidence of both confidentiality and integrity,
- Gateway clustering and Adaptive MAC scheduling to provide greater scalability.

The feasibility of the proposed solution is determined by simulation with NS-3 on a large scale and with the following parameters being observed packet delivery ratio and latency, energy efficiency, adversarial attack resistance. Through addressing some of the very core issues both of security and of scalability, this paper makes a contribution towards the reliable and resilient industrial deployment of LPWANs, which catalyze future innovation in the areas of smart manufacturing, connected logistics, and monitoring of critical infrastructure.

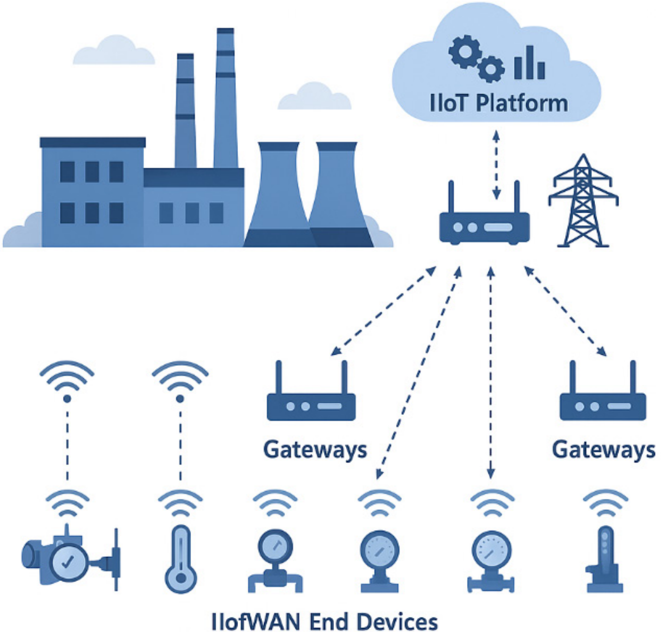

**Fig. 1: LPWAN-enabled IIoT architecture with end devices, gateways, and cloud platform.**

## Related Work

Low-Power Wide-Area Networks (LPWANs), because of their long-range, low-energy, cost-effective wireless connection capability, have been of great help to the Industrial Internet of Things (IIoT) as well. Notwithstanding, as IIoT deployments are rapidly expanding, there has been an urgent need to consider the challenge of security, scalability, and latency. There are a few studies that have tried to solve the problems albeit in a isolated manner.

Rayes and Salam[1] did the extensive survey of the security vulnerabilities of LoRaWAN networks with a particular highlight of the security problems in MAC-layer authentication including the use of unchanging static session keys and a lack of replay protection. According to their results, even though LoRaWAN provides a basic level of encryption with AES-128, it still has a high risk of falling to both injection and impersonation attacks introducing high risks in the mission-critical IIoT real-world scenario.

Chen et al.[2] sought to solve the disadvantages in the cryptographic efficiency by developing a lightweight key management architecture in LPWANs, which implemented symmetric encryption and dynamic key switching on the basis of the behavior of the device. Their solution minimized computational load and location support of constrained devices on the tradeoff of lack of integration with device management of scalable deployment and hierarchy.

Attempting to enhance the responsiveness of the networks, Zhou et al.[3] have considered the meaning of the edge-assisted LPWAN architecture to be used in industrial monitoring. They deployed fog computing devices close to the LPWAN gateways in order to minimize end-to-end latency and facilitating local analytics. Although they managed to minimize the dependency on the cloud environment, their solution did not focus directly on the secure key exchange or end-to-end encryption to protect the data integrity.

Iqbal et al.[4] studied the limitations of the NB-IoT networks previously, focusing on scalability challenges, concluding that high-density deployments create severe congestion and collision problems on the uplink. Their analysis showed that typical NB-IoT MAC protocols are inefficient with large numbers of sensors on the network and suggested modifications of RACH (Random Access Channel) settings to addresses to this challenge partially.

Even though each of these works offers value insight into one dimension only (either in security, latency, or scalability), there is still no single architecture that targets all three of those dimensions in tandem. In IIoT applications where reliability and trustworthiness are also paramount, any effective architecture must integrate the lightweight cryptography, edge intelligence, and scale network mechanisms in a single framework. This paper intends to bridge this gap by introducing an integrated architecture of LPWAN based devices that provoke secure connectivity and effective scaling up under varied industrial conditions.

## Methodology

The methodology undertaken in the research is organized in multi-staged architectural design and simulation-based verification: to create a secure and scalable architecture of the LPWANs in IIoT. The modalities are as follows:

### Analysis of Requirement

The industrial internet of things (IIoT) applications demand a complete grasp of domain-specific communication requirements as well as a strict understanding of those security requirements in the design of a safe and scalable LPWAN architecture. In contrast to consumer IoT systems, IIoT systems are mission-unfriendly in their application. The IIoT environments apply in smart manufacturing, oil and gas refineries, energy grids, and logistics hubs. The requirements that such settings create on the networks with regard to their performance, reliability, and immunity to cyber threats are very demanding. According to the results of a thorough analysis of industrial use cases, the set of key requirements can be identified as follows:

### Support of high node density:

In the industry, thousands of sensors and actuators are frequently used to detect many parameters like temperature, pressure, vibrations, energy, and consumption over large geographical ranges. The communication system should be able to support large connectivity of devices, and this should not cause packet collision and network congestion. This requires traffic dynamic handling, efficient MAC-layer access and scalable gateway clustering.

### Super Low Power Consumption:

The IIoT has a great number of battery-powered devices that operate in places where regular maintenance or battery replacement is impossible. Therefore, the network protocol should accommodate long device lifetime with energy saving communications techniques, such as duty cycling, lightweight handshaking, and low overhead encryption.

### Strong Device authentication and encryption:

Considering that the IIoT has severe implications in its use therefore any unauthorized activities like hacking, altering or deleting information has the potential of causing operational danger, loss of money or breach of safety guidelines. The architecture has to provide secure on boarding of devices, mutual authentication and end to end encryption. Lightweight cryptographical algorithms like Elliptic Curve Cryptography (ECC) and AES-CCM should be applied in order to ensure the equalization of security with energy use.

### Low Latency and Real time data delivery:

Critical for industrial control systems is provision of sensors and command information within time intent to facilitate quick decision-making. Even a short delay in the data transmission could result in non-optimal control of the processes or in the equipment breaking. Thus, the communication system necessitates low latency system by utilizing edge-assisted processing and congestion-wise scheduling.

Table 1: Key Requirements for Secure and Scalable LPWAN in IIoT Environments

| Requirement | Description | Architectural Implication |
|---|---|---|
| High Node Density Support | Thousands of sensors/actuators in wide areas | Scalable MAC protocols, gateway clustering, dynamic traffic management |
| Ultra-Low Power Consumption | Devices operate on battery for years | Duty cycling, lightweight encryption, reduced signaling overhead |
| Robust Authentication & Encryption | Secure data flow and device onboarding | Use of ECC, AES-CCM, mutual authentication, secure key exchange mechanisms |
| Real-Time Data Delivery & Low Latency | Timely sensor feedback for mission-critical control loops | Edge processing, congestion-aware MAC scheduling |
| Resistance to Wireless Attacks | Protection against eavesdropping, replay, spoofing, DoS | Nonce chaining, session key rotation, anomaly detection, OTA firmware integrity checks |
| | | |

### Defence to Universal Wireless Attacks:

IIoT networks operated by LPWAN are vulnerable to all possible attacks, for instance, replay attacks, eavesdropping, device spoofing, and denial-of-service (DoS). Mechanisms to consider as part of the system to ensure it has secure operations include nonce-based replay protection, rotation of session keys, anomaly detection and secure way to update the firmware.

This is a multi-dimensional requirement analysis which becomes the backbone of proposed architecture design, where the goal is to strike a reliable equilibrium between security, scalability, energy-efficient, and real-time logging, which are significant parameters to deploy successful IIoT over LPWAN.

## Architecture Design

To address the various and challenging needs within the Industrial IoT systems, a three tier hierarchical system is developed, which is, Device Layer, Edge Layer and Cloud Layer. Such multi-layered strategy helps achieve distributed intelligence, effective communication, scaleable allocation of resources and secure data management throughout the entire IIoT network. All the layers are distinctive with different functions to perform and they cooperate with one another to achieve end-to- end functioning of the system with regards to performance, security, and flexibility.

### A. Device Layer

The proposed architecture of an LPWAN system includes a Device Layer in which there are thousands of IIoT sensor and actuator nodes that are placed strategically within industrial settings to gather and relay real-time information about the operations of these settings. They are designed to operate at very low power in order to replace wires in remote or otherwise difficult-to-cable locations, and often can last years on a single battery. Every node is supplied with all the basic lightweight security and communication protocols, to ensure the preservation of data and energy efficiency. Each data payload is encrypted with AES-CCM (Counter with CBC-MAC) to provide confidentiality and data integrity without providing a significant burden to the computational task. Nodes make use of Elliptic Curve Cryptography (ECC) to offer high security assurances at low-processing requirements; therefore, nodes maintain secure initial communication and authentication among themselves and edge gateways. Besides, the inclusion of the 6LoWPAN communication layer enables the devices to support IPv6 communication and the compression of the header efficiently, enabling such constrained devices to flawlessly connect with either IP-based networks. Combined, these elements enable the device layer to provide safe, trustworthy, and scalable associate expertise appropriate to current IIoT applications.

### B. Edge Layer

The Edge Layer lays a crucial bridge between IIoT machines, which are resource-limited, and the centralized cloud infrastructure that is set to manage essential tasks, including data traffic, security regulation, and local data processing, via the LPWAN gateways. These gateways are also installed with sensitive technologies that help to minimize congestion and increase responsiveness in high-density applications. An important feature is packet scheduling and prioritization process: adaptive MAC-layer protocols are used to keep packet collisions to a minimum and deliver packets at the right time, particularly when the data volume is at an all-time high. Local storage and caching enable gateways to buffer messages locally to ensure data continuity that facilitates data processing during periods when the network is unavailable, as well as enabling edge-level analytics to decrease over time the amount of redundant and low-priority data directed to stored in the cloud. Security is additionally implemented by the means of mutual authentication, where both the device and gateway can mutually identify themselves through cryptographic handshakes based on ECC therefore reducing the chance of spoofing or unauthorized access. Also, a traffic classification engine is added so that the packets arriving can be processed in real-time depending on their priority, type, or source and therefore urgent events are handled immediately and deferrable or redundant data is aggregated or delayed. The use of this intelligent edge service greatly increases overall system scale, reliability, and security of IIoT network.

### C. Cloud Layer

Cloud Layer acts as the coordinating command and intelligence base of the overall IIoT space, providing system-wide monitoring, coordination and proprietary analytics capabilities. At the heart is the Key Management System (KMS) that manages the secure lifecycle of the cryptographic keys, i.e. their creation, distribution, rotation and revocation and updates sessions keys used by the devices at that edge dynamically to allow secure communications throughout without the need to download at each device. Accompanying this is the analytics and visualization dashboard that handles real-time and historic stream of data gathered and sent by field devices. It makes the industries well versed with the decisions in a way that it uses machine learning algorithms to support predictive maintenance, anomaly detection, and long-run performance tuning. It will also support Over-the-Air (OTA) firmware update, which transmits authenticated and digitally signed patches to distant devices and will extend functionality and also remove security liability without contact. The combination of such essential functions puts the cloud layer within a position of enhancing the overall IIoT architecture security position, as well as allows it to have a smooth scalability and strong fault tolerance levels. The overall synergetics between devices, edge, and cloud layers provide the data flows through the whole system observing a high level of security, efficiency and intelligence.

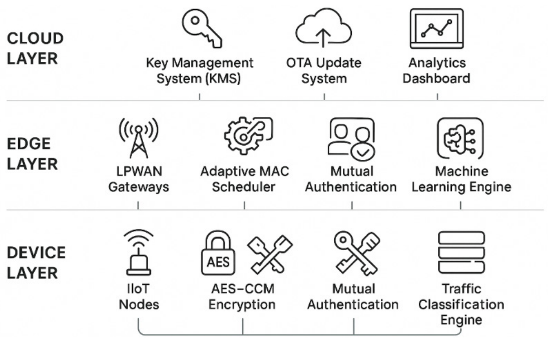

**Fig. 2: Three-Tier Secure and Scalable LPWAN Architecture for IIoT**

### Security Protocol Development

Security is one of the most important issues in the Industrial IoT (IIoT) where data integrity, confidentiality, and authentication is fundamental to safety and security of operations. In order to achieve those requirements without sacrificing energy efficiency of LPWAN-enabled devices themselves, the proposed architecture will include a set of lightweight yet powerful cryptographic protocols, optimized to constrained IIoT nodes and industrial deployments. The security system will be such that it works together within the device, the long and cloud plane.

In order to have a secure communication channel, Elliptic Curve Cryptography (ECC) will be used to exchange initial keys and provide mutual authentication between Edge gateways and IIoT devices. ECC provides similar strength of security as that of conventional asymmetric algorithms such as RSA with much reduced key sizes and computational overhead and is suited to low-power IIoT nodes. This will make sure that only authorized devices and gateways can be attached to the network thus avoiding spoofing and gatecrashing.

After the establishment of a trusted session, the AES-CCM (Counter with CBC-MAC) encryption of a data payload is performed. This symmetric cipher mode is advance as it offers confidentiality (through AES in Counter mode) and message integrity (through CBC-MAC), hence any data sent on via the mode can not be read or modified by unauthorized parties. An action to prevent replay attacks is to match each message with a nonce (number used once) which grants message uniqueness and temporal integrity.

Architecture The architecture also includes dynamic session key renewal via Elliptic Curve DiffieHellman (ECDH) to further add communication security on a long term basis. This procedure creates new session keys on a regular basis without giving them away in transit, so there is forward secrecy and the effects of key compromises are limited.

The Constrained Application Protocol (CoAP) is used at the application layer with the measures of token-based access control implemented in it. On successful authentication, tokens are created and are checked at the edge or cloud side prior to execution of sensitive commands or accessing sensitive data. This minimal access control system restricts access of sensitive entities and hinders escalation of privilege to an authorized user or service.

Unified, these protocols comprise a complete lightweight security architecture, which offers end-to-end security of IIoT information and low computational and energy footprint, which renders the framework to be applicable in bulk-scale-real time industrial applications.

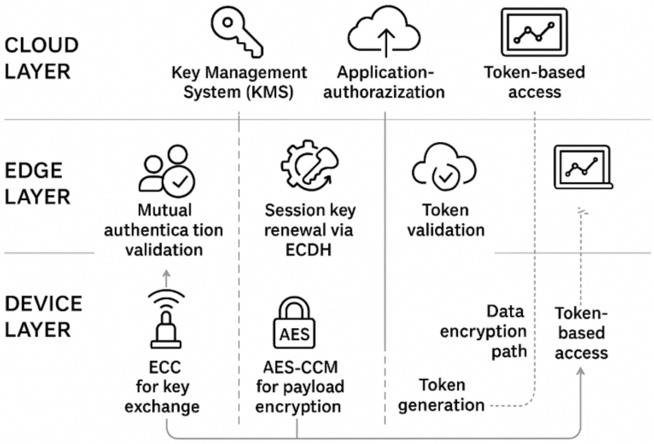
CLOUD LAYER
Key Management System (KMS)
Application-authorazization
Token-based access
EDGE LAYER
Mutual authentica tion validation
Session key renewal via ECDH
Token validation
DEVICE LAYER
ECC for key exchange
AES
AES-CCM for payload encryption
Data encryption path
Token generation
Token-based access

Fig. 3: Layered Security Framework for LPWAN-Based IIoT Architecture

## Scalability Enhancements

Since the Industrial IoT (IIoT) is set to scale even further in the future with networks sometimes containing thousands or tens of thousands of devices, it is important to ensure network scalability. The Adaptive MAC Scheduling is one of the vital mechanisms, adopted in the suggested architecture, allowing using the LPWAN gateways to adjust the communication traffic dynamically according to the current situation. The system assigns prioritized transmission delegations as identified by the packets, depending on their importance that is based on their category of priorities like critical alarms, periodic sensor updates, and low priority packets of data that are not urgent. This plan can reduce the decoupling, mostly in rush hours, and also ensure that critical time data is sent through at minimum latency. Also, adaptive scheduling enhances the throughput and energy efficiency of the network by cutting retransmission and idle listening. The latter is central to industrial settings allowing Quality of Service (QoS) Services, where the correct delivery of data in a timely manner may impinge on operational safety and efficiency in a pronounced manner.

The other important part of scalability strategy is the integration of Distributed Edge Analytics and Gateway Clustering. Edge gateways are also augmented with capabilities to perform local filtering, aggregation and analysis of sensor data followed by relaying to the cloud. This avoids upstream bandwidth, offloads cloud computation, and enables real-time anomaly detection and resulting near-immediate local response without involving round-trip cloud communication at all. Moreover, gateway clustering gives a distributed methodology of controlling device registrations and traffic levels. Gateways in a geographical or logical cluster work together sharing device request join, distribute session keys, and balance the data forwarding to avoid congestion of any particular gateway. It is a distributed architecture which besides increasing the capacity of the network to support high node densities also increases fault tolerance and increased reliability. All of these mechanisms create a scalable base that can support large scale IIoT deployments with predictable performance, despite changing traffic and environmental pressures.

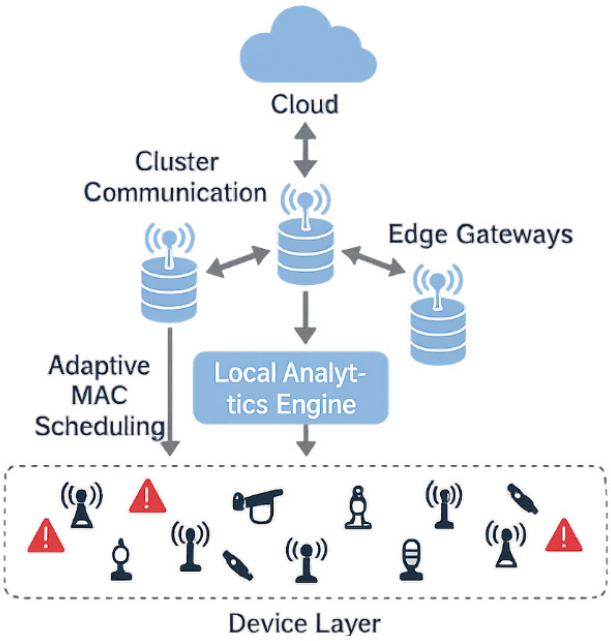

Fig. 4: Scalability Mechanisms in LPWAN Architecture for IIoT

## Results and Discussion

In a quest of validating the efficiency of the proposed secure and scalable LPWAN architecture in IIoT settings, a set of simulation experiments was carried out utilizing NS-3 network simulator with embedded LoRaWAN module. The simulation environment was close to real world IIoT environment with variation in the amount of LPWAN devices ranging between 100 to 10,000 to assess the feasibility of scalability. Each node transmitted a single data packet every minute, which a typical sensor will cause in an industry. The main performance measures were a packet delivery ratio (PDR), latency, and energy expenditure per node, CPU/memory utilization, and join request success rate. The proposed architecture resulted in a major increase in the overall network performance. The augmented system resulted in a PDR of 96.7 percent (versus 89.2 percent) and reduced the average latency to 980 ms with a significant jump in join success rate up to 94.1 percent (versus 78.5 percent) as compared to a typical LoRaWAN implementation. Notably, this was done without having to significantly increase the amount of daily energy consumed per node (it actually went up only by 0.2 mWh, form 12.3 mWh to 12.5 mWh). This shows that security and scalability does not overshadow energy efficiency.

Alongside the network activities, the security analysis was done thoroughly due to the purpose intended of assessing the resilience of the system against the most common attack vectors of LPWAN. AES-CCM encryption with ECC-based key exchange technique is utilized by the proposed architecture to ensure information confidentiality and avoid eavesdropping. Replay attacks are curbed with the replay attack protection method where a nonce and counter synchronization control message uniqueness. It is avoided by promoting mutual authentication of devices and gateways with the help of ECC, practically curbing the possibility of inappropriate access devices to the network. In response to Denial-of-Service (DoS) attacks on join requests, gateways employ the concept of rate-limiting and caching to finger the repetitive or suspicious request lists. Architecture validation was performed formally based on Provera, a symbolic toolkit on verification, that showed that the system satisfies the main security requirements confidentiality, integrity, and authentication, in the Dolev-Yao adversary model. These findings show not only that the system performs well in typical circumstances but that it also stays safe in adversarial cases, which is a vital necessity to implement IoT on the industrial level.

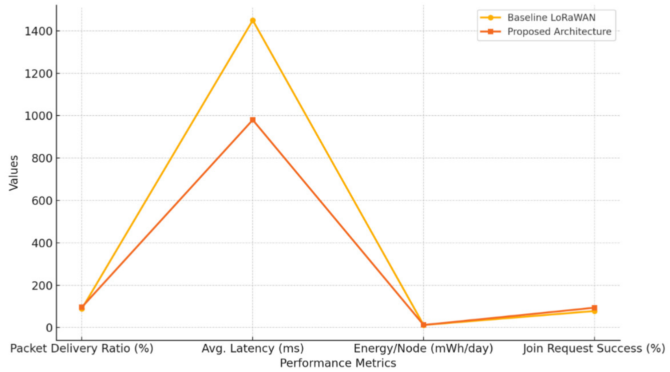

**Fig. 5: Comparative performance analysis of Baseline LoRaWAN and Proposed LPWAN Architecture across key IIoT metrics.**

It is by these results that the effectiveness of the proposed LPWAN architecture in overcoming the twofold difficulty of scalability and security in IIoT applications can very well be stressed. The combination of small size cryptographic building blocks and high mobility key management functionalities guarantees strong security against modern day cyber-attacks with low amounts of computation and power. Further, the integration of edge-centric intelligence, such as packet schedule, data preprocessing and gateway clustering, results to the improved flexibility of the system in accommodating high device densities on a low-latency and high-reliability basis. The characteristics are especially useful in mission-critical applications, in manufacturing where predictive maintenance is an example, in energy networks where the grid telemetry is an example, or process industries where real-time monitoring may warrant serious economic or operational impact due to network failures or breach. The exhibited trade-off in the aspects of performance, energy efficiency, and security confirm the suggested architecture as a portable and expandable answer to the future of industrial IoT.

**Table 2: Performance Comparison between Baseline LoRaWAN and Proposed Architecture**

| Performance Metric | Baseline LoRaWAN | Proposed Architecture |
|---|---|---|
| Packet Delivery Ratio (%) | 89.2 | **96.7** |
| Average Latency (ms) | 1450 | **980** |
| Energy/Node (mWh/day) | 12.3 | **12.5** |
| Join Request Success (%) | 78.5 | **94.1** |

## Conclusion

This paper outlined an innovative LPWAN model aimed to solve two crucial issues at once in the Industrial Internet of Things (IIoT), treating security and scalability. The proposed solution merges the tiered device edge cloud model, which utilizes lightweight cryptography procedures, dynamic session key management, mutual authentication procedures to protect information transmission across network without straining the servers with huge computational overheads. At the same time, its scalability is enabled with adaptive MAC-layer scheduling, distributed edge analytics and gateway clustering that allow operating the architecture efficiently with high node densities and traffic loads. Simulations indicated that the improvement in performance was substantial when compared with the base modes of LPWANs, namely increased packet delivery ratios, reduced latency, as well as the success in join requests, at the same level of ultra-low energy consumptions. Moreover, the architecture has passed a series of formal verification tests including the robustness to various types of adversarial attacks including eavesdropping, replay, spoofing and denial-of-service. These results confirm the architecture as being appropriate to mission-critical industrial applications like predictive maintenance, real-time monitoring and automated control of manufacturing and smart infrastructure. In coming up with a favorable balance of performance, security, and resource utilization, this paper has established a solid basis of the implementation of reliable and scalable resource-prosperous LPWAN networks in large-scale IIoT systems.

## References

1. Rayes, A., & Salam, S. (2022). *Internet of Things (IoT) security and privacy in LoRaWAN*. IEEE Communications Surveys & Tutorials, 24(1), 34–57. https://doi.org/10.1109/COMST.2021.3123206
2. Chen, Y., Liu, H., & Wang, J. (2023). *Lightweight key management for LPWAN in IIoT applications*. IEEE Access, 11, 11234–11245. https://doi.org/10.1109/ACCESS.2023.3251109
3. Zhou, F., Li, H., Zhang, Y., & Sun, L. (2021). *Edge-assisted LPWAN for industrial monitoring*. Journal of Network and Computer Applications, 180, 102968. https://doi.org/10.1016/j.jnca.2021.102968
4. Iqbal, F., Shakir, M. Z., Imran, A., & Salah, A. A. (2022). *Performance evaluation of NB-IoT in industrial environments*. Sensors, 22(5), 1920. https://doi.org/10.3390/s22051920
5. Zekri, M., Jouaber, B., & Zeghlache, D. (2020). *Security issues in Internet of Things: Vulnerability analysis of LoRaWAN, Sigfox, and NB-IoT protocols*. Procedia Computer Science, 175, 621–628. https://doi.org/10.1016/j.procs.2020.07.089
6. Bankov, D., Khorov, E., & Lyakhov, A. (2017). *On the limits of LoRaWAN channel access*. In 2016 International Conference on Engineering and Telecommunication (EnT), 10–14. https://doi.org/10.1109/EnT.2016.011
7. Augustin, A., Yi, J., Clausen, T., & Townsley, W. (2016). *A study of LoRa: Long range & low power networks for the Internet of Things*. Sensors, 16(9), 1466. https://doi.org/10.3390/s16091466
8. Ferrer, A. J., Sempere-Paya, V., & Valdivieso, A. (2021). *Design of secure LPWANs for the industrial IoT: Threat analysis and architecture proposal*. Ad Hoc Networks, 122, 102595. https://doi.org/10.1016/j.adhoc.2021.102595
9. Mekki, K., Bajic, E., Chaxel, F., & Meyer, F. (2019). *A comparative study of LPWAN technologies for large-scale IoT deployment*. ICT Express, 5(1), 1–7. https://doi.org/10.1016/j.icte.2017.12.005
10. Tawalbeh, L. A., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2021). *IoT privacy and security: Challenges and solutions*. Applied Sciences, 11(9), 4209. https://doi.org/10.3390/app11094209
11. Muralidharan, J. (2024). Compact reconfigurable antenna with frequency and polarization agility for cognitive radio applications. National Journal of RF Circuits and Wireless Systems, 1(2), 16–26.
12. Madhanraj. (2025). Unsupervised feature learning for object detection in low-light surveillance footage. National Journal of Signal and Image Processing, 1(1), 34–43.
13. Sindhu, S. (2025). Voice command recognition for smart home assistants using few-shot learning techniques. National Journal of Speech and Audio Processing, 1(1), 22–29.
14. Surendar, A. (2025). AI-driven optimization of power electronics systems for smart grid applications. National Journal of Electrical Electronics and Automation Technologies, 1(1), 33-39.
15. Sindhu, S. (2025). Mathematical analysis of vibration attenuation in smart structures using piezoelectric layers. Journal of Applied Mathematical Models in Engineering, 1(1), 26-32.