Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

Hybrid LoRaWAN-MQTT Security for Industry 4.0/5.0: Zone-Conduit Hardening for Hybrid Process Infrastructures

Mohammed Shoukatuddin
Senior Specialist - OT Network & Cybersecurity, Ma'aden Aluminum Company, Saudi Arabia

Mohammed Aqheel
Senior IT Specialist, Ma'aden Aluminum Company, Saudi Arabia

Mohammed Afzal
Specialist I - Systems Administration, Saudi Arabian Mining Company (Ma'aden), Saudi Arabia

Abstract - LoRaWAN enables long-range, low-power industrial sensing and is widely used for condition monitoring and environment tracking. In Industrial IoT (IIoT) deployments, LoRaWAN telemetry is commonly forwarded into IP networks where MQTT brokers distribute data to historians, analytics platforms, and operator dashboards. This layered integration introduces security challenges at multiple trust boundaries (device provisioning, join server, gateways, network server, edge broker, and upstream brokers). The challenges become more pronounced in Industry 4.0/5.0 environments where hybrid process infrastructures combine deterministic OT control networks with wireless sensing overlays and edge-to-cloud analytics. This paper provides a LoRaWAN-centric threat model and proposes a practical hardening architecture that combines LoRaWAN key discipline, secure MQTT brokering at the edge, and zone–conduit segmentation patterns aligned with ISA-95/IEC 62264 and IEC 62443 concepts. The approach strengthens confidentiality, integrity, availability, and resilience while maintaining LPWAN operational constraints.

***Keywords - LoRaWAN security, MQTT, Industry 4.0, Industry 5.0, hybrid process infrastructure, zone and conduit, IIoT hardening*.**

I. INTRODUCTION

Industry 4.0 introduced cyber-physical systems, automation, and real-time data exchange across production assets. These initiatives rely on broad sensing coverage to enable predictive maintenance, quality improvements, and energy optimization. Industry 5.0 complements this direction by adding explicit goals for human-centric operations, sustainability, and resilience. In practice, this means plants must maintain safe and reliable telemetry pipelines even when facing disruptions such as network outages, cyber incidents, or supply chain constraints.

LoRaWAN is well suited for industrial sensing overlays because it provides long-range coverage for battery-powered devices and supports large device populations with minimal infrastructure. Typical deployments include vibration and temperature monitoring for rotating equipment, corrosion monitoring, tank level sensing, environmental compliance sensors, and remote utility metering. However, LoRaWAN data rarely remains within the radio network domain. It is usually consumed by enterprise applications, where MQTT is frequently selected as the messaging backbone due to its lightweight publish–subscribe model and compatibility with cloud and on-premises platforms.

The integration of MQTT over LoRaWAN creates an end-to-end trust chain in which security is only as strong as the weakest boundary. LoRaWAN provides AES-based confidentiality and integrity for frames, but telemetry is typically decrypted for application processing and may traverse gateways, network servers, integration middleware, and brokers. This paper focuses on LoRaWAN-first security: it treats MQTT as an extension layer that must be governed through identity mapping, topic control, and segmentation patterns that prevent lateral movement into OT zones.

II. INDUSTRY 4.0/5.0 CONTEXT AND HYBRID PROCESS INFRASTRUCTURE

A hybrid process infrastructure is a realistic architecture for modern plants and remote industrial sites. It combines deterministic OT control networks (PLC/RTU to SCADA/DCS) with non-invasive sensing overlays (LoRaWAN) and higher-level analytics (edge computing and cloud services). In this model, LoRaWAN sensors provide supplementary measurements without altering safety-critical control loops. This supports Industry 4.0 optimization and Industry 5.0 resilience by enabling better asset health insight, reduced unplanned downtime, and improved sustainability reporting.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

Hybrid infrastructures also reflect the reality of mixed connectivity: Ethernet for control, Wi-Fi/5G for mobility, and LPWAN for low-power sensing. The architectural requirement is not to connect everything to everything, but to connect the right data flows through controlled boundaries. For security, wireless overlays must not become unmanaged bridges into OT zones. Instead, telemetry should be normalized at the edge, passed through a controlled OT DMZ conduit, and then distributed via MQTT using explicit topic namespaces and least-privilege access controls.

Industry 5.0 demands additional properties from the same architecture: graceful degradation when connectivity is disrupted, clear accountability for decisions derived from analytics, and transparency for compliance and sustainability reporting. Practically, this means that LoRaWAN sensing should continue locally even if upstream services fail, operators should have access to last-known-good values and alarms, and the infrastructure should provide audit-ready logging. These requirements motivate placing governance close to the edge and formalizing conduits between OT and IT domains.

III. LORAWAN ARCHITECTURE AND SECURITY MODEL (LORAWAN-FIRST)

LoRaWAN uses a star-of-stars topology: end devices transmit uplinks that can be received by multiple gateways. Gateways forward frames to a network server where deduplication, frame counter validation, and MIC checks are performed. Join procedures (typically OTAA) establish session keys via a join server using root credentials such as JoinEUI and AppKey. Session keys are then used for application payload confidentiality and frame integrity.

From a security engineering viewpoint, LoRaWAN security has three pillars: cryptography, replay resistance, and governance. Replay resistance depends on correct handling of DevNonce/JoinNonce and frame counters, including persistence across device resets. Governance includes secure provisioning (unique identifiers, controlled onboarding), key custody (protecting root keys), and operational monitoring (join anomalies, uplink floods).

LoRaWAN operational features can also be abused. Adaptive Data Rate (ADR) improves efficiency but can be manipulated if adversaries can influence link-quality assumptions, potentially degrading reliability. Class B/C downlink behavior affects how quickly devices can receive configuration or commands, which matters for recovery and incident response. Roaming and multi-tenant deployments can introduce additional trust relationships. For industrial systems, it is safer to constrain optional features to the minimum needed and document the trust assumptions explicitly.

LoRaWAN version selection matters. LoRaWAN 1.1 adds security enhancements and clearer join-server responsibilities. LoRaWAN 1.0.4 introduces additional requirements around counters and nonce handling to reduce replay risk in practice. A practical deployment should align device behavior and server configuration to the selected LoRaWAN version and regional parameters, with explicit policies for counter persistence, join attempts, and device reset behavior.

IV. MQTT OVER LORAWAN: THREATS AND SECURITY GAPS

MQTT provides publish–subscribe messaging where clients publish to topics and brokers route messages to subscribers. MQTT includes QoS levels, retained messages, and persistent sessions. These features are valuable for telemetry distribution but can be abused if governance is weak. When MQTT is used for LoRaWAN telemetry, common gaps include identity fragmentation, weak broker authorization, and plaintext exposure at processing points where LoRaWAN payloads are decrypted.

Availability threats are prominent. Attackers can stress gateways, join services, or brokers with excessive traffic, causing delays and data loss without breaking LoRaWAN cryptography. MQTT brokers can also be affected by message storms if clients publish rapidly or if retained messages and session queues are mismanaged. Integrity threats also matter: false telemetry can mislead maintenance decisions or trigger unnecessary work orders.

MQTT security controls should be treated as mandatory in IIoT. Transport encryption (TLS), mutual authentication where feasible, and strong credential hygiene reduce interception and impersonation. Topic-level authorization must prevent cross-tenant leakage and separate telemetry topics from control topics. Broker hardening should include rate limits, payload validation, and logging. When combined with LoRaWAN, these controls should be enforced at the first IP boundary (edge broker) rather than relying solely on a centralized cloud broker.

V. STANDARD VS PROPOSED ARCHITECTURE

The baseline architecture forwards LoRaWAN telemetry from network services directly to an MQTT broker and cloud applications. The proposed architecture introduces a hybrid edge zone with an MQTT edge broker and a controlled OT DMZ conduit, which enables policy enforcement close to where LoRaWAN data first enters IP systems. Fig. 1 and Fig. 2 summarize these patterns.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

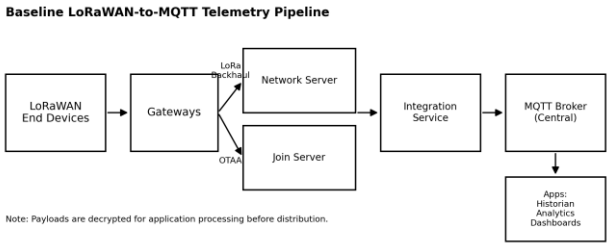

Fig. 1. Standard LoRaWAN-to-MQTT data path (baseline Industry 4.0 telemetry pipeline).

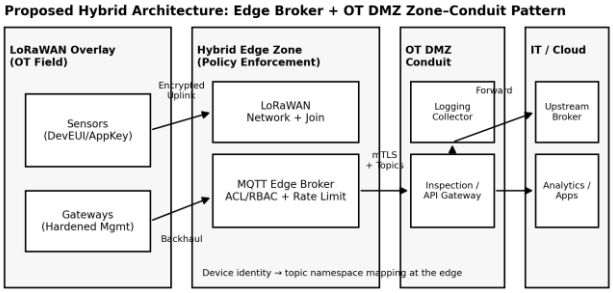

Fig. 2. Proposed hybrid process infrastructure integrating LoRaWAN overlay, edge brokering, and OT DMZ zoning (Industry 5.0-ready).

VI. PROPOSED HARDENING CONTROLS (IMPLEMENTABLE)

A LoRaWAN-first hardening program starts with onboarding and join governance: protect root keys, control provisioning, and monitor joins for anomalies. Enforce counter persistence and nonce discipline to reduce replay risk. Harden gateways by restricting management plane exposure, applying secure configurations, and monitoring uplink rates and backhaul behavior. Secure network and join server interfaces with strong authentication between components and audit logging for correlation.

At the integration boundary, edge brokering is central. An MQTT edge broker inside a hybrid edge zone can normalize payloads, enforce topic namespaces, and apply RBAC/ACL policies before forwarding data upstream. Mapping LoRaWAN identities to topic-level authorization provides a practical binding between the radio identity domain and the messaging domain. Broker-to-broker communication should use mutual TLS where feasible, and upstream brokers should enforce quotas and rate limits to prevent message storms.

A dedicated OT DMZ should be treated as a conduit boundary that controls egress to IT/cloud services and prevents inbound lateral movement. The DMZ can host inspection services, logging collectors, and controlled API gateways for analytics. Finally, lightweight anomaly detection can be deployed to identify unusual publish rates, topic deviations, repeated authentication failures, and join anomalies. Integrating these signals into SIEM supports Industry 5.0 objectives by improving resilience and enabling auditable response.

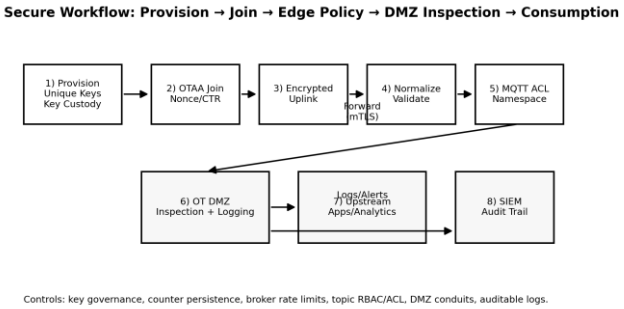

Fig. 3. Secure workflow for provisioning, joining, encrypted uplink, edge policy enforcement, DMZ inspection, and analytics consumption.

VII. PURDUE VS HYBRID: COMPARISON AND BENEFITS

Purdue-style architectures provide a useful mental model for segmentation and operational stability, but they were not designed for large-scale wireless overlays and edge-to-cloud analytics. The proposed hybrid process infrastructure adapts segmentation principles to modern IIoT by integrating LoRaWAN sensing overlays through a governed edge zone and a controlled conduit (OT DMZ). Table I summarizes architectural differences, and Table II provides a threat-to-control mapping.

Table I. Purdue-Style Segmentation vs Hybrid Process Infrastructure

Criterion	Purdue-Style (Classic)	Hybrid LoRaWAN Overlay (Proposed)
Objective	Hierarchical OT segmentation	OT segmentation + scalable sensing + resilience
Wireless integration	Often separate from OT model	Explicit LoRaWAN overlay integrated via edge broker
Cloud/analytics path	Limited or ad-hoc	Controlled via OT DMZ conduit
Identity governance	OT identity separate from IT	Unified mapping at edge (DevEUI→topic/RBAC)
Industry 5.0 readiness	Partial	Strong (resilience, sustainability data, operator support)
Operational benefit	Clear layering, stable operations	Faster deployment, reduced cabling, better asset visibility

Table II. Threat-to-Control Mapping for LoRaWAN-to-MQTT Hybrid Infrastructure

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

Threat	Where it occurs	Recommended control(s)
Key compromise / weak onboarding	Device provisioning / join	Root key custody, controlled onboarding, join monitoring
Replay / counter misuse	LoRaWAN session handling	Strict counter policy, server validation, device NVM counters
Gateway flooding / DoS	Gateway/backhaul	Rate limiting, segmentation, hardened mgmt plane
Unauthorized topic access	MQTT edge/upstream broker	RBAC/ACL, namespace governance, mutual TLS
False telemetry / data tampering	Edge/broker/application	Payload validation, anomaly detection, audit logging

VIII. BENEFITS FOR INDUSTRY 4.0 AND 5.0

For Industry 4.0 programs, the main benefit is scalable sensing without extensive cabling. LoRaWAN overlays provide coverage across wide areas and enable faster deployment of condition monitoring. When combined with MQTT, telemetry can be integrated with historians and analytics tools to improve maintenance planning and reduce unplanned downtime. The proposed architecture improves data quality by normalizing payloads and enforcing topic governance at the edge, reducing integration errors and misrouting.

For Industry 5.0 programs, resilience and accountability are primary. The hybrid design introduces clear conduits and a DMZ boundary, reducing blast radius and supporting containment during incidents. Human-centric operations benefit from more reliable telemetry and clearer operator dashboards, while sustainability goals benefit from consistent environmental and energy monitoring. Audit-ready logs and controlled data flows support compliance and post-incident learning, aligning operational priorities with resilience and worker-centered decision-making.

IX. CONCLUSION

LoRaWAN sensing overlays are a practical foundation for IIoT in Industry 4.0 programs and become even more important in Industry 5.0 where resilience and sustainability reporting require reliable, secure telemetry. Securing MQTT-over-LoRaWAN requires more than AES at the radio layer; it requires disciplined identity governance, protected gateways and servers, controlled edge brokering, and an OT DMZ conduit boundary to contain risk. The proposed hybrid process infrastructure strengthens confidentiality, integrity, availability, and operational resilience while respecting LPWAN constraints and OT safety requirements.

REFERENCES

[1] LoRa Alliance, 'LoRaWAN® Specification v1.1', 2017.
[2] LoRa Alliance, 'TS001-1.0.4 LoRaWAN® L2 Specification', 2020.
[3] OASIS, 'MQTT Version 3.1.1', 2014.
[4] OASIS, 'MQTT Version 5.0', 2019.
[5] European Commission (DG RTD), Breque, De Nul, Petridis, 'Industry 5.0: Towards a sustainable, human-centric and resilient European industry', 2021.
[6] H. Kagermann, J. Helbig, W. Wahlster, 'Recommendations for implementing the strategic initiative INDUSTRIE 4.0', acatech, 2013.
[7] ISA, 'ISA-95 Standard: Enterprise-Control System Integration (IEC 62264)', ISA.org.
[8] M. G. Jaatun et al., 'Security Aspects of Zones and Conduits in IEC 62443', J. Cybersecur. Priv., 2026.
[9] F. Hessel et al., 'ChirpOTLE: a framework for practical LoRaWAN security evaluation', ACM WiSec, 2020.
[10] C. Segarra et al., 'MQT-TZ: Secure MQTT Broker for Biomedical Signal Processing on the Edge', SHTI, 2020.
[11] A. Rizzardi et al., 'Analysis on functionalities and security features of IoT-related protocols', Wireless Networks, 2022.