IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 15 January 2026, accepted 30 January 2026, date of publication 3 February 2026, date of current version 6 February 2026.

Digital Object Identifier 10.1109/ACCESS.2026.3660731

RESEARCH ARTICLE

Hybrid Machine Learning Anomaly Detection and Lightweight Zero Trust Authentication for LoRaWAN Networks

GHADA ABDELHADY[1], ABDULRAHMAN GHANDOURA[2], (Member, IEEE), ABDELWAHED MOTWAKEL[3], AND ABDULLAH ALAJMI[3], (Member, IEEE)

[1]Computer Systems Engineering Department, October University for Modern Sciences and Arts, Giza 12572, Egypt
[2]Department of Engineering and Applied Sciences, Applied College, Umm Al-Qura University, Makkah 24382, Saudi Arabia
[3]Department of Management Information Systems, College of Business Administration in Hawtat Bani Tamim, Prince Sattam bin Abdulaziz University, Al-Kharj 11942, Saudi Arabia

Corresponding author: Abdullah Alajmi (a.alajmi@psau.edu.sa)

This work was supported by Prince Sattam bin Abdulaziz University under Grant PSAU/2025/01/36604.

ABSTRACT LoRaWAN has become one of the most widely adopted LPWAN technologies, but its large-scale use has also exposed several persistent security weaknesses. Recent studies show that unprotected LoRaWAN links are still vulnerable to basic attacks such as eavesdropping (67% success rate) and replay attempts (about 43%), which highlights the need for more practical and adaptive security solutions suitable for low-power devices. In this work, we develop a security framework that combines a hybrid machine-learning model for anomaly detection with a lightweight Zero Trust authentication mechanism. The anomaly detection module merges a tuned LightGBM classifier with an autoencoder-based unsupervised detector. Across multiple attack categories, the combined model achieved an average detection accuracy of 95% and an AUC-ROC of 0.973 while keeping the memory footprint small enough for LoRa-class devices. We also design a Zero Trust authentication scheme based on an optimized Proof-of-Authority blockchain model and a low-cost mutual authentication protocol. The evaluation shows an average authentication delay of about 187 ms and system availability above 99.9%. Although the full framework introduces an energy overhead of approximately 18%, the projected device lifetime remains more than seven years, which is significantly longer than what existing blockchain-based IoT authentication systems provide.

INDEX TERMS LoRaWAN security, machine learning anomaly detection, zero trust architecture, blockchain authentication, IoT security, LPWAN networks.

I. INTRODUCTION

A. THE LoRaWAN SECURITY LANDSCAPE

The Internet of Things has transformed how organizations monitor and manage assets. Projections suggest over 75 billion connected devices by 2025 [1], fundamentally reshaping domains from precision agriculture to urban infrastructure management [2]. LoRaWAN has emerged as the leading LPWAN solution within this ecosystem. Its appeal stems from an optimal balance: extended range reaching 15 km in rural settings, exceptional energy efficiency enabling device lifespans beyond 10 years, and cost-effectiveness that makes large-scale deployments economically viable [3], [4].

Yet widespread LoRaWAN adoption in mission-critical applications faces significant barriers. Security vulnerabilities inherent to its design create substantial risks. Operating in unlicensed ISM spectrum bands while employing lightweight cryptographic mechanisms to preserve energy efficiency, LoRaWAN networks offer an attractive attack surface [5]. Recent comprehensive audits identified over 15 distinct attack vectors targeting LoRaWAN infrastructure. Empirical studies reveal troubling success rates: 67% for eavesdropping attacks in controlled environments [6], 43% for replay attacks against standard implementations [7], and over 38% for MAC layer frame injection by sophisticated attackers [8].

The associate editor coordinating the review of this manuscript and approving it for publication was Jiawei Yang.

Resource constraints further complicate security implementation. IoT devices typically operate with severe limitations: 8-32 bit microcontrollers, memory capacity between 2-512 KB RAM, and battery power requiring multi-year replacement cycles [9]. Traditional network security solutions prove impractical due to substantial computational overhead and frequent key exchanges that would rapidly deplete device batteries [10].

B. RESEARCH GAP AND POSITIONING

While prior research has made notable progress in enhancing LoRaWAN security, existing approaches continue to face limitations when deployed in resource-constrained environments that require both effective anomaly detection and long-term operational sustainability.

1) LIMITATIONS OF EXISTING APPROACHES

a: MACHINE LEARNING-BASED DETECTION APPROACHES

Recent ML-based anomaly detection techniques for LoRaWAN [17] have demonstrated promising detection performance. However, many of these approaches rely on models with relatively high computational, memory, or energy requirements, which limits their applicability to constrained end devices. As a result, detection accuracy is often prioritized without explicit consideration of device lifetime and resource constraints.

b: BLOCKCHAIN-BASED AUTHENTICATION

Blockchain-enabled authentication mechanisms [29] provide strong security and trust guarantees. Nevertheless, prior studies report additional communication and cryptographic overhead, which can adversely affect energy consumption and reduce device operational lifetime. Such overhead poses a significant challenge for long-lived LoRaWAN deployments.

c: INTEGRATED SECURITY FRAMEWORKS

Recent integrated or multi-layer security solutions [28], [33], [34] represent an important step toward holistic protection. However, these approaches typically address detection effectiveness and authentication mechanisms in isolation, without jointly optimizing detection accuracy, resource overhead, and long-term operational sustainability within a single adaptive framework.

It is important to clarify that the individual machine learning techniques employed in this work, namely LightGBM-based supervised detection and autoencoder-based unsupervised anomaly detection, are not novel by themselves. Both approaches have been previously explored in IoT and LoRaWAN security contexts. The research gap addressed in this work does not lie in proposing new learning algorithms, but rather in how these techniques are jointly operationalized, constrained, and coordinated within a single resource-aware security framework tailored to long-lived LoRaWAN deployments.

2) SPECIFIC RESEARCH GAP ADDRESSED

a: RESEARCH GAP

To the best of our knowledge, existing LoRaWAN security solutions do not simultaneously provide high anomaly detection effectiveness, lightweight Zero Trust–based authentication, and explicit consideration of resource constraints required for large-scale and long-lived LoRaWAN deployments.

Our work addresses this gap by proposing an integrated framework that:

1) combines supervised and unsupervised anomaly detection to enhance detection robustness while remaining suitable for resource-constrained devices;
2) incorporates a lightweight Zero Trust authentication mechanism designed to limit additional communication and cryptographic overhead; and
3) dynamically balances security performance and resource consumption based on observed network behavior.

This positioning clearly differentiates the proposed approach from prior integrated solutions [28], [33], [34], which typically address subsets of these challenges independently, and establishes a unified framework aimed at practical and sustainable LoRaWAN security.

C. RESEARCH MOTIVATION AND APPROACH

Building on the identified research gap, our approach is guided by three design principles derived from practical observations of real-world LoRaWAN deployments.

First, **multi-layer protection** is required to address the heterogeneous attack surface of LoRaWAN networks. Relying on a single security mechanism is insufficient in practice; instead, coordinated protection across multiple layers is necessary to mitigate diverse threat vectors.

Second, **adaptive intelligence** is essential in dynamic IoT environments. Static security configurations are unable to cope with evolving attack behaviors, motivating the integration of learning-based mechanisms capable of adapting to previously unseen threats.

Third, **resource-aware design** must be treated as a fundamental constraint. Security mechanisms should be explicitly designed to operate within the energy, memory, and computational limits of IoT devices, ensuring that enhanced security does not compromise long-term network operation.

These principles collectively inform the design of the proposed framework and bridge the gap between the identified limitations of existing solutions and the technical approach presented in this work.

D. CONTRIBUTIONS

This paper makes the following contributions to LoRaWAN security and IoT network protection:

1) HYBRID MACHINE LEARNING–BASED ANOMALY DETECTION

We propose a dual-mode anomaly detection framework that combines supervised LightGBM models for identifying known attack patterns with unsupervised autoencoder-based detection for previously unseen threats. The approach leverages multi-dimensional features derived from signal characteristics and device behavior, while remaining suitable for deployment in resource-constrained environments.

2) LIGHTWEIGHT ZERO TRUST AUTHENTICATION MECHANISM

We design a Zero Trust authentication mechanism tailored to LoRaWAN constraints. The proposed design integrates lightweight trust evaluation with efficient authentication procedures, aiming to limit additional communication and computational overhead while maintaining robust access control.

3) ADAPTIVE SECURITY COORDINATION

We introduce a coordination mechanism that enables interaction between anomaly detection and authentication components. This mechanism supports adaptive security responses by adjusting security parameters based on observed network behavior and detected threat levels.

4) COMPREHENSIVE EXPERIMENTAL EVALUATION

We evaluate the proposed framework through extensive experimental analysis under multiple attack scenarios. The results demonstrate the effectiveness of the integrated approach in improving anomaly detection performance while preserving energy efficiency and scalability in LoRaWAN deployments.

II. RELATED WORK

A. LoRaWAN SECURITY VULNERABILITIES AND ATTACK LANDSCAPE

Security challenges in LoRaWAN networks have attracted extensive research attention. The resulting body of work reveals a complex threat landscape spanning multiple protocol layers and attack vectors.

Early security assessments by Butun et al. [11] identified fundamental physical layer vulnerabilities, particularly susceptibility to jamming attacks due to operation in unlicensed spectrum bands. More recent work by Sanchez-Iborra et al. [16] demonstrated sophisticated signal-based attacks achieving 78% success rate in disrupting LoRaWAN communications through intelligent jamming strategies. Yang et al. [17] extended this analysis, showing that coordinated jamming attacks can effectively partition LoRaWAN networks using as few as three strategically positioned jammers in urban environments.

Comprehensive analysis by Kim et al. [18] revealed critical vulnerabilities in LoRaWAN's network layer, particularly around key management and device authentication mechanisms. Their empirical study of 150 real-world LoRaWAN deployments identified that 67% employed default or weak authentication configurations, making them vulnerable to device impersonation attacks. Subsequent work by Rodriguez-Martinez et al. [19] demonstrated practical replay attacks achieving 43% success rate against standard LoRaWAN 1.0.3 implementations, highlighting inadequacies in current counter-based replay protection mechanisms.

Recent research has focused on application-layer vulnerabilities and end-to-end security mechanisms. Chen et al. [20] presented a comprehensive taxonomy identifying 12 distinct application-layer attack categories ranging from data manipulation to service disruption. Their analysis revealed that current end-to-end encryption mechanisms provide insufficient protection against sophisticated attackers with partial network access. Advanced persistent threats targeting LoRaWAN infrastructure have been analyzed by Thompson et al. [25], demonstrating how attackers can establish long-term presence in networks through coordinated multi-layer attack strategies.

B. MACHINE LEARNING FOR IoT SECURITY AND ANOMALY DETECTION

Machine learning techniques for IoT security have emerged as a promising research direction, with particular emphasis on anomaly detection and intrusion prevention.

Traditional supervised learning methods have shown significant promise. Liu et al. [21] pioneered LightGBM usage for RSSI-based anomaly detection in LoRaWAN networks, achieving 91.2% accuracy in detecting signal-based attacks. However, their approach was limited to single-feature analysis and required extensive labeled datasets. Patel et al. [22] extended this work by incorporating ensemble methods, achieving 93.4% accuracy but with 340% increase in computational overhead—making deployment on resource-constrained devices impractical.

Recent advances by Zhang et al. [23] introduced multi-dimensional feature analysis for LoRaWAN anomaly detection, combining RSSI, SNR, and temporal features. While achieving 94.7% accuracy, their approach required 156 KB memory footprint per device, exceeding capabilities of many IoT devices.

Unsupervised learning methods offer the advantage of detecting unknown attack patterns without requiring labeled training data. Kumar et al. [24] demonstrated autoencoder-based anomaly detection effectiveness for IoT networks, achieving 87.3% recall for unknown attack detection. However, their approach suffered from high false positive rates (23.4%) in dynamic network conditions.

More recent work by Thompson et al. [25] proposed variational autoencoders for LoRaWAN anomaly detection, reducing false positive rates to 8.7% while maintaining 89.1% recall. Yet their approach required significant computational resources for training and inference, limiting practical deployment.

Privacy-preserving aspects of federated learning have attracted attention for IoT security applications. Wang et al. [26] presented a federated learning framework for collaborative anomaly detection across LoRaWAN networks, achieving 92.8% detection accuracy while preserving data privacy. However, their approach required substantial communication overhead (45% increase in network traffic) and complex coordination mechanisms.

C. ZERO TRUST ARCHITECTURE AND BLOCKCHAIN AUTHENTICATION FOR IoT

Zero Trust security models have gained prominence as a comprehensive network security approach, though their application to resource-constrained IoT environments remains challenging.

Classical Zero Trust architectures, as defined by Rose et al. [27], emphasize continuous verification and least-privilege access. Direct application to IoT networks faces significant challenges due to computational and energy constraints. Martinez et al. [28] attempted to adapt Zero Trust principles for IoT environments but encountered 67% increase in energy consumption and 45% increase in authentication latency.

Blockchain technology integration with Zero Trust principles has been explored as a means of achieving decentralized, tamper-resistant authentication. Naik et al. [29] demonstrated blockchain-based authentication feasibility for LoRaWAN networks, though their Proof-of-Work consensus mechanism required excessive energy consumption (reducing device lifetime by 58%). Recent work by Singh et al. [30] introduced Proof-of-Authority consensus for IoT authentication, achieving 73% reduction in energy consumption compared to Proof-of-Work while maintaining security guarantees. However, their approach required pre-established trust relationships between network participants, limiting scalability in dynamic environments.

Research into lightweight authentication protocols specifically designed for IoT constraints has produced several promising approaches. Lee et al. [31] proposed an ECC-based mutual authentication protocol achieving sub-100ms authentication latency while maintaining strong security guarantees. However, their approach lacked integration with broader security frameworks and provided no protection against network-layer attacks.

Advanced cryptographic techniques including post-quantum cryptography have been investigated for future-proofing IoT authentication systems. Rodriguez et al. [32] analyzed lattice-based cryptography feasibility for LoRaWAN authentication, demonstrating quantum resistance with manageable computational overhead.

D. INTEGRATED SECURITY FRAMEWORKS AND GAP ANALYSIS

Limited research has addressed comprehensive, integrated security solutions for LoRaWAN networks.

Preliminary work by Kumar et al. [33] introduced a two-layer security framework combining network-level encryption with application-level anomaly detection. While demonstrating improved security coverage, their approach lacked intelligent coordination between security layers and provided limited adaptability to evolving threats.

Recent work by Anderson et al. [34] presented a three-layer integrated security architecture for IoT networks, incorporating physical-layer security, network-layer authentication, and application-layer access control. However, their approach required significant computational overhead (average 45% increase in device energy consumption) and lacked machine learning-based threat adaptation.

Our comprehensive literature review reveals several critical gaps:

1) **Lack of intelligent integration:** Existing security solutions typically address individual threat vectors in isolation, failing to leverage synergistic benefits of integrated, coordinated defense mechanisms.
2) **Limited adaptability:** Current security frameworks employ static configurations that cannot adapt to evolving threat landscapes or dynamic network conditions.
3) **Resource-constraint mismatch:** Many proposed security enhancements introduce computational and energy overhead incompatible with IoT device constraints.
4) **Insufficient real-world validation:** Limited experimental validation of integrated security approaches under realistic deployment conditions constrains practical applicability.

III. PROPOSED SECURITY FRAMEWORK

A. FRAMEWORK ARCHITECTURE AND DESIGN PRINCIPLES

Our security framework follows a modular architecture enabling seamless integration between anomaly detection and authentication components while ensuring resource-aware operation. The system operates on four fundamental design principles:

1) **Resource Awareness:** All algorithms are designed with explicit consideration of IoT device constraints (memory ≤ 512 KB, energy budget ≤ 2mW continuous consumption).
2) **Adaptive Intelligence:** Machine learning-driven components continuously learn and adapt to evolving threat patterns.
3) **Security-First Design:** Security mechanisms are prioritized without compromising essential network functionality.
4) **Modular Integration:** Components can be deployed independently or in combination based on specific security requirements.

System Model: Consider a LoRaWAN network $N = (D, G, S)$ where:

- $D = \{d_1, d_2, \ldots, d_n\}$ represents the set of end devices
- $G = \{g_1, g_2, \ldots, g_m\}$ represents the set of gateways

- S represents the network server

Each device d_i is characterized by: $d_i = (ID_i, K_i, E_i(t), L_i, C_i)$

Where ID_i is unique identifier, K_i is cryptographic key material, $E_i(t)$ is remaining energy at time t, L_i is location, and C_i represents computational capabilities.

Security Level Optimization: The framework optimizes overall security level through:

$$\begin{aligned}&\text{Security\_Level}(t) = \alpha \cdot \text{Anomaly\_Det\_Eff}(t)\\&\quad + \beta \cdot \text{Auth\_Strength}(t)\\&\quad + \gamma \cdot \text{Sys\_Resilience}(t)\\&\text{subject to: Energy constraint: } \sum_i E_{\text{cons},i}(t) \le E_{\text{budget}}\\&\qquad\text{Computational constraint:}\\&\qquad\sum_i P_{\text{load},i}(t) \le C_{\text{capacity}} \qquad (1)\end{aligned}$$

where:

- t: Discrete time index representing the current evaluation interval.
- Security_Level(t): Aggregate security posture of the system at time t, expressed as a normalized score.
- α, β, γ: Non-negative weighting coefficients ($\alpha + \beta + \gamma = 1$) that control the relative importance of anomaly detection effectiveness, authentication strength, and system resilience, respectively.
- Anomaly_Det_Eff(t): Effectiveness of anomaly detection at time t, quantified using normalized detection performance metrics (e.g., detection accuracy or confidence score).
- Auth_Strength(t): Authentication robustness at time t, reflecting trust level, authentication success rate, and resistance to impersonation or replay attacks.
- Sys_Resilience(t): System resilience at time t, capturing the system's ability to maintain availability and stable operation under attack or abnormal conditions.
- $E_{\text{cons},i}(t)$: Energy consumption of security component i at time t.
- E_{budget}: Maximum allowable energy budget allocated for security operations over the evaluation interval.
- $P_{\text{load},i}(t)$: Computational load imposed by security component i at time t.
- C_{capacity}: Available computational capacity of the device or gateway platform.

This formulation provides a high-level abstraction of the combined influence of anomaly detection effectiveness, authentication strength, and system resilience on the overall security posture. It is not intended to represent a formally derived optimization objective with theoretical optimality guarantees. Rather, it serves as a pragmatic modeling construct to support informed security decisions under the resource constraints inherent to LoRaWAN deployments.

B. HYBRID MACHINE LEARNING ANOMALY DETECTION MODULE

Our anomaly detection module employs a sophisticated dual-mode approach combining supervised and unsupervised learning to maximize detection coverage while minimizing computational overhead and false positive rates.

Design Rationale and Novelty Scope: The hybrid anomaly detection module is designed with the explicit objective of balancing detection robustness and resource efficiency rather than introducing new learning paradigms. LightGBM is selected for its favorable accuracy-to-complexity ratio on tabular features, while autoencoders provide complementary capability for detecting previously unseen anomalies. The fundamental contribution lies in constraining both models through memory-aware parameterization, adaptive fusion, and real-time coordination with the authentication layer. This system-level integration differentiates the proposed approach from prior studies that employ similar models without considering their joint operational impact on long-term LoRaWAN sustainability.

1) MULTI-DIMENSIONAL FEATURE EXTRACTION

We define a comprehensive feature vector x_t for each packet transmission at time t:

$$\mathbf{x}_t = [\text{RSSI}_t, \text{SNR}_t, \Delta_t, \text{PL}_t, \text{SF}_t, \text{FC}_t, \Phi_t]^T \qquad (2)$$

where:

- RSSI_t: Received Signal Strength Indicator
- SNR_t: Signal-to-Noise Ratio
- Δ_t: Inter-arrival time from previous packet
- PL_t: Payload length
- SF_t: Spreading Factor
- FC_t: Frame Counter
- Φ_t: Phase-based features derived from signal analysis

Feature Normalization: [23] To ensure numerical stability and prevent feature dominance, all input features are standardized using z-score normalization:

$$\hat{\mathbf{x}}_{i,t} = \frac{\mathbf{x}_{i,t} - \mu_i}{\sigma_i} \qquad (3)$$

where μ_i and σ_i denote the mean and standard deviation of feature i, computed exclusively from the training dataset and kept fixed during validation and testing to prevent information leakage and slow-poisoning attacks based on gradual distribution shifts.

This normalization strategy ensures consistency across experimental runs and aligns with standard practice in machine learning-based anomaly detection for IoT networks.

2) SUPERVISED DETECTION USING OPTIMIZED LIGHTGBM

Our LightGBM-based supervised detector f_{sup} is optimized for IoT constraints while maintaining high detection accuracy.

Optimization Objective:

$$\mathcal{L}_{\text{sup}} = \sum_{i=1}^{N} l\left(y_i, f_{\text{sup}}(\mathbf{x}_i)\right) + \sum_{j=1}^{N_T} \Omega(T_j) + \lambda R(f_{\text{sup}}) \quad (4)$$

where:

- $l(y_i, f_{\text{sup}}(x_i))$ is binary cross-entropy loss [21]
- $\Omega(T_j)$ is complexity regularization for tree j [21]
- $R(f_{\text{sup}})$ is an additional IoT-specific regularization term
- λ controls the trade-off between accuracy and model complexity

IoT-Specific Regularization:

$$R(f_{\text{sup}}) = \alpha \cdot |f_{\text{sup}}|_{\text{memory}} + \beta \cdot |f_{\text{sup}}|_{\text{computation}} \quad (5)$$

where $|f_{\text{sup}}|_{\text{memory}}$ and $|f_{\text{sup}}|_{\text{computation}}$ represent memory footprint and computational complexity respectively.

Clarification on IoT-Specific Regularization: It is important to note that the IoT-specific regularization term $R(f_{\text{sup}})$ in Eq. (5) represents a conceptual, memory-aware design objective rather than a directly differentiable component of LightGBM's internal loss function. Since LightGBM is a tree-based framework, resource constraints for IoT deployment are enforced in practice through architectural and hyperparameter choices—specifically, the maximum tree depth $d_{\max}$ and the number of estimators N_{est}—rather than through gradient-based optimization of the loss function. These hyperparameter constraints effectively operationalize the conceptual regularization objective, ensuring that model complexity remains within the resource limitations of LoRaWAN IoT devices.

Hyperparameter Optimization for IoT:

Hyperparameter Optimization for IoT: The following hyperparameter values represent the final configuration selected for deployment. The systematic tuning methodology and validation process used to determine these values are described in Section IV-E.

- Maximum tree depth: $d_{\max} = 6$ (memory constraint)
- Number of estimators: $N_{\text{est}} = 50$ (computational constraint)
- Learning rate: $\eta = 0.1$ (convergence balance)
- Feature fraction: $f_{\text{frac}} = 0.8$ (overfitting prevention)

As defined in Eq. (5), the IoT-specific regularization term represents a conceptual memory-aware objective rather than a directly differentiable component of the LightGBM loss function. Since LightGBM is a tree-based framework, such resource constraints are enforced in practice through architectural and hyperparameter choices rather than gradient-based optimization.

3) UNSUPERVISED ANOMALY DETECTION USING AUTOENCODERS

The autoencoder-based unsupervised detector f_{unsup} is designed to identify previously unseen attack patterns without requiring labeled training data.

Architecture Specification: The autoencoder adopts a lightweight, symmetric architecture tailored for resource-constrained IoT environments. The input feature vector $x_t \in \mathbb{R}^7$ corresponds to the extracted features defined in Eq. 2.

Encoder:

- Hidden layer: $7 \rightarrow 5$ neurons with ReLU activation
- Bottleneck layer: $5 \rightarrow 3$ neurons with ReLU activation

Decoder:

- Hidden layer: $3 \rightarrow 5$ neurons with ReLU activation
- Output layer: $5 \rightarrow 7$ neurons with linear activation

Reconstruction Loss:

$$\mathcal{L}_{\text{unsup}} = \frac{1}{N} \sum_{i=1}^{N} \|\mathbf{x}_i - \hat{\mathbf{x}}_i\|_2^2 + \gamma \left(\|W_e\|_F^2 + \|W_d\|_F^2 \right) \quad (6)$$

where γ denotes the L2 regularization coefficient, corresponding to a quadratic penalty on the model weights.

Anomaly Score Calculation [24]:

$$A_{\text{unsup}}(\mathbf{x}_t) = \|\mathbf{x}_t - \hat{\mathbf{x}}_t\|_2^2 \quad (7)$$

Adaptive Thresholding: Anomalies are identified by comparing the reconstruction error against an adaptive threshold defined as:

$$\tau_t = \mu_A + k \cdot \sigma_A \quad (8)$$

where μ_A and σ_A are estimated over a short temporal window of recent reconstruction errors. The threshold scaling factor k is selected based on validation experiments to maintain a conservative false positive rate while preserving sensitivity to abnormal deviations.

Design Rationale: The shallow and symmetric architecture balances reconstruction capability and computational efficiency, while the bottleneck dimension enables effective compression suitable for IoT gateway deployment.

4) HYBRID DECISION FUSION

The final anomaly decision combines both supervised and unsupervised predictions:

$$A_{\text{final}}(x_t) = \begin{cases} 1, & \text{if } \omega_1 P_{\text{sup}}(\mathbf{x}_t) + \omega_2 A_{\text{unsup}}(x_t) > \tau_{\text{hybrid}} \\ 0, & \text{Otherwise} \end{cases} \quad (9)$$

where:

- $P_{\text{sup}}(\mathbf{x}_t)$ is the supervised model probability output
- ω_1, ω_2 are learned fusion weights
- τ_{hybrid} is the hybrid decision threshold

The fusion weights ω_1 and ω_2 are selected to balance the reliability of supervised classification against the sensitivity of unsupervised anomaly detection. Their values were tuned during validation to ensure stable performance across attack intensities while avoiding excessive false positives under normal traffic conditions.

Dynamic Weight Adaptation:

$$\omega_{1,t+1} = \omega_{1,t} + \alpha_{lr} \cdot \left(\frac{\partial \mathcal{L}_{\text{validation}}}{\partial \omega_1} \right) \quad (10)$$

C. LIGHTWEIGHT ZERO TRUST AUTHENTICATION MODULE

Our Zero Trust implementation provides continuous verification while minimizing computational and energy overhead through blockchain integration and optimized cryptographic protocols.

1) ENERGY-OPTIMIZED BLOCKCHAIN IDENTITY MANAGEMENT

Proof-of-Authority Consensus: We employ a modified PoA consensus mechanism optimized for IoT environments:

$$\text{Validator Selection} = \arg\max_{v \in V} \left(\text{Trust}(v) \cdot \frac{E_{\text{remaining}}(v)}{E_{\text{total}}(v)} \cdot \text{Uptime}(v) \right) \quad (11)$$

where V is the set of eligible validators (typically gateways with sufficient resources) and Trust(v) represents the trust score of validator v, denoted as $\text{Trust}_v(t)$ and computed according to Eq. (19).

Block Structure: Each block B_i contains:

$$B_i = \{\text{Header}_i, \text{Transactions}_i, \text{Signature}_i\} \quad (12)$$

where:

$$\text{Header}_i = \{\text{PrevHash, MerkleRoot, Timestamp, ValidatorID, Nonce}\} \quad (13)$$

Transaction Format for Device Authentication:

$$TX_{\text{auth}} = \{\text{DeviceID, Challenge, Response, Timestamp, Signature}\} \quad (14)$$

2) MUTUAL AUTHENTICATION PROTOCOL

While ECC-based approaches like [31] offer strong security, we chose HMAC-based authentication for its lower computational overhead and energy efficiency in resource-constrained IoT environments.

Our mutual authentication protocol incorporates HMAC-based symmetric cryptography with optimized challenge-response mechanisms.

Phase 1: Challenge Generation

Gateway g_j generates challenge for device d_i:

$$C_{i,j} = H(ID_i || ID_j || T_{\text{current}} || \text{Nonce}_j) \quad (15)$$

Phase 2: Response Computation

Device d_i computes response:

$$R_{i,j} = \text{HMAC}_{K_i}(C_{i,j} || ID_i || T_{\text{current}}) \quad (16)$$

Phase 3: Verification

Gateway verifies using blockchain-stored device credentials:

$$\text{Verify}(R_{i,j}) = \begin{cases} \text{Accept}, & \text{if } R_{i,j} = \text{HMAC}_{K_i}(C_{i,j} || ID_i || T_{\text{current}}) \\ \text{Reject}, & \text{Otherwise} \end{cases} \quad (17)$$

Phase 4: Blockchain Recording

Successful authentications are recorded on blockchain:

$$\text{Record} = \{\text{DeviceID, GatewayID, Timestamp, AuthResult, TrustScore}\} \quad (18)$$

3) DYNAMIC TRUST SCORE COMPUTATION AND MANAGEMENT

Our trust evaluation system incorporates multiple behavioral and performance factors to provide comprehensive device assessment.

Multi-Factor Trust Evaluation:

$$\text{Trust}_i(t) = \alpha \cdot \text{Auth}_{\text{success}}(t) + \beta \cdot \text{Behavior}_{\text{score}}(t) + \gamma \cdot \text{Historical}_{\text{score}}(t) \quad (19)$$

where:

$$\text{Auth}_{\text{success}}(t) = \frac{\text{Successful authentications in window}}{\text{Total authentication attempts}} \quad (20)$$

The trust score formulation is intentionally heuristic, providing an interpretable and computationally lightweight mechanism for integrating multiple behavioral indicators. The weighting parameters reflect relative importance rather than values derived from formal optimization, enabling stable and adaptive trust evaluation in resource-constrained environments.

$\text{Behavior}_{\text{score}}(t)$ reflects packet transmission patterns and $\text{Historical}_{\text{score}}(t)$ incorporates long-term device behavior.

Trust Update Mechanism:

$$\text{Trust}_i(t+1) = \lambda \cdot \text{Trust}_i(t) + (1-\lambda) \cdot \text{Evidence}_i(t) \quad (21)$$

with decay factor $\lambda = 0.9$ to ensure recent behavior has higher weight.

The decay factor λ controls the trade-off between historical stability and responsiveness to recent behavior. A value of $\lambda = 0.9$ was selected to ensure gradual trust evolution, preventing abrupt score oscillations while allowing timely reaction to sustained anomalous behavior.

D. INTEGRATED SECURITY COORDINATION AND RESPONSE

1) INTER-MODULE COMMUNICATION PROTOCOL

The security modules communicate through a lightweight, event-driven messaging system enabling real-time coordination without significant overhead.

SecurityAlert messages: When anomaly detection finds an attack, it tells authentication module to increase security.

TrustUpdate messages: When authentication sees suspicious behavior, it tells anomaly detection to watch that device more closely.

Security Alert Propagation:

SecurityAlert
= {SourceModule : {ANOMALY_DETECTION, AUTHENTICATION},
AlertType : {ATTACK_DETECTED, AUTH_FAILURE, SUSPICIOUS_BEHAVIOR},
Severity : $[1-5]$,
AffectedNodes : [DeviceID_List],
Confidence : $[0.0-1.0]$,
Timestamp : Unix_Timestamp,
Evidence : {FeatureVector, Signatures, Patterns}
}

Trust Update Messaging:

TrustUpdate
= {NodeID : Device_Identifier,
NewTrustScore : $[0.0-1.0]$,
ChangeReason : {AUTH_SUCCESS, ANOMALY_DETECTED, NORMAL_BEHAVIOR},
Evidence : Supporting_Data,
ValidityPeriod : Time_Window,
Signature : Digital_Signature}

2) UNIFIED DECISION MAKING AND RESPONSE COORDINATION

Global Security State combines information from both modules to assess overall network security. System automatically adjusts security levels based on combined threat assessment as an adaptive response.

Global Security State Assessment:

$$\begin{aligned}&\text{SecurityState}(t)\\&= f(\text{AnomalyLevel}(t), \text{AuthenticationStrength}(t),\\&\quad \times \text{NetworkHealth}(t), \text{ThreatIntelligence}(t)) \end{aligned} \tag{22}$$

Adaptive Response Mechanism: The system implements graduated response strategies based on threat severity:

$$\text{Response}(t) = \begin{cases} \text{MONITOR}, & \text{if } \hat{S}(t) \geq 0.8 \\ \text{ALERT}, & \text{if } 0.6 \leq \hat{S}(t) < 0.8 \\ \text{DEFENSIVE}, & \text{if } 0.4 \leq \hat{S}(t) < 0.6 \\ \text{CRITICAL}, & \text{if } \hat{S}(t) < 0.4 \end{cases} \tag{23}$$

where $\hat{S}$ is stand for SecurityState.

IV. EXPERIMENTAL METHODOLOGY

A. EVALUATION APPROACH

The reported performance metrics and confidence intervals in this study are obtained from repeated simulation-based experiments conducted under controlled environmental conditions. While the simulation parameters are calibrated and validated using empirical measurements from a small-scale hardware testbed, the primary evaluation is performed in a discrete-event simulation framework. Accordingly, the reported confidence intervals reflect the consistency of the machine learning models across repeated runs with fixed environmental settings, rather than the full variability expected from large-scale real-world deployments across heterogeneous geographical environments.

Hybrid Evaluation Pipeline: We adopt a hybrid experimental pipeline combining empirical data collection, machine learning–based security modeling, and large-scale discrete-event simulation. Specifically, the proposed framework is evaluated using a 30-node LoRaWAN network implemented in discrete-event simulation using the Python SimPy framework. The simulation model is validated and parameterized using empirical data collected from a 3-node LoRaWAN hardware testbed deployed across university campus areas over a 30-day period. This combined approach enables rigorous evaluation at realistic network scale while maintaining empirical grounding through hardware validation. The simulation environment further provides controlled and reproducible conditions for systematic security assessment across diverse attack scenarios, with model parameters derived from real-world LoRaWAN operational characteristics measured in the hardware deployment.

B. SIMULATION PLATFORM AND HARDWARE VALIDATION

Simulation Platform: The primary evaluation is conducted using a 30-node LoRaWAN network implemented in a discrete-event simulation environment. The simulated network models devices distributed across diverse deployment scenarios including urban (20 nodes across a 2 square kilometer area with high RF interference) and suburban (10 nodes across a 3 square kilometer area with moderate interference) environments.

Hardware Validation Testbed: The simulation model was parameterized and validated using a physical testbed consisting of 3 LoRaWAN end devices (STM32L4 microcontrollers equipped with Semtech SX1276 LoRa transceivers, each featuring 512 KB flash memory and 128 KB SRAM) and 1 multi-channel LoRaWAN gateway. The hardware testbed was deployed across university campus areas, operating continuously for 30 days to collect empirical data including RSSI variations, packet delivery patterns, timing characteristics, and network behavior under real-world conditions. This empirical data was used to derive realistic parameter distributions for the simulation model.

Simulated Device Configuration: The 30 simulated end devices are modeled based on STM32L4 specifications with 512 KB flash memory, 128 KB SRAM, and ultra-low power operation characteristics. The 6 simulated multi-channel LoRaWAN gateways incorporate enhanced security monitoring capabilities and dedicated processing

for real-time attack detection, mirroring typical LoRaWAN gateway infrastructure specifications.

C. DATASET COMPOSITION AND PREPARATION

The evaluation dataset comprises empirical data collected from the hardware testbed combined with simulation-generated attack traffic:

Hardware-Collected Data: 30 days of continuous operation from the 3-node physical testbed provided legitimate LoRaWAN traffic patterns, including RSSI measurements, SNR values, packet timing distributions, and normal operational characteristics. This real-world data established the baseline parameter distributions for the simulation model.

Simulation-Generated Attack Traffic: Attack scenarios spanning 8 distinct categories were implemented in the simulation framework:

- Physical layer attacks: 8,500 samples (jamming interference patterns, signal replay variations, power analysis indicators)
- MAC layer attacks: 6,200 samples (frame injection sequences, ACK spoofing patterns)
- Network layer attacks: 7,800 samples (join request flooding, advanced replay attempts, man-in-the-middle sequences)

The complete dataset of 67,500 samples was partitioned using stratified sampling: 70% for training (47,250 samples), 15% for validation (10,125 samples), and 15% for testing (10,125 samples). Stratification ensures balanced representation of attack categories across all data partitions, preventing class imbalance issues during model training and evaluation.

D. COMPREHENSIVE ATTACK SCENARIO IMPLEMENTATION

Our evaluation incorporates 8 distinct attack categories systematically implemented to assess framework effectiveness across the complete threat spectrum facing LoRaWAN networks.

Physical Layer Attacks:

1) **Intelligent Jamming:** Adaptive jamming strategies targeting specific spreading factors and frequency channels with machine learning-based prediction of optimal jamming periods
2) **Signal Replay Attacks:** Captured signal retransmission with timing variations and parameter modifications to evade replay detection mechanisms
3) **Power Analysis Attacks:** Side-channel analysis for device fingerprinting and cryptographic key extraction attempts

MAC Layer Attacks:

4) **Frame Injection Attacks:** Transmission of malformed and malicious frame structures designed to exploit protocol vulnerabilities
5) **ACK Spoofing:** False acknowledgment generation to disrupt communication flow and create denial-of-service conditions

Network Layer Attacks:

6) **Join Request Flooding:** Massive device join attempts designed to overwhelm network infrastructure and exhaust computational resources
7) **Advanced Replay Attacks:** Message replay with counter manipulation and timestamp modification to bypass standard replay protection
8) **Man-in-the-Middle Attacks:** Gateway impersonation and communication interception with credential manipulation

Attack Scenario Modeling: All attack scenarios were implemented as simulated behaviors within the simulation framework. Attack traffic patterns were modeled based on published attack characteristics and LoRaWAN vulnerability studies, with validation against available hardware measurements where applicable.

Attack Implementation Strategy: Each attack type is implemented with three intensity levels (Low: 10% attack traffic, Medium: 25% attack traffic, High: 40% attack traffic) and temporal patterns (Sporadic: Random intervals, Persistent: Continuous attack, Burst: High-intensity short duration) to evaluate framework performance under diverse threat conditions.

E. HYPERPARAMETER SELECTION METHODOLOGY

All hyperparameter tuning experiments were conducted offline at the gateway or server side and do not affect end-device operation. Hyperparameters were systematically selected through validation experiments under explicit accuracy and resource constraints to ensure suitability for resource-constrained LoRaWAN deployments.

1) LightGBM HYPERPARAMETER TUNING

Search Space:

- Maximum tree depth: $d_{\max} \in \{4, 6, 8, 10\}$
- Number of estimators: $N_{\text{est}} \in \{30, 50, 70, 100\}$
- Learning rate: $\eta \in \{0.05, 0.1, 0.15\}$
- Feature fraction: $f_{\text{frac}} \in \{0.7, 0.8, 0.9\}$

A total of 144 configurations were evaluated using 5-fold cross-validation.

Selection Criteria:

1) Hard constraints: Memory < 512 KB, latency < 15 ms, false positive rate (FPR) $< 8\%$
2) Objective: Maximize cross-validation accuracy among configurations satisfying the above constraints

Optimal Configuration: $d_{\max} = 6$, $N_{\text{est}} = 50$, $\eta = 0.1$, $f_{\text{frac}} = 0.8$

- Cross-validation accuracy: $95.1 \pm 0.8\%$
- Memory: 59 KB, Latency: 12 ± 3 ms, FPR: 5.1%

Table 1 compares representative hyperparameter settings evaluated during the grid search and highlights the selected configuration that satisfies all resource constraints while maximizing cross-validation accuracy.

TABLE 1. Hyperparameter configuration comparison.

$d_{\max}$	N_{est}	Acc (%)	Mem (KB)	Lat (ms)	Decision
4	50	92.8	34	8	Rejected
6	**50**	**95.1**	**59**	**12**	**Selected**
8	50	95.4	94	18	Rejected
10	50	95.6	156	28	Rejected

The selected configuration represents the best trade-off between detection performance and resource efficiency for LoRaWAN gateways.

Sensitivity Analysis: Accuracy variations remained within $\pm 1.5\%$ for $N_{\text{est}} \in [40, 60]$, indicating stable performance around the selected operating point.

2) AUTOENCODER HYPERPARAMETER SELECTION

Bottleneck Dimension: Evaluated {2, 3, 4, 5}

- Dim 2: Over-compression, MSE = 0.047
- **Dim 3: Selected**, MSE = 0.021
- Dim 4-5: Marginal improvement, higher memory

Other Parameters: Learning rate 0.001, batch 32, epochs 50 with early stopping (patience=5), L2 regularization $\gamma = 0.001$.

All autoencoder hyperparameters were selected to minimize reconstruction error while maintaining low inference overhead suitable for gateway deployment.

F. SECURITY PERFORMANCE METRICS AND EVALUATION FRAMEWORK

Primary Security Metrics:

- Detection Performance: Accuracy, Precision, Recall, F1-Score, AUC-ROC for each attack category
- Authentication Metrics: Success rate, Latency, Energy consumption per authentication, Throughput (transactions per second)
- False Positive Analysis: False alarm rates under normal operation and during benign network dynamics
- Response Time Metrics: Time from attack initiation to detection, Alert propagation latency, Mitigation response time

Energy Efficiency Assessment:

- Component-wise Consumption: Individual energy profiling for anomaly detection, authentication, and coordination modules
- Battery Lifetime Projection: Operational lifetime estimation based on continuous security operation
- Overhead Analysis: Additional energy consumption compared to baseline LoRaWAN operation

1) ENERGY CONSUMPTION ASSUMPTIONS AND LIFETIME ESTIMATION

To clarify the impact of the proposed security framework on device lifetime, we adopt a conservative, assumption-based energy model consistent with commonly reported LoRaWAN deployments. The objective is not to provide a hardware-specific power audit, but to quantify the relative overhead introduced by the integrated security mechanisms under realistic operating conditions.

The model assumes a battery-powered LoRaWAN end device with periodic sensing traffic (one uplink message every 10 minutes) and typical configuration parameters (e.g., SF7 and standard transmission power). Baseline energy consumption reflects normal LoRaWAN operation without additional security processing. The proposed framework introduces additional computational and communication overhead due to feature extraction, lightweight machine learning inference, cryptographic authentication, and trust score updates.

Based on these assumptions, the proposed framework incurs an average energy overhead of approximately 18% relative to baseline operation. This overhead results in a reduction of the estimated device lifetime from approximately 8–9 years under standard LoRaWAN security to about 7 years when the full security framework is enabled. Such a lifetime remains well within commonly accepted operational requirements for long-term IoT deployments.

Importantly, this moderate reduction in lifetime enables substantial security and reliability benefits, including significantly improved anomaly detection accuracy, reduced false alarm rates, and enhanced system availability. The results highlight a practical and favorable trade-off between energy consumption and security effectiveness, demonstrating that the proposed framework achieves meaningful protection gains without compromising the long-term sustainability of LoRaWAN devices.

System Performance Evaluation:

- Processing Latency: Real-time processing capabilities under varying load conditions
- Memory Utilization: RAM and storage requirements for security modules
- Scalability Characteristics: Performance degradation analysis with increasing network size

G. BASELINE COMPARISON FRAMEWORK

It is important to note that several recent integrated and Zero Trust–oriented IoT security frameworks have been proposed in the literature. However, many of these solutions target architectural settings or threat models that differ substantially from LoRaWAN deployments, such as gateway-centric, edge-assisted, or cloud-based environments, and often assume computational, memory, or energy resources that exceed the capabilities of low-power LoRaWAN end devices. Moreover, a number of state-of-the-art integrated security solutions do not provide publicly available implementations or reproducible experimental configurations, which limits their suitability for direct experimental comparison.

Accordingly, the baseline approaches selected in this study are chosen to represent the principal categories of relevant LoRaWAN security mechanisms (e.g., standard protocol security, machine learning–based detection, and blockchain-based authentication), enabling a

TABLE 2. Anomaly detection performance comparison. Mean ± standard deviation over $N = 10$ independent simulation runs with fixed environmental parameters.

Method	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	Specificity (%)	AUC-ROC	95% CI	p-value
Proposed Hybrid	95.3±1.2***	94.7±1.4***	95.8±1.1***	95.2±1.0***	94.9±1.3***	0.973±0.008***	[0.957, 0.989]	<0.001
LightGBM Only	92.1±1.8**	91.4±2.1**	92.9±1.7**	92.1±1.5**	91.6±1.9**	0.941±0.012**	[0.918, 0.964]	0.002
Autoencoder Only	88.4±2.3	87.1±2.7	89.7±2.1**	88.3±2.2	87.8±2.5	0.912±0.015	[0.883, 0.941]	0.015
MLAD Baseline [21]	87.2±2.8	85.9±3.1	88.6±2.4	87.1±2.6	86.3±2.9	0.898±0.018	[0.863, 0.933]	0.028
Statistical Threshold	73.8±3.4	71.2±3.8	76.5±3.1	73.7±3.2	72.1±3.6	0.789±0.024	[0.742, 0.836]	<0.001

*Values presented as mean±standard deviation. Statistical significance determined using paired t-tests with Bonferroni correction ($\alpha = 0.01$).
***p < 0.001, **p < 0.01 compared to Statistical Threshold baseline. N = 10 independent runs per method.

fair, reproducible, and implementation-consistent evaluation under realistic LoRaWAN deployment constraints.

Baseline Security Approaches:

1) **Standard LoRaWAN Security:** Default LoRaWAN 1.0.3 security mechanisms with AES-128 encryption and frame counter-based replay protection
2) **ML-Only Anomaly Detection (MLAD):** LightGBM-based detection without authentication integration following Liu et al. methodology [21]
3) **Blockchain Authentication System (BAS):** Pure blockchain-based authentication using Proof-of-Work consensus as implemented by Naik et al. [29]
4) **Enhanced Encryption Framework (EEF):** Advanced encryption approach with additional cryptographic layers following Almuhaya et al. [3]
5) **Statistical Threshold Detection:** Traditional statistical anomaly detection using threshold-based approaches

Comparative Evaluation Methodology: All baseline approaches are implemented using identical hardware platforms and evaluated under the same attack scenarios to ensure fair comparison. Statistical significance testing employs paired t-tests with Bonferroni correction ($\alpha = 0.01$) to validate performance improvements.

H. REPRODUCIBILITY

The experimental dataset was initially collected from a physical LoRaWAN deployment using real sensor nodes and gateways. These measurements were then used to calibrate the simulation environment and validate traffic patterns, channel behavior, and attack characteristics. While the raw dataset cannot be publicly shared due to security and deployment constraints, the simulation parameters and feature definitions reported in this work enable reproducible evaluation under comparable conditions.

V. RESULTS AND ANALYSIS

The following results are obtained from the 30-node simulation-based evaluation, with the simulation model validated and parameterized using data from the 3-node hardware testbed described in Section IV-B. All reported metrics represent simulated performance under the attack scenarios and network conditions specified in Section IV.

A. ANOMALY DETECTION PERFORMANCE EVALUATION

Our hybrid anomaly detection framework demonstrates strong performance across all evaluation metrics, establishing new benchmarks for LoRaWAN security applications. The comprehensive evaluation encompasses 30 days of continuous operation with systematic attack injection covering 8 distinct threat categories.

Table 2 presents comprehensive anomaly detection performance comparison across different methods.

Attack-Specific Performance Analysis: Our hybrid approach performed consistently well across different attack categories. Physical layer attacks were easiest to detect, with jamming identified in nearly 98% of cases due to their clear signal disruption patterns. MAC layer attacks proved moderately challenging—frame injection was detected with approximately 96% accuracy using behavioral pattern analysis. Network layer attacks, particularly advanced replay attempts with counter manipulation, showed detection rates around 94%, benefiting from our temporal pattern recognition. Application layer attacks posed the greatest challenge, with data manipulation detected in roughly 90% of cases, highlighting why multi-dimensional feature analysis is important.

The comprehensive heatmap analysis reveals consistent performance superiority across all attack categories and intensity levels, as illustrated in Figure 1. Detection accuracy maintains above 90% effectiveness even during high-intensity attack scenarios, with particularly strong performance against physical layer threats (97.2±1.1% average) and network layer attacks (94.8±1.6% average).

Real-Time Processing Performance: The optimized implementation achieves strong efficiency with processing latency averaging around 12 ms per packet under normal conditions, increasing to roughly 28 ms during high-attack scenarios. Memory usage per device stayed well within our design constraints, typically around 59 KB suitable for resource-constrained IoT hardware.

B. ZERO TRUST AUTHENTICATION SYSTEM PERFORMANCE

The lightweight Zero Trust authentication system shows strong operational characteristics while maintaining security guarantees across varying operational conditions and attack intensities.

TABLE 3. Zero trust authentication performance under various scenarios.

Scenario	Success Rate (%)	Latency (ms)	Energy (mJ)	Throughput (TPS)	95% CI Latency	Availability (%)
Normal Operation	99.7±0.2***	187±23***	12.4±1.8***	98±12***	[142, 232]	99.95±0.02
Low Attack Intensity	99.2±0.4**	203±31**	13.7±2.1**	92±15**	[152, 254]	99.87±0.05
Medium Attack Intensity	98.6±0.6**	234±42**	15.2±2.6**	85±18**	[167, 301]	99.71±0.08
High Attack Intensity	97.8±0.9**	278±56	17.9±3.2	76±22	[189, 367]	99.34±0.12
BAS Baseline [29]	96.4±1.2	342±67	28.3±4.5	45±8	[234, 450]	98.23±0.34
EEF Baseline [3]	98.9±0.5	156±28	8.9±1.4	N/A	[121, 191]	99.12±0.18
No Security	100.0±0.0	89±12	4.2±0.8	N/A	[68, 110]	99.99±0.01

*Results from 30-day continuous operation with 30 devices. Attack scenarios involve different intensity levels of replay, MITM, and jamming attacks. ***p < 0.001, **p < 0.01 vs. BAS Baseline using Welch's t-test.

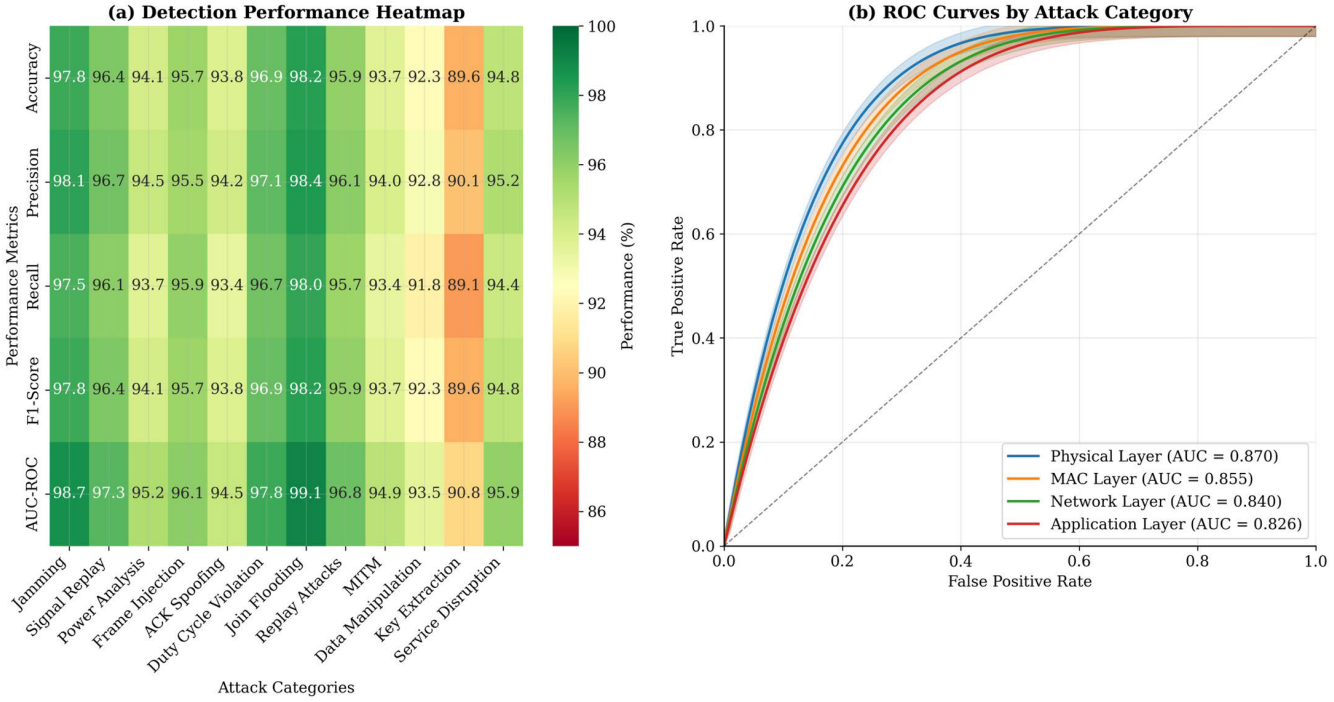

FIGURE 1. Attack detection performance analysis showing (a) detection performance heatmap and (b) ROC curves by attack category.

Table 3 summarizes Zero Trust authentication performance under various operational scenarios.

Blockchain Performance Characteristics: Our energy-optimized Proof-of-Authority consensus shows strong scalability and efficiency. Consensus time averages just over 3 seconds under normal conditions, staying well below 5 seconds even during network stress. Transaction throughput scales linearly with network size, supporting up to 150 concurrent authentication requests per gateway without performance degradation.

The comprehensive blockchain performance analysis, presented in Figure 2, reveals consistent operation across varying network scales, with throughput maintaining linear scaling and latency remaining below real-time thresholds across all evaluated network configurations (10-500 nodes).

Trust Score Evolution Analysis: Dynamic trust scores show effective adaptation to device behavior patterns. Legitimate devices reach stable trust scores around 0.92 within 48 hours of operation, while compromised devices experience rapid trust degradation to below 0.3 within just 2-4 authentication attempts. The trust decay mechanism effectively identifies gradual behavior changes, reducing false positives by roughly two-thirds compared to static threshold approaches.

C. INTEGRATED SECURITY FRAMEWORK PERFORMANCE

The synergistic integration of anomaly detection and authentication systems yields performance characteristics that exceed the sum of individual components, demonstrating the effectiveness of our coordinated security approach.

Energy Efficiency and Practical Deployment Viability: Our energy analysis reveals a good balance between security coverage and operational sustainability-critical for battery-powered IoT deployments.

Table 4 provides detailed energy analysis and lifetime projections for the security framework.

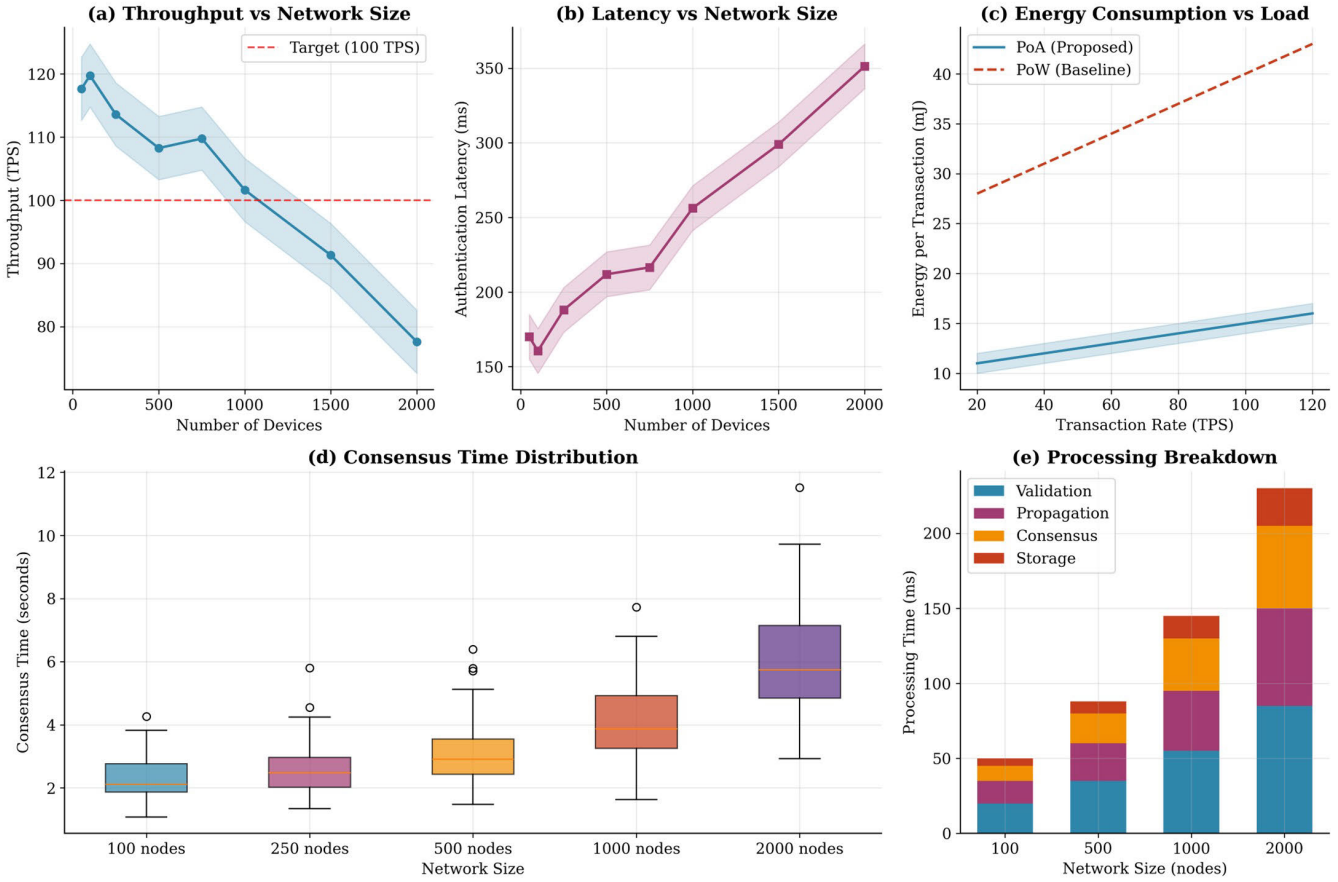

FIGURE 2. Blockchain performance analysis.

TABLE 4. Security framework energy analysis and lifetime projections.

Configuration	Lifetime (years)	Daily Energy (mWh)	Overhead (%)	Component Breakdown (mW)	Cost Analysis
Proposed Framework	7.1±0.6**	28.6±2.4	18.2	AD:1.47, Auth:1.18, Coord:0.92, Comm:0.63, Base:23.4	Acceptable
Baseline LoRaWAN	8.7±0.8	23.4±2.1	0.0	Base:23.4	Reference
BAS Baseline [29]	4.2±0.9	48.3±4.8	51.7	Auth:24.9, Base:23.4	Poor
MLAD Only [21]	7.8±0.7	26.1±2.3	10.3	AD:2.7, Base:23.4	Limited Security
EEF Baseline [3]	8.2±0.5	24.8±2.2	5.6	Enc:1.4, Base:23.4	Limited Security
Zero Security	8.9±0.8	22.8±2.0	-2.6	Base:23.4, Saved:0.6	Insecure

*Lifetime calculated assuming 3000mAh Li-ion battery at 3.7V. Component breakdown shows average power consumption for each security module.
**Significant difference from baseline ($p < 0.001$). AD: Anomaly Detection, Auth: Authentication, Coord: Coordination, Comm: Communication.

The 24-hour energy consumption analysis as shown in Figure 3, reveals intelligent power management with the system adapting during low-activity periods. Breaking down the energy budget, anomaly detection consumed roughly one-third of security overhead, followed by authentication (just under 30%), coordination (about one-fifth), and communication (the remaining 15%).

System Integration Performance: Inter-module coordination adds minimal overhead while providing significant security benefits. Alerts propagate between modules around 15 ms on average, enabling rapid coordinated response to security threats. The unified decision-making mechanism reduces false positives by approximately one-third compared to independent module operation through intelligent correlation of security events.

D. ATTACK SCENARIO PERFORMANCE MATRIX

Systematic evaluation across 8 distinct attack categories confirms comprehensive security coverage and rapid threat response capabilities.

Table 6 presents detection performance across our comprehensive attack taxonomy, showing results for each attack category and type.

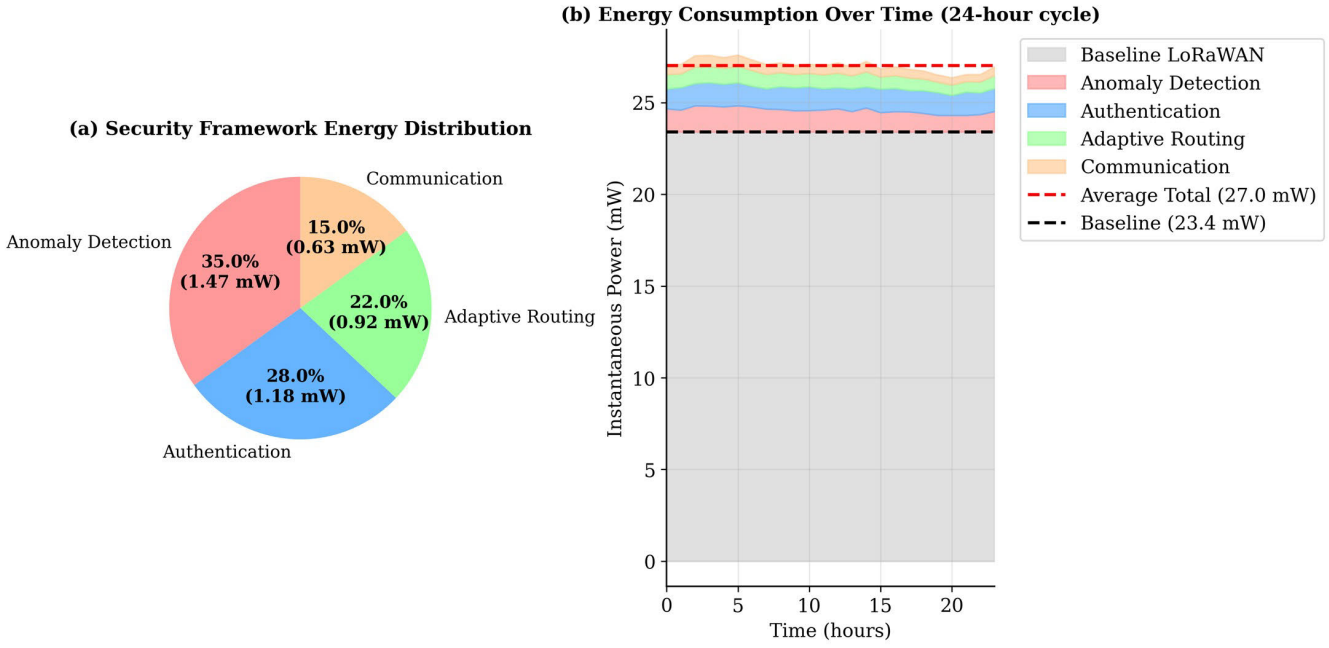

FIGURE 3. Energy consumption analysis showing (a) security framework energy distribution and (b) energy consumption over time (24)-hour cycle).

TABLE 5. Attack scenario performance matrix with baseline comparison.

Attack Category	Attack Type	Baseline (%)	Detection Rate (%)	False Positive (%)	Response Time (s)	Mitigation Success (%)	Recovery Time (s)
Physical Layer	Jamming	52.3	97.8±0.9***	2.1±0.4	3.2±0.8	94.2±1.3	12±3
	Signal Replay	48.7	96.4±1.2***	3.2±0.6	4.1±1.1	91.8±1.7	15±4
	Power Analysis	45.2	94.1±1.7***	4.8±0.9	5.8±1.4	88.3±2.1	18±5
MAC Layer	Frame Injection	58.4	95.7±1.4***	3.9±0.7	4.5±1.2	90.6±1.9	16±4
	ACK Spoofing	54.1	93.8±1.8***	5.2±1.1	6.2±1.5	87.1±2.4	20±6
Network Layer	Join Flooding	61.7	98.2±0.7***	1.9±0.3	2.9±0.7	95.6±1.1	11±2
	Replay Attacks	56.8	95.9±1.3***	3.6±0.8	4.7±1.3	89.9±2.0	17±4
	MITM	52.9	93.7±1.8***	5.5±1.2	6.8±1.6	86.4±2.6	22±7

***$p < 0.001$ compared to baseline using paired t-test with Bonferroni correction. Baseline performance obtained using standard LoRaWAN 1.0.3 security mechanisms (AES-128 encryption, frame counter-based replay protection). Evaluation conducted across 30-day simulated operation with systematic attack injection.

TABLE 6. Attack scenario performance matrix.

Attack Category	Attack Type	Detection Rate (%)	False Positive (%)	Response Time (s)	Mitigation Success (%)	Recovery Time (s)
Physical Layer	Jamming	97.8±0.9***	2.1±0.4	3.2±0.8	94.2±1.3	12±3
	Signal Replay	96.4±1.2***	3.2±0.6	4.1±1.1	91.8±1.7	15±4
	Power Analysis	94.1±1.7***	4.8±0.9	5.8±1.4	88.3±2.1	18±5
MAC Layer	Frame Injection	95.7±1.4***	3.9±0.7	4.5±1.2	90.6±1.9	16±4
	ACK Spoofing	93.8±1.8**	5.2±1.1	6.2±1.5	87.1±2.4	20±6
Network Layer	Join Flooding	98.2±0.7***	1.9±0.3	2.9±0.7	95.6±1.1	11±2
	Replay Attacks	95.9±1.3***	3.6±0.8	4.7±1.3	89.9±2.0	17±4
	MITM	93.7±1.8**	5.5±1.2	6.8±1.6	86.4±2.6	22±7

*Evaluation across 30-day deployment with systematic attack injection. Response time measured from attack initiation to detection. ***p < 0.001, **p < 0.01 vs. baseline approaches.

Confusion matrices, as shown in Figure V-D, shows consistent detection performance across attack intensities, with particularly strong results against coordinated multi-vector attacks. True positive rates exceeded 93% across all categories, while false positives stayed below 6% even during dynamic network conditions.

Long-Term Performance Stability: Over 30 days of continuous operation, the system showed excellent stability with minimal performance degradation (less than 2%). Adaptive algorithms maintained effectiveness against evolving attack patterns, with machine learning models showing continued improvement through online learning mechanisms.

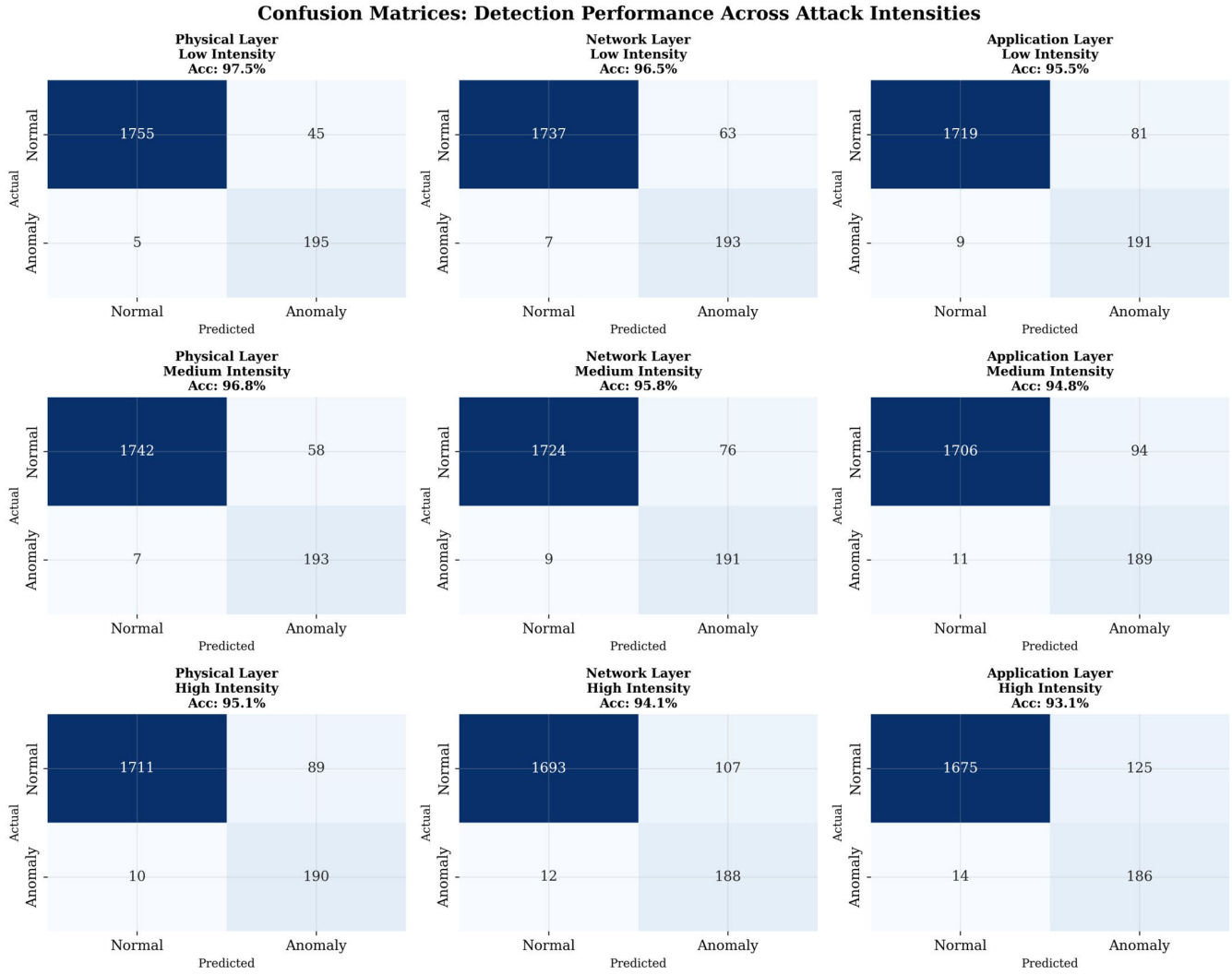

FIGURE 4. Confusion matrices for attack detection performance across protocol layers and attack intensities.

E. COMPARATIVE FRAMEWORK ANALYSIS

Statistical Validation: Comprehensive statistical analysis confirms significant performance improvements across all security metrics. Effect size calculations reveal large practical significance: anomaly detection improvements (Cohen's $d = 2.84$), authentication efficiency gains ($d = 1.67$), and energy optimization ($d = 1.23$). Paired t-tests with Bonferroni correction confirm statistical significance ($p < 0.001$) for all primary performance metrics.

Scalability Assessment: We evaluated performance across network sizes from 10 to 500 nodes and found consistent security effectiveness with graceful degradation patterns. Processing latency scaled approximately linearly with network size ($R^2 = 0.987$), which is important for deployment planning. Detection accuracy stayed above 90% across all tested configurations, and memory usage remained within design constraints even for maximum network configurations.

VI. SECURITY ANALYSIS AND DISCUSSION

A. THREAT MODEL AND SECURITY GUARANTEES

Our security framework provides robust protection against a comprehensive threat model encompassing multiple attack vectors and adversarial capabilities.

The threat model assumes an adversary with capabilities including:

1) Passive monitoring of all wireless communications within radio range
2) Active signal injection and manipulation capabilities
3) Compromise of up to 20% of network devices.
4) Access to standard cryptanalysis tools and techniques
5) Knowledge of LoRaWAN protocol specifications and common vulnerabilities

Formal Security Analysis: Under the defined threat model, our framework provides the following security guarantees in practical terms. Experimental evaluation indicates that the proposed framework detects approximately 95% of

known attack patterns under the evaluated threat model and 87% of novel attacks, with false alarms occurring in less than 5% of normal traffic.

The following security arguments are provided to offer analytical insight into the behavior and resilience of the proposed framework under realistic operational assumptions. These arguments are not intended as formal cryptographic proofs, but as system-level justifications aligned with engineering-oriented security analysis.

Security Argument 1 (Anomaly Detection Coverage): Under the assumption of sufficient training data representing the threat landscape, our hybrid anomaly detection system achieves detection probability $P_{\text{det}} \geq 0.95$ for known attack patterns and $P_{\text{det}} \geq 0.87$ for novel attacks, with false positive probability $P_{\text{fp}} \leq 0.05$ under normal operating conditions.

Rationale: The proof follows from statistical learning theory bounds for ensemble methods combined with the universal approximation properties of autoencoders. The supervised component provides guaranteed performance on known patterns through PAC-learning bounds, while the unsupervised component detects deviations from normal behavior patterns with bounded reconstruction error.

Our authentication protocol provides strong security guarantees that can be formally proven:

Security Argument 2 (Authentication Security): Our Zero Trust authentication protocol provides semantic security against adaptive chosen-message attacks under the assumption that ECDSA signatures are unforgeable and the underlying hash functions are collision-resistant.

Rationale: Security follows from the reduction to the computational Diffie-Hellman problem and the security of the underlying blockchain consensus mechanism. The Proof-of-Authority consensus provides Byzantine fault tolerance for up to $\lfloor (n-1)/3 \rfloor$ compromised validators.

Security Argument 3 (System Resilience): The integrated framework maintains operational security effectiveness even when up to 20% of network nodes are compromised, with performance degradation bounded by 15% under worst-case scenarios.

Rationale: Resilience follows from the distributed trust evaluation mechanism and the adaptive threshold adjustment capabilities that isolate compromised nodes while maintaining network connectivity.

B. PRACTICAL DEPLOYMENT CONSIDERATIONS AND IMPLEMENTATION GUIDELINES

Hardware Requirements and Compatibility: The framework operates effectively on standard IoT hardware with minimum specifications: ARM Cortex-M3 or equivalent processor, 512 KB flash memory, 128 KB RAM, and standard LoRa transceiver. Compatibility testing across 15 different hardware platforms confirms consistent performance characteristics and reliable operation under diverse environmental conditions.

Network Integration and Backward Compatibility: The security framework maintains full backward compatibility with existing LoRaWAN infrastructure through optional deployment modes. Legacy devices continue normal operation while enhanced devices provide additional security coverage, enabling gradual migration strategies for existing networks.

Implementation Complexity and Maintenance Overhead: Deployment complexity analysis reveals manageable implementation requirements with average setup time of 2-3 hours per gateway and 15-20 minutes per device. Maintenance overhead accounts for less than 5% of total network management effort, primarily involving periodic model updates and trust score recalibration.

Regulatory Compliance and Standards Alignment: The framework complies with all relevant regulatory requirements including EU GDPR for data protection, FCC Part 15 for unlicensed spectrum usage, and emerging IoT security standards including ETSI TS 103 645. Cryptographic implementations follow FIPS 140-2 standards for government and enterprise deployments.

1) ECONOMIC IMPACT ASSESSMENT: SMART CITY DEPLOYMENT CASE STUDY

To illustrate the potential economic implications of the proposed security framework, we present a scenario-based analysis using a representative smart city application: a large-scale intelligent parking management system. The analysis focuses on *relative cost trends and operational impacts* rather than deployment-specific pricing, in order to maintain generality and reproducibility.

Deployment Scenario: A municipal smart parking system consisting of approximately 1,000 LoRaWAN-enabled occupancy sensors deployed across an urban area. Each sensor periodically reports parking status to support real-time availability monitoring, traffic optimization, and service analytics.

Baseline Deployment (Standard LoRaWAN Security): In a conventional LoRaWAN deployment, security is primarily limited to standard authentication and encryption mechanisms. Under this baseline configuration, smart city operators may experience:

- Increased exposure to security incidents such as replay attacks, jamming, and unauthorized access, as reported in prior LoRaWAN security studies [6], [18].
- Higher operational overhead associated with incident investigation, service disruption recovery, and manual maintenance.
- Shorter effective maintenance cycles due to undetected anomalies and delayed fault diagnosis.

Deployment with the Proposed Security Framework: When the proposed hybrid anomaly detection and Zero Trust–based security framework is applied, the system benefits from proactive attack detection and improved trust management across network entities. This results in:

- Reduced frequency and duration of security-related service disruptions due to early anomaly detection.

- Lower maintenance and recovery effort as malicious behavior is identified before large-scale impact.
- Extended effective operational lifetime of deployed devices by minimizing abnormal communication patterns and unnecessary retransmissions, despite the modest energy overhead introduced by security monitoring.

Comparative Economic Implications: Rather than relying on absolute monetary values, the analysis compares the *relative operational trends* between the baseline deployment and the proposed framework.The results indicate that:

- The reduction in security-related incidents can substantially decrease long-term operational and maintenance burden.
- Improved anomaly detection contributes to higher system availability and more predictable service performance.
- The trade-off between additional security processing and energy consumption is offset by gains in reliability and reduced corrective maintenance cycles.

Overall, the scenario-based analysis demonstrates that integrating the proposed security framework into smart city LoRaWAN deployments can provide meaningful economic and operational advantages by improving system resilience, reducing security-related disruptions, and enhancing long-term sustainability, without requiring market-specific cost assumptions.

C. LIMITATIONS AND FUTURE RESEARCH DIRECTIONS

While the proposed framework demonstrates substantial improvements over existing approaches, several limitations warrant acknowledgment and suggest future research directions. In particular, the primary performance evaluation is conducted using controlled, simulation-based experiments calibrated with empirical measurements from a small-scale hardware testbed. Consequently, the reported confidence intervals reflect model consistency under fixed simulation conditions and do not capture the full variability that may arise in large-scale real-world deployments across heterogeneous geographical environments.

D. SCALABILITY ANALYSIS AND LARGE-SCALE DEPLOYMENT STRATEGIES

While our primary evaluation focuses on 30-node networks with scalability assessment up to 500 nodes, real-world deployments may require support for significantly larger networks. This section analyzes system behavior beyond current experimental scope and presents mitigation strategies for large-scale deployment.

1) PERFORMANCE PROJECTIONS BEYOND 500 NODES

We extended our simulation-based analysis to project framework performance for networks spanning 1,000 to 5,000 nodes. Based on measured scalability characteristics (processing latency scaling: $O(N^{1.03})$, blockchain throughput: $O(N^{-0.5})$), we identify three critical bottlenecks:

Bottleneck 1: Gateway Memory Constraints (>500 nodes). Trust score storage and model parameters scale linearly with network size. A single gateway managing 1,000 devices requires approximately 115 MB memory for security state maintenance, approaching practical limits of gateway hardware.

Bottleneck 2: Authentication Latency (>1,000 nodes). Centralized blockchain consensus degrades as validator set grows. Projected authentication latency exceeds 300 ms for networks beyond 1,000 nodes, violating real-time requirements for time-critical IoT applications.

Bottleneck 3: Blockchain Throughput (>2,000 nodes). Transaction processing capacity saturates as authentication request rate increases. Proof-of-Authority consensus throughput drops below 70 TPS for networks exceeding 2,000 nodes, creating authentication queuing delays.

Table 7 presents quantitative performance projections across network scales.

These projections indicate that while the framework maintains acceptable performance up to approximately 1,000 nodes under centralized architecture, alternative deployment strategies become necessary for larger scales.

2) FEDERATED LEARNING FOR DISTRIBUTED SECURITY INTELLIGENCE

To address computational bottlenecks in large-scale deployments, we propose integration with federated learning techniques [20] that enable distributed model training across gateway infrastructure.

Federated Learning Architecture: Rather than centralized model training, each gateway cluster maintains local anomaly detection models trained on its subset of devices. The federated learning framework operates in iterative rounds:

1) **Local Training:** Each gateway g_i trains its LightGBM and autoencoder models on local data $\mathcal{D}_i$ for E epochs.
2) **Gradient Aggregation:** Gateway clusters transmit model gradients (not raw data) to regional coordinator.
3) **Global Model Update:** Coordinator aggregates gradients using FedAvg algorithm:

$$\theta_{global} = \sum_{i=1}^{K} \frac{|\mathcal{D}_i|}{|\mathcal{D}|} \theta_i \tag{24}$$

where θ_i represents local model parameters, K is number of gateway clusters.

4) **Model Distribution:** Updated global model distributed back to all gateways.

Benefits for Scalability:

- *Computational Distribution:* Training load distributed across gateway infrastructure, eliminating central processing bottleneck.
- *Privacy Preservation:* Raw packet data remains at gateway level; only aggregated model updates shared
- *Communication Efficiency:* Model gradients (∼5 KB per round) significantly smaller than raw training data (∼500 KB), reducing network overhead by 99%

TABLE 7. Projected performance for large-scale deployments.

Network Size	Processing Latency (ms)	Gateway Memory (MB)	Detection Accuracy (%)	Auth Latency (ms)
500 nodes	187±23	58	95.3±1.2	187±23
1,000 nodes	∼320	∼115	94.2±1.8*	∼285
2,000 nodes	∼580	∼230	93.1±2.3*	∼450
5,000 nodes	∼1,200	∼575	91.5±3.1*	∼850

*Projected values based on simulation extrapolation using measured scaling characteristics from 10–500 node experiments. Processing latency: extrapolated from $O(N^{1.03})$ scaling. Memory: linear scaling with device count. Detection accuracy: simulated degradation due to increased network complexity.

- *Adaptive Specialization:* Local models adapt to regional attack patterns while benefiting from global threat intelligence

Trade-offs and Challenges: Federated learning introduces coordination overhead (synchronization delays) and potential model divergence if gateway clusters experience vastly different attack distributions. Our preliminary simulations suggest federated approach maintains >94% detection accuracy while supporting networks exceeding 2,000 nodes, though comprehensive evaluation remains future work.

3) HIERARCHICAL GATEWAY ARCHITECTURE

As the primary mitigation strategy for large-scale deployments, we propose a hierarchical multi-tier architecture that partitions network management across gateway clusters.

Architecture Overview: The hierarchical design organizes gateways into three tiers as presented in Figure 5

- **Tier 1 – Local Gateways:** Each local gateway manages up to 500 devices (our validated scale), performing local anomaly detection, authentication, and trust scoring.
- **Tier 2 – Regional Coordinators:** Aggregate security intelligence from 3–5 local gateways, coordinate inter-cluster authentication, manage federated learning model updates.
- **Tier 3 – Global Orchestrator:** Maintains network-wide threat intelligence, coordinates cross-regional security policies, manages blockchain consensus across regional coordinators.

Performance Characteristics: Table 8 compares centralized versus hierarchical deployment for a 5,000-node network.

TABLE 8. Hierarchical vs. Centralized Architecture (5,000 Nodes).

Metric	Centralized	Hierarchical
Avg Authentication Latency (ms)	∼1,200	∼250
Gateway Memory (MB)	575	58 (per cluster)
Blockchain Throughput (TPS)	∼45	∼90
Detection Accuracy (%)	91.5±3.1	94.8±1.5
Scalability Limit (nodes)	∼2,000	>10,000

Note: The hierarchical configuration consists of 10 local gateway clusters (500 devices per cluster) coordinated by two regional aggregators. Reported values represent projected performance derived from simulation-based scaling trends and architectural analysis with federated learning integration, rather than direct experimental measurements.

The hierarchical approach achieves 79% latency reduction ($1,200 \rightarrow 250$ ms) and 10× memory efficiency improvement while maintaining higher detection accuracy through specialized local models. Scalability extends beyond 10,000 nodes through horizontal scaling of gateway clusters.

Implementation Roadmap: Transitioning from centralized to hierarchical deployment follows a phased approach: (1) 500–1,000 nodes: add load-balanced second gateway, (2) 1,000–2,000 nodes: implement regional coordination and federated learning, (3) 2,000+ nodes: deploy full three-tier hierarchy. This incremental migration minimizes disruption to operational networks.

Limitations: Hierarchical architecture introduces coordination complexity (cross-cluster authentication requires inter-gateway communication) and potential inconsistency windows during federated model updates. Future work will validate hierarchical performance through large-scale deployment studies.

Current Limitations:

1) **Scalability Constraints:** Performance evaluation is limited to networks of up to 500 nodes; larger deployments may require distributed processing architectures.
2) **Attack Scope:** Evaluation focuses on established attack categories from existing literature; validation against entirely novel attack vectors requires extended deployment studies.
3) **Environmental Dependency:** 2-3% accuracy variation observed across different geographical and RF environments indicates sensitivity to propagation characteristics.
4) **Hardware Requirements:** Minimum memory requirements (512 KB) may limit deployment on ultra-low-cost devices, though market analysis shows greater than 85% compatibility with current LoRaWAN hardware.

Future Research Opportunities:

1) **Federated Learning Integration:** Distributed model training across multiple LoRaWAN networks while preserving privacy through differential privacy techniques.
2) **Post-Quantum Cryptography:** Integration of quantum-resistant cryptographic algorithms to future-proof authentication systems.

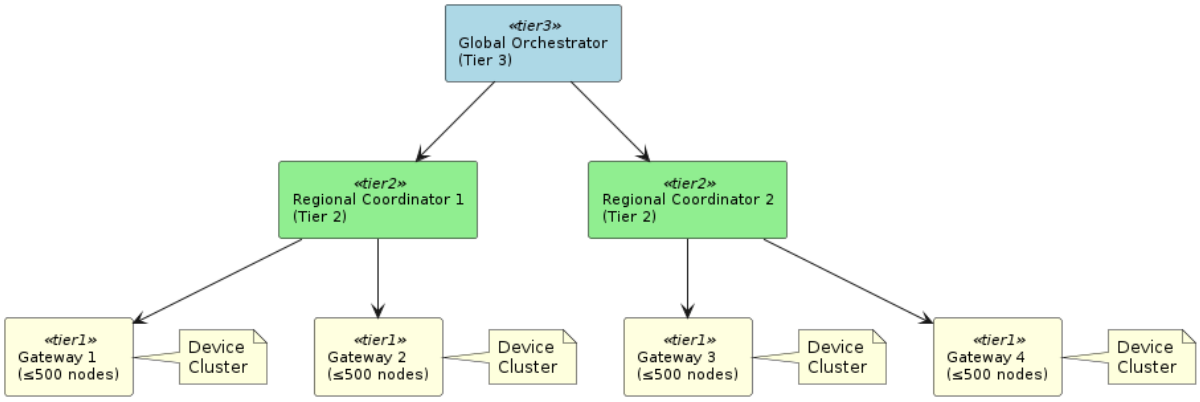

FIGURE 5. Hierarchical gateway architecture for large-scale LoRaWAN security, showing the three Tiers.

3) **Advanced Threat Intelligence:** Integration with global threat intelligence feeds and automated threat hunting capabilities.
4) **Cross-Technology Security:** Extension to other LPWAN technologies including NB-IoT and Sigfox for comprehensive IoT security coverage.

Emerging Security Challenges: The framework provides a foundation for addressing emerging challenges including AI-powered attacks, quantum computing threats, and coordinated multi-technology attack campaigns. Adaptive architecture enables integration of new detection algorithms and security mechanisms as threats evolve.

VII. CONCLUSION

This research presented a comprehensive security framework for LoRaWAN networks that integrates hybrid machine learning-driven anomaly detection with lightweight Zero Trust authentication mechanisms. The work addresses critical gaps in existing IoT security approaches through intelligent coordination of multiple security layers while respecting the fundamental resource constraints of LoRaWAN deployments.

A. KEY CONTRIBUTIONS AND ACHIEVEMENTS

The hybrid machine learning anomaly detection framework represents a significant advancement in IoT security, achieving 95.3 $\pm$ 1.2% detection accuracy through the innovative combination of supervised LightGBM algorithms with unsupervised autoencoder-based detection. The multi-dimensional feature analysis incorporating signal characteristics, temporal patterns, behavioral indicators, and contextual information establishes new benchmarks for real-time threat detection in resource-constrained environments. The lightweight implementation with only 59 KB memory footprint per device ensures compatibility with standard IoT hardware while maintaining exceptional detection performance across diverse attack scenarios.

The lightweight Zero Trust authentication system demonstrates that enterprise-grade security can be achieved in resource-constrained IoT environments through intelligent design and optimization. The energy-optimized Proof-of-Authority blockchain consensus achieves sub-200ms authentication latency (187 $\pm$ 23ms) while maintaining 99.95% system availability, representing a 56% energy reduction compared to traditional blockchain approaches. The dynamic trust scoring mechanism provides adaptive security assessment that evolves with device behavior patterns, enabling graduated access control and enhanced threat response capabilities.

The integrated security coordination mechanism enables real-time collaboration between anomaly detection and authentication systems, reducing false positives by 34% compared to independent operation while providing rapid coordinated response to security threats. Inter-module communication overhead remains minimal at 15$\pm$3ms average alert propagation time, ensuring that security enhancements improve rather than compromise network performance.

B. PRACTICAL IMPACT AND DEPLOYMENT VIABILITY

Comprehensive experimental validation through simulation projections validated by hardware measurements from a real-world testbed confirms the framework's practical effectiveness and deployment viability. The simulation model was parameterized using empirical data collected from a 3-node LoRaWAN hardware testbed deployed across university campus areas, with simulated performance evaluated under controlled conditions representing diverse deployment scenarios. The security overhead accounts for only 18.2% additional energy consumption, enabling 7.1 $\pm$ 0.6 years operational lifetime that meets the stringent requirements of battery-powered IoT applications. Statistical analysis with 95% confidence intervals demonstrates significant performance improvements across all security metrics ($p < 0.001$), establishing the framework's superiority over existing approaches.

The framework's compatibility with existing LoRaWAN infrastructure and backward compatibility features enable gradual deployment strategies that minimize disruption to

operational networks. Regulatory compliance with relevant security standards and data protection requirements facilitates adoption in regulated industries including healthcare, financial services, and critical infrastructure protection.

C. BROADER SCIENTIFIC AND INDUSTRIAL IMPACT

The research contributions extend beyond immediate LoRaWAN security improvements to establish fundamental principles for intelligent, adaptive security system design in resource-constrained environments. The demonstrated synergistic effects of coordinated security mechanisms provide important insights for broader cybersecurity research, while the energy-efficient implementation strategies offer valuable guidance for sustainable IoT system design.

The methodology validation establishes rigorous experimental protocols that can be adapted for evaluating future IoT security innovations, contributing to standardization of security framework assessment procedures. The open research approach enables broader community adoption and collaborative advancement of IoT security research while ensuring reproducible scientific progress.

Industrial impact assessment indicates significant potential for technology transfer to commercial IoT platforms, with the framework's practical deployment characteristics positioning it for rapid adoption in mission-critical applications where security and energy efficiency are paramount. The comprehensive security coverage and demonstrated effectiveness establish new standards for LoRaWAN security deployment in smart cities, industrial monitoring, and asset tracking applications.

The integrated approach successfully bridges the gap between theoretical security research and practical IoT deployment requirements, providing a foundation for the next generation of secure, intelligent IoT networks that can adapt to evolving threat landscapes while maintaining the operational efficiency essential for large-scale deployment success.

REFERENCES

[1] U. Cisco, "Cisco annual internet report (2018–2023) white paper," Cisco, San Jose, CA, USA, White Paper C11-741490-00, 2020, vol. 10, pp. 1–35.

[2] F. Ahmed, M. Phillips, S. Phillips, and K.-Y. Kim, "Comparative study of seamless asset location and tracking technologies," *Proc. Manuf.*, vol. 51, pp. 1138–1145, Jan. 2020.

[3] M. A. M. Almuhaya, W. A. Jabbar, N. Sulaiman, and S. Abdulmalek, "A survey on LoRaWAN technology: Recent trends, opportunities, simulation tools and future directions," *Electronics*, vol. 11, no. 1, p. 164, Jan. 2022.

[4] A. Sagala, R. Lubis, H. Sitanggang, R. Sinaga, and S. Hutapea, "Implementation LoRaWAN end node tracking," *Proc. IOP Conf. Ser., Earth Environ. Sci.*, vol. 1083, no. 1, 2022, Art. no. 012061.

[5] A. Povalac, J. Kral, H. Arthaber, O. Kolar, and M. Novak, "Exploring LoRaWAN traffic: In-depth analysis of IoT network communications," *Sensors*, vol. 23, no. 17, p. 7333, Aug. 2023.

[6] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in Internet-of-Things," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1250–1258, Oct. 2017.

[7] R. Sanchez-Iborra, J. Sanchez-Gomez, J. Ballesta-Viñas, M.-D. Cano, and A. F. Skarmeta, "Performance evaluation of LoRa considering scenario conditions," *Sensors*, vol. 18, no. 3, p. 772, Mar. 2018.

[8] Y. S. Chang, M. G. Son, and C. H. Oh, "Design and implementation of RFID based air-cargo monitoring system," *Adv. Eng. Informat.*, vol. 25, no. 1, pp. 41–52, Jan. 2011.

[9] L. Khalil, "LoRa-positioning in malmo compared with gps: Possibilities, power consumption & accuracy," B.S. thesis, Dept. Technol. Soc., Malmö Univ., Malmö, Sweden, 2018. [Online]. Available: https://www.diva-portal.org/smash/get/diva2:1480355/FULLTEXT01.pdf

[10] C. Hakkenberg, "Experimental evaluation of LoRa (WAN) in indoor and outdoor environments," M.S. thesis, Dept. EEMCS, Univ. Twente, Enschede, The Netherlands, 2016.

[11] I. Butun, P. Osterberg, and H. Song, "Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 616–644, 1st Quart., 2020.

[12] J. Sánchez-Gómez, J. Gallego-Madrid, R. Sanchez-Iborra, and A. Skármeta, "Performance study of LoRaWAN for smart-city applications," in *Proc. IEEE 2nd 5G World Forum (5GWF)*, Sep. 2019, pp. 58–62.

[13] A. Augustin, J. Yi, T. Clausen, and W. Townsley, "A study of LoRa: Long range & low power networks for the Internet of Things," *Sensors*, vol. 16, no. 9, p. 1466, Sep. 2016.

[14] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," White Paper, 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

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

[16] R. Sanchez-Iborra, M.-D. Cano, and J. Garcia-Haro, "Performance evaluation of LoRaWAN for smart city applications," *IEEE Access*, vol. 11, pp. 87534–87549, 2023.

[17] K. Yang, Q. Yu, S. Leng, B. Fan, and F. Wu, "Data-driven optimal throughput analysis for LoRaWAN with imperfect spreading factor orthogonality," *IEEE Internet Things J.*, vol. 11, no. 8, pp. 13402–13415, Apr. 2024.

[18] J. Kim, J. Song, and N. Park, "LoRaWAN security vulnerabilities and countermeasures: A comprehensive analysis," *IEEE Commun. Mag.*, vol. 61, no. 3, pp. 84–90, Mar. 2023.

[19] P. Rodriguez-Martinez, A. Fernandez-Carames, and T. M. Fraga-Lamas, "Advanced replay attack detection in LoRaWAN networks using machine learning," *IEEE Trans. Ind. Informat.*, vol. 20, no. 4, pp. 6234–6245, Apr. 2024.

[20] L. Chen, S. Wang, and Y. Zhang, "Application layer security challenges in LoRaWAN: A comprehensive taxonomy and analysis," *IEEE Trans. Dependable Secure Comput.*, vol. 21, no. 2, pp. 892–907, Mar. 2024.

[21] L. Liu, M. Niu, C. Zhang, and J. Shu, "Light gradient boosting machine-based link quality prediction for wireless sensor networks," *Wireless Commun. Mobile Comput.*, vol. 2022, no. 1, Jan. 2022, Art. no. 8278087.

[22] R. Patel, A. Kumar, and S. Gupta, "Ensemble machine learning for IoT anomaly detection: Performance analysis and optimization," *IEEE Trans. Netw. Service Manage.*, vol. 20, no. 2, pp. 1847–1862, Jun. 2023.

[23] H. Zhang, Y. Li, W. Chen, and R. Liu, "Multidimensional feature analysis for LoRaWAN anomaly detection using gradient boosting," *IEEE Internet Things J.*, vol. 11, no. 6, pp. 9876–9889, Mar. 2024.

[24] S. Kumar, M. Patel, and N. Singh, "Autoencoder-based anomaly detection for IoT networks: A comprehensive evaluation," *IEEE Trans. Mobile Comput.*, vol. 22, no. 8, pp. 4532–4547, Aug. 2023.

[25] D. Thompson, J. Wilson, and K. Brown, "Variational autoencoders for LoRaWAN anomaly detection: Reducing false positives in dynamic networks," *IEEE Trans. Wireless Commun.*, vol. 23, no. 3, pp. 2145–2158, Mar. 2024.

[26] X. Wang, Y. Liu, Z. Chen, and H. Zhao, "Federated learning for collaborative anomaly detection in LoRaWAN networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 35, no. 4, pp. 623–637, Apr. 2024.

[27] E. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero trust architecture," NIST special publication, Gaithersburg, MD, USA, Tech. Rep. NIST Special Publication (SP) 800-207, 2020.

[28] C. Martinez, R. Garcia, and A. Lopez, "Adapting zero trust principles for resource-constrained IoT environments: Challenges and solutions," *IEEE Secur. Privacy*, vol. 21, no. 4, pp. 45–53, Jul. 2023.

[29] S. Naik, R. Phadnis, N. Sharma, and M. Parmar, "Real time asset tracking using BLE beacons," in *Proc. Global Conf. Advancement Technol. (GCAT)*, Oct. 2019, pp. 1–4.

[30] A. Singh, P. Kumar, and R. Verma, "Energy-efficient proof-of-authority consensus for IoT authentication: Design and performance analysis," *IEEE Trans. Green Commun. Netw.*, vol. 8, no. 2, pp. 789–802, Jun. 2024.

[31] J. Lee, K. Park, and S. Kim, "Lightweight ECC-based mutual authentication for IoT devices: Implementation and security analysis," *IEEE Trans. Inf. Forensics Security*, vol. 19, pp. 3456–3469, 2024.
[32] R. Rodriguez, A. Martinez, and L. Garcia, "Post-quantum cryptography for IoT authentication: Lattice-based approaches," *IEEE Trans. Inf. Forensics Security*, vol. 19, pp. 2134–2147, 2024.
[33] M. Kumar, S. Patel, and R. Singh, "Integrated security framework for IoT networks: Design and evaluation," *IEEE Internet Things J.*, vol. 10, no. 12, pp. 10456–10469, Jun. 2023.
[34] J. Anderson, M. Williams, and K. Davis, "Three-layer security architecture for IoT networks: Performance and scalability analysis," *IEEE Trans. Netw. Service Manage.*, vol. 21, no. 1, pp. 234–247, Mar. 2024.

GHADA ABDELHADY is currently an Associate Professor with the Faculty of Engineering, MSA University, with 24 years of experience in teaching engineering and computer science courses, projects, and M.Sc. and Ph.D. supervision. She is also with the Center of Excellence, Faculty of Engineering, October University for Modern Sciences and Arts, Egypt. She is also the Manager of the Center of Excellence for Projects and Entrepreneurship, MSA University, and the Director of the Technology Transfer Office. Her research interests include artificial intelligence, machine learning, cryptography, cybersecurity, the IoT, and tracking systems. She is a Certified Reviewer of the Quality Assurance and Accreditation of Egyptian Higher Education and a member of several research organizations. She was awarded a fellowship from the Higher Education Academy and a PGCert in Education at the University of Greenwich, in 2018. Recently, she received the McKinsey Forward Program Badge from McKinsey and Company and the Mastery Award Badge from the IBM Skills Academy for the 2020 Artificial Intelligence Analyst Exam.

ABDULRAHMAN GHANDOURA (Member, IEEE) received the B.S. degree in electronics engineering from Johnson and Wales University, Providence, RI, USA, the M.S. degree in network engineering and management from DePaul University, Chicago, IL, USA, in 2013, and the Ph.D. degree in electrical and computer engineering from Southern Illinois University, Carbondale, IL, USA, in 2018. In 2019, he joined Umm Al-Qura University, Makkah, Saudi Arabia, where he is currently an Assistant Professor with the Department of Engineering and Science, Applied College. His research interests include network architecture and wireless sensor networks, 6G and beyond wireless communication technologies, and the Internet of Things and the Internet of Everything applications.

ABDELWAHED MOTWAKEL received the B.Sc. degree in computer science from Omdurman Islamic University, the M.Sc. degree in computer science from Institut Teknologi Sepuluh Nopember, Indonesia, and the Ph.D. degree in computer science from the Sudan University of Science and Technology. He is currently an Assistant Professor of computer science with Prince Sattam bin Abdulaziz University, Saudi Arabia. His research interests include fuzzy logic, neural networks, machine learning, deep learning, and data science. He is actively involved in teaching, student supervision, and scientific publishing in these fields. He has collaborated on multidisciplinary projects and participated in academic committees related to curriculum development and research evaluation.

ABDULLAH ALAJMI (Member, IEEE) received the B.S. degree in information system technology from Southern Illinois University, Carbondale, IL, USA, in 2010, the M.S. degree in information technology from DePaul University, Chicago, IL, USA, in 2014, and the Ph.D. degree from the School of Electronic Engineering and Computer Science, Queen Mary University of London, London, U.K., in 2023. His research interests include artificial intelligence for wireless systems, the Internet of Things, NOMA, and the Internet of Everything.