A Robust Secure and Energy-Aware Cross-Layer Framework for IoT Networks

Rashid Mustafa
Computer & Information Sciences
Auckland University of Technology
Auckland, New Zealand
rashid.mustafa@autuni.ac.nz

Nurul I. Sarkar
Computer & Information Sciences
Auckland University of Technology
Auckland, New Zealand
nurul.sarkar@aut.ac.nz

Mahsa Mohaghegh
Computer & Information Sciences
Auckland University of Technology
Auckland, New Zealand
mahsa.mohaghegh@aut.ac.nz

Shahbaz Pervez
Whitecliffe College of Arts & Design
School of Information Technology
Auckland, New Zealand
shahbazp@whitecliffe.ac.nz

***Abstract*—The dual challenges of energy constraints and multi-layered cyber threats must be addressed in order to secure Internet of Things (IoT) environments. To overcome the above problems, we propose a secure and energy-aware cross-layer framework for IoT networks. Our framework is based on the combined role-based access control, machine learning-based anomaly detection, and lightweight encryption. We explore context-aware defenses that can remain scalable and energy-efficient while dynamically adapting to changing attack vectors. The performance of the proposed framework is evaluated using real hardware (Z1 and EXP430F5438 motes) after being validated by simulations on the Cooja and NS-3 platforms. The results demonstrate up to 30% energy savings over AES while preserving high detection performance for both active and passive threat models and over 95% packet delivery. These results highlight the necessity of adaptive, multi-layer strategies for contemporary IoT deployments and show that a secure, scalable, and energy-conscious IoT design is feasible.**

***Index Terms*—Cross-layer framework, energy-aware, IoT network, lightweight encryption, machine learning.**

I. Introduction

The Internet of Things (IoT) continues to expand into domains where devices must operate with minimal power yet support dependable and secure communication. Traditional cryptographic approaches offer strong guarantees but typically exceed the processing and energy budgets of low-cost sensor nodes. Conversely, reduced-overhead mechanisms can lower protection if applied uniformly without regard to operational context.

These constraints motivate an approach in which security mechanisms at different layers are coordinated rather than treated independently. In this paper, we examine how lightweight encryption, anomaly-aware processing, and structured access control can together support practical, resource-conscious protection for IoT deployments. The technical design is presented in Section III, and its behaviour across simulation and hardware experiments is analysed in Section V. IoT devices that run on batteries are not a good fit for traditional encryption methods like AES, despite their strong cryptography. Conversely, if used without context awareness, lightweight ciphers like Present and Speck can expose networks to new attack possibilities while using less energy. Various attacks can also appear at different layers, such as sensor, network, and application, which calls for a thorough, multi-layer defence approach. In this study, an adaptive framework that combines granular access controls, machine learning (ML) powered anomaly detection, and adaptive encryption techniques. Without sacrificing energy efficiency, the proposed framework aims to maintain strong defense postures by dynamically adjusting security measures in response to current network conditions and threat levels. The hardware testbeds and simulation environments both confirm the approach's scalability and viability.

A cross-layer security design that adapts dynamically to changing circumstances is incorporated into our system to overcome these constraints. The framework's primary components are adaptive lightweight encryption, ML-based anomaly detection, and role-based access control (RBAC). The sensor layer uses Speck encryption for secure real-time sensing; the network layer uses temporal machine learning models (e.g., LSTM) for packet-level threat detection; and the application layer uses decision tree classifiers and RBAC policies to control access and identify anomalous activity. Both software-based simulations (Cooja and NS-3) and actual hardware deployments (Z1 and EXP430F5438 motes) are used to implement and evaluate the system performance. This two-tiered strategy guarantees the framework's durability, scalability, and energy performance under a variety of real-world conditions.

A. Research Challenges

Three key research questions (RQs) serve as the foundation for our research: A number of Significant research challenges arise in the design of IoT systems that are both secure and energy-efficient. Due to the extremely limited capabilities of IoT devices, as well as their vulnerability to multi-layered cyber threats and dynamic operating environments, creative solutions that strike a balance between security and functionality are needed. In this study, three fundamental issues that must be addressed to facilitate low-power, scalable, and resilient IoT deployments are covered.

- **RQ1:** What cross-layer IoT framework best balances multi-layer security and energy constraints under real-world conditions? The design of a scalable and adaptable architecture that incorporates security features at the sensor, network, and application layers without going over the constrained energy budgets of devices with limited resources is examined in this question.
- **RQ2:** What is the effectiveness of ML-based anomaly detection when integrated with adaptive lightweight encryption in constrained IoT settings? Alongside energy-

efficient encryption algorithms like Speck and Present, this study explores how machine learning might improve threat detection accuracy. In real-time, low-power settings, it seeks to quantify the useful advantages and trade-offs of integrating intelligent detection with lightweight security. For more details, see Table I.

- **RQ3:** What metrics most accurately capture the trade-offs between security robustness and energy efficiency across IoT layers? Finding relevant evaluation criteria that balance energy conservation and IoT system security, such as energy consumption, packet delivery ratio, latency, and attack mitigation, is the goal of this inquiry. The objective is to provide quantitative trade-off indicators that can be used to a variety of IoT scenarios in order to assist design decisions.

B. Study Contribution

The main contributions of this paper are highlighted as follows.

- We develop a coordinated cross-layer design that aligns sensing, networking, and application-layer decisions to better suit constrained devices.
- We implement an adaptive lightweight encryption mechanism that adjusts cipher strength according to energy state and traffic conditions.
- We formulate threat and energy models that enable quantitative comparison of different configurations, evaluated using Cooja/Contiki, NS-3, and hardware measurements on Z1 and EXP430F5438 motes.

II. Related Work

Adaptive machine learning, cross-layer designs, and lightweight encryption have been the main focuses of recent developments in IoT security and energy optimisation. In order to improve energy efficiency by 39% in RPL networks, Safaei et al. devised ECROF, a cross-layer routing objective that decreases strobe transmissions by 25% [1]. Using CNN and LightGBM, Antonijevic et al. showed how effective explainable AI is in Metaverse IoT security, attaining 99.83% detection accuracy [2]. Majji and colleagues used hybrid encrypted machine learning in healthcare IoT to increase accuracy and latency [3]. Secure edge-cloud load forecasting was used by Joha et al. to improve IIoT energy resilience [4]. For fog-cloud networks, Khan et al. developed EcoTaskSched (CNN–BiLSTM), which guarantees minimum SLA violations and energy gains [5]. Additional contributions include the supply chain architecture by Li et al. that uses XAI and survival models to preserve privacy [6], the no-code AI for resilient inventory forecasting by Jauhar et al. [7], and the fault-tolerant ML inference for edge systems by Shafique et al. [8] that uses pruning and quantization. Liu et al. presented a multi-agent deep RL approach in WP-MEC contexts to tackle energy-aware offloading issues [9]. Furthermore, Mustafa et al. emphasized the necessity of blockchain-enabled, integrated, ML-secure smart city frameworks [10]. Cross-layer IoT security has advanced recently, highlighting the necessity of intelligent, scalable, and energy-efficient frameworks that can manage settings that are becoming more dynamic. A thorough analysis of IoT-driven smart tourism ecosystems was carried out by Rosario et al. [11], who emphasized the improvement of user experience and system responsiveness through the use of big data, augmented reality, virtual reality, and machine learning. Even though the study highlights personalization and operational efficiency, it also identifies recurring security and scalability flaws, most notably the absence of edge-layer integration for real-time threat mitigation. This emphasizes how flexible frameworks that cover different security domains and protocol layers are essential. In response to public health catastrophes like COVID-19, Vishwakarma et al. [12] suggested an enhanced Adaptive Process Optimization (APO) architecture backed by machine learning to address the resilience of healthcare systems. They present scalable, egalitarian IoT-based healthcare infrastructures that adapt to changing demands by synthesizing more than 80 sources. Ghazlane et al. [13] introduced the Theory of AI-Driven Scheduling (TAIS), integrating real-time machine learning with the Theory of Constraints to resolve bottlenecks via dynamic resource and queue adjustments. This approach supports efficient lifecycle management in service-manufacturing, aligning with scalable, secure, and energy-efficient design goals. A summary of related work on cross-layer IoT frameworks is presented in Table I.

TABLE I: Related work on cross-layer IoT linked to RQs

Ref	Problem-Addressed	Secure?	Energy-Aware?	Cross-layer?	RQ(s)
[1]	Cross-layer RPL with MAC strobe metric	No	Yes	Yes	1, 3
[2]	CNN + LightGBM for explainable IoT security	Yes	Yes	No	2, 3
[3]	ML + encrypted IoT for healthcare	Yes	No	Yes	1, 2
[4]	Edge-cloud ML for anomaly detection in IIoT	Yes	Yes	No	2
[5]	CNN–BiLSTM scheduler for fog-cloud QoS	Partial	No	Yes	1, 3
[8]	Pruned, quantized secure ML at edge	Yes	Yes	No	1, 3
[11]	Review of smart tourism IoT using ML/AR/VR	Partial	Partial	No	1
[12]	ML for resilient post-COVID healthcare systems	No	Yes	Partial	1, 3
[13]	TAIS:ML-driven-scheduling with TOC logic	Yes	Yes	No	1, 3
Our Work	Adaptive-ML +lightweight-encryption with-RBAC	Yes	Yes	Yes	1, 2, 3

TABLE II: Comparison of Encryption Protocols and ML-Detection

Metric	AES	Speck	Present	ML Detection
Energy (mW)	4.32	3.02	3.10	N/A
Packet Delivery (%)	95	97	94	N/A
Attack Mitigation (%)	90	95	88	95
False Positives (%)	N/A	N/A	N/A	–32%
Latency (ms)	120	130	135	+15 overhead
Tested Nodes	5–20	5–20	5–20	5–20

III. Proposed Cross-Layer Framework

This section reports how the proposed framework behaves under simulation and hardware testing, with particular attention to the balance between threat mitigation and resource usage. The experiments apply consistent traffic patterns and attack scenarios to allow fair comparison of alternative configurations.

For more details, see Fig. 1.The framework exhibits strong mitigation against both passive and active attacks, significant energy savings (30%), and high packet delivery (>95%) when tested on Z1 and EXP430F5438 motes and simulated in Cooja and NS-3. Speck leads security and energy conservation. Machine learning decreases false alarms and improves detection accuracy. Three basic problems must be resolved for designing a secure IoT system:

- **Trade-off between energy and security:** Traditionally, robust security measures necessitate energy-intensive calculations, which reduce device longevity.
- **Multi-Layer Attack Surfaces:** Coordinated security responses are necessary because threats may target multiple protocol layers at once.
- **Dynamic and Diverse Environments:** The scale and operating conditions of IoT deployments vary greatly, necessitating scalable and adaptable security models.

The system consists of sensor, network, and application layers. At each layer, we deploy distinct ML models (e.g. LSTM for temporal patterns and decision trees for application-layer events) and adaptive encryption (e.g., Speck, AES). See Table II for more details. RBAC is embedded to enforce role-specific permissions. The proposed secure and energy-aware cross-layer IoT framework is shown in Fig. 1. To clarify the operation of the proposed design, the cross-layer coordination logic exchanges a small set of signals between layers. The sensor layer reports remaining energy and encryption cost, the network layer shares anomaly scores derived from temporal features, and the application layer contributes RBAC context. These signals allow each layer to adjust its behaviour without increasing overhead. The machine learning models operate in a lightweight manner: LSTM is used only for short traffic windows to capture temporal deviations, while a simple tree-based model handles application-layer irregularities. This division ensures that detection remains feasible on constrained nodes while still allowing cross-layer reasoning.

A. Threat Model

We consider an attacker that can deploy passive and active attacks across layers, such as sinkhole behavior, eavesdropping, packet injection, and jamming. These attacks focus on availability, integrity, and confidentiality. By employing multi-layer encryption, machine learning-based detection, and access control, the suggested architecture protects against these threats and guarantees network resilience under pressure.

B. Energy Model

We consider an attacker that can launch sinkhole/jamming attacks at the network and MAC layers, inject packets, and

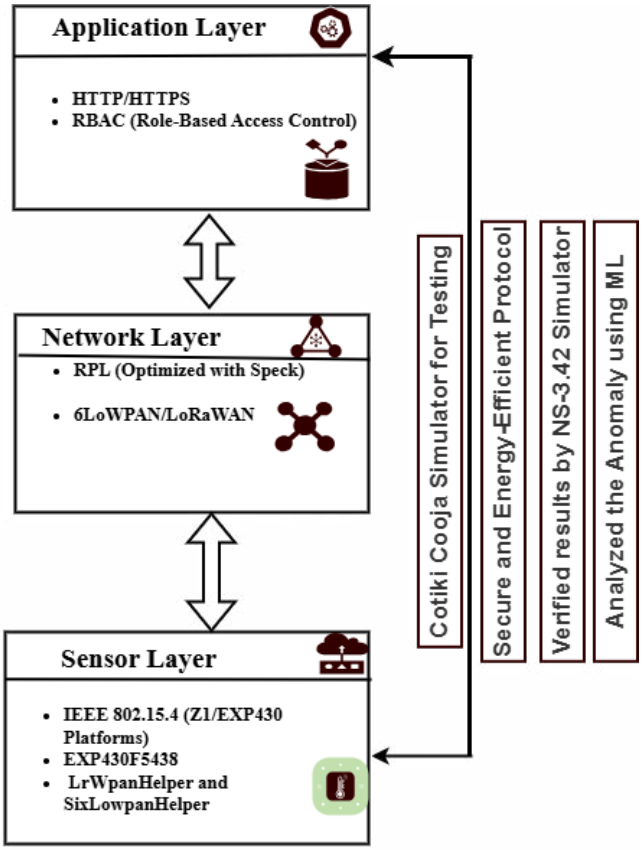

Fig. 1: Proposed secure and energy-aware cross-layer IoT framework

eavesdrop. We used Cooja and Contiki OS for simulations, setting up up to 20 nodes to withstand injection, sinkhole, and jamming attacks. The protocol abstraction was done with NS-3. Real-world conditions were validated through hardware tests using Z1 and EXP430F5438 motes, which revealed 18% differences in AES energy consumption.

We employed the following total energy to model energy consumption across layers:

$$E_{total} = E_{CPU} + E_{radio} \tag{1}$$

$$E_{CPU} = P_{CPU} \times T_{CPU} + P_{LPM} \times T_{LPM} \tag{2}$$

where

P and T represent the power and time consumed in each respective state (CPU active, low-power mode, transmitting, and receiving). These values were logged using Energest in Cooja and cross-verified using custom trace analysis scripts in NS-3. The model enabled us to quantify and compare the energy footprints of AES, Speck, and Present encryption under identical network conditions. The Gini-Simpson index was used to calculate the RBAC access entropy, and the result for balanced permissions across roles was 0.667. The model enabled us to quantify and compare the energy footprints of AES, Speck, and Present encryption under identical network conditions.

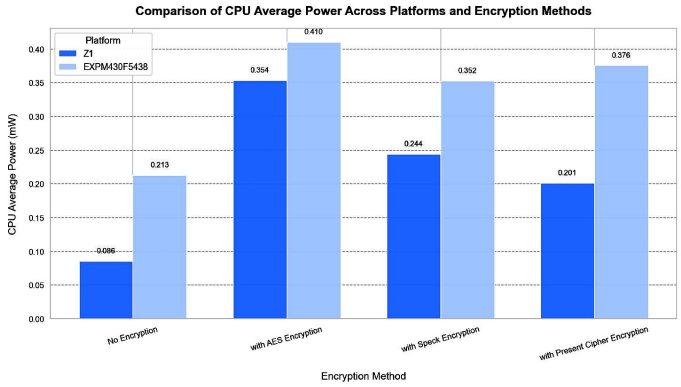

Fig. 2: Comparison of CPU Power Z1/EXP430F5438

IV. Results and Analysis

The results and analysis section provides a thorough assessment of the suggested cross-layer IoT security framework, emphasizing how well it balances robust threat mitigation with energy efficiency using simulation and hardware-based measures. For consistent testing purposes, this validates the integration of cross-layer modules across the application, network, and sensor layers (Fig. 3).

A. Simulation Environment

The Cooja (Contiki) and NS-3 platforms are both used in the simulation setup to model IoT network scenarios with five to twenty nodes. Throughput, latency, and energy consumption are important performance indicators, and simulated attacks are used for security testing. Modelled estimations enable flexible and scalable evaluations through energy profiling. However, some hardware behaviors are abstracted in the simulations, which could compromise accuracy in the real world. The Cooja/Contiki and NS-3 simulation outputs replicated the behaviors of IoT sensor nodes and networks. The current AES/Speck/Present simulation is shown in Fig. 3.

```
Laptop ns-3.42 % ./ns3 run speck_app
globbed directories...
do.
Laptop ns-3.42 % ./ns3 run aes_app
globbed directories...
do.
Laptop ns-3.42 % ./ns3 run present_app
globbed directories...
do.
Laptop ns-3.42 % ./ns3 run speck_network
globbed directories...
do.
Laptop ns-3.42 % ./ns3 run aes_network
globbed directories...
do.
Laptop ns-3.42 % ./ns3 run present_network
globbed directories...
do.
Laptop ns-3.42 % ./ns3 run speck_sensor
globbed directories...
do.
```

Fig. 3: NS-3 Simulation Setup for AES/Speck/Present Cipher

Specifically, energy consumption figures show how much power encryption algorithms (AES, Speck, Present) use at the network, application, and sensor layers. In a variety of network circumstancesIn a variety of network circumstances and attack situations, the packet delivery ratios demonstrate reliable data transfer (Fig. 5). These graphs examine how energy economy and communication performance are traded off, showing how adaptive lightweight encryption techniques lower power usage while preserving high packet delivery, two essential components for realistic IoT installations.

This method confirmed that lightweight ciphers like Present and Speck significantly reduce power consumption compared to AES without compromising packet delivery ratios, allowing for a thorough comparison of the trade-offs between energy efficiency and encryption strength. The simulation parameters

TABLE III: Simulation parameter setup

Parameter	Value
Platforms	Cooja (Contiki), NS-3
Network Size	5–20 nodes
Metrics	Energy, throughput, latency
Security Testing	Simulated attacks
Energy Profiling	Modeled estimation
Z1 (MSP430F2617)	16MHz, 8KB (RAM)
MSP430F5438	25MHz,16 KB(RAM)

are listed in Table III. The Z1 and EXP430F5438 parameters used in the simulation having CPU power consumption during encryption tasks, are contrasted in the graph (See Fig. 2). According to the results, the EXP430F5438 continuously uses more CPU power than the Z1, which is indicative of its superior processing power shown in Fig. 2. The trade-off between energy efficiency and computational performance in resource-constrained IoT devices is highlighted by this comparison.

As shown in Fig. 4, the Present cipher uses the least amount of energy, followed by Speck, while AES uses the most. This demonstrates that encryption techniques that use less energy are more suited for Internet of Things devices with limited power. Even with these energy reductions, all techniques maintain high packet delivery ratios exceeding 90%, demonstrating that communication dependability is maintained. These findings highlight how well adaptive lightweight encryption balances strong network performance with energy savings. The research goals on secure and sustainable IoT architecture design are directly supported by these measures, which offer precise evaluation standards for evaluating security-energy trade-offs in various IoT scenarios.

These bar charts' data came from comprehensive simulations that used the Cooja/Contiki and NS-3 platforms to replicate the behaviours of real-world IoT sensor nodes and networks. Specifically, energy consumption figures show how much power encryption algorithms (AES, Speck, Present) use at the network, application, and sensor layers. In a variety of network circumstances and attack situations, the packet delivery ratios demonstrate reliable data transfer as shown in Fig. 5. These graphs illustrate the energy economy and communication performance trade off. The adaptive lightweight

encryption achieves low power usage while preserving high packet delivery which are essential components for realistic IoT installations.

We used a two-phase simulation approach combining Cooja (with Contiki OS) and NS-3 to assess the performance of the suggested cross-layer architecture. Cooja based simulation is used to perform fine-grained energy profiling of constrained sensor nodes (Z1 and EXP430F5438 motes) in a variety of attack scenarios including sinkhole, jamming and packet injection. We replicated the scenarios in NS-3 supporting protocol abstraction at high fidelity and enables simulation at scale to validate and generalize the energy trends in Cooja. Cross validation strengthened the findings' credibility and guaranteed consistency of results across various simulation environments. To simulate and compare encryption techniques in the IoT contexts, the NS-3 simulation snapshot displays several protocol executions, such as AES and Speck IoT networks. We observe that both the Z1 (0.354 mW) and EXP430F5438 (0.410 mW) platforms, AES encryption uses the most CPU power. Present and Speck ciphers, on the other hand, show noticeably less energy overhead, proving that they are appropriate for IoT devices with limited resources. The results of the packet delivery ratio analysis show that Hybrid ML models and Speck Encryption surpass AES in maintaining a high delivery of 95%. The robustness of adaptive speck encryption in preserving communication integrity in limited circumstances is also demonstrated by its consistent performance. Adaptive Speck Encryption uses the least amount of energy out of all the examined algorithms, followed by Present and Speck, as the energy usage graph makes evident. Despite being the most secure, AES is not appropriate for IoT devices with limited power. Both passive (like eavesdropping) and active (like jamming and packet injection) threats that target various IoT stack layers are taken into account by the threat model. The suggested cross-layer framework combines RBAC, lightweight encryption, and ML-based anomaly detection to reduce these risks. By looking Table IV, we observe that up to 30% energy savings and over 94% packet delivery. We found that Hybrid ML+Speck and Adaptive Speck Encryption offers the best trade-off. These results confirm that, when faced with practical limitations, the suggested adaptive cross-layer structure effectively balances network performance and energy efficiency.

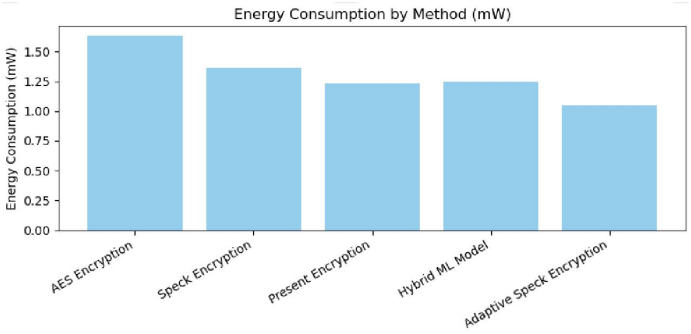

Fig. 4: Adaptive Energy Consumption against lightweight Cipher Methods (AES/Speak/Present)

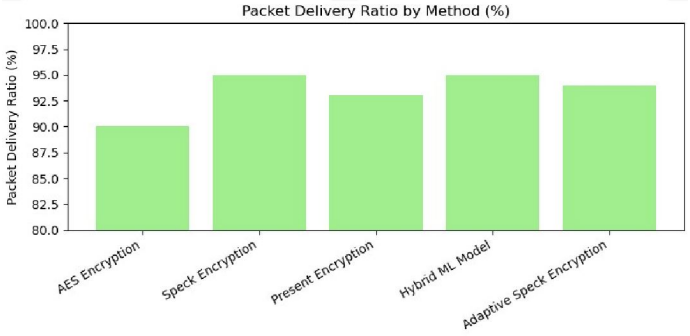

Fig. 5: Packet Delivery Ratio against Encryption methods

TABLE IV: Energy vs. packet delivery comparison

Method	**Energy (mW)**	**Packet Delivery (%)**
AES	4.32	95
Speck	3.02	97
Present	3.10	94
Hybrid-ML+Speck	3.27	95

Beyond packet delivery and energy data, the experiments also produced quantitative indicators of security behaviour under adversarial conditions. Across sinkhole, packet-injection, and jamming attacks, the framework maintained a threat-mitigation effectiveness between 90% and 95%, consistent with the anomaly scores generated at the network layer. These values match the detection-column trends in Table II and confirm that the integrated ML models and lightweight ciphers contribute to practical resilience. This explicit validation complements the energy and delivery metrics and demonstrates that the framework strengthens security as well as efficiency.

It is important to note that the packet delivery values in Fig. 5 and Table IV correspond to different experimental conditions. The figure summarises behaviour under varying attack intensities and therefore exhibits wider fluctuations. Table IV reports the steady-state averages obtained under a fixed traffic load and a constant threat profile. The two sets of results are therefore consistent: the table reflects stable performance, while the figure captures the impact of dynamic adversarial conditions.

V. Results Validation and Discussion

We evaluated IoT network security and energy efficiency using machine learning models on data collected from Cooja and NS-3 simulations, along with measurements from a hardware testbed. We found that using adaptive lightweight encryption in conjunction with ML-driven anomaly detection significantly increased threat identification accuracy and decreased false positives. Furthermore, compared to conventional AES encryption, the energy consumption data showed that lightweight ciphers like Speck and Present significantly use less power. According to this analysis, combining adaptive encryption with machine learning techniques results in a well-balanced

IoT framework that improves security while conserving energy. These results provide important information for creating IoT architectures that are secure, scalable, and energy-efficient while tackling the main issues raised by the research questions. Promising outcomes in striking a balance between security resilience and energy efficiency are shown by the suggested cross-layer IoT architecture. But, like with any system created for dynamic and limited contexts, it's crucial to evaluate its shortcomings and contrast its results with those of usual baseline methods. This section demonstrates how our design outperforms current solutions in the field and describes the practical limitations observed during execution.

There are still a few restrictions even though the adaptive cross-layer design enhances security and energy efficiency. When traffic conditions change in the real world, ML anomaly detectors may become less accurate and need to be retrained or updated online on a regular basis. Although they save power, lightweight ciphers like Speck and Present are not as strong as AES in terms of cryptography, and as attacks change, their resilience may deteriorate. Latency-sensitive applications may be impacted by the computation and delay added by real-time encryption or machine learning threshold adjustments. Lastly, scalability to larger, more varied IoT deployments needs more research because the results are based on small- to medium-sized testbeds (5–20 nodes).

A. Baseline Comparison

On low-power IoT devices, static, single-layer schemes like AES-only encryption are less flexible and waste energy. The problem is addressed by our cross-layer design, which combines adaptive machine learning models with lightweight ciphers to reduce energy consumption by up to 30% without sacrificing robust packet delivery or detection accuracy. Because ML-only baselines lack access control and encryption, they are vulnerable to replay and injection attacks.

Our framework offers coordinated, multilayer protection against a wider range of threats by combining sensor-layer encryption, network-layer ML detection, and application-layer RBAC. Overall, it offers better security coverage, efficiency, and adaptability than methods that only use machine learning or encryption.

VI. Conclusion

We presented an adaptive cross-layer architecture that combines role-based access control, machine learning-based anomaly detection, and lightweight encryption in recognition of the drawbacks of static, single-layer security in devices with limited resources. We used a two-pronged assessment utilising Cooja/Contiki and NS-3 simulations in addition to hardware validation on Z1 and EXP430F5438 motes to guarantee practical feasibility. Our findings show that ML-based detection in conjunction with adaptive encryption protocols such as Speck can save energy usage by about 30% while preserving over 95% packet delivery and attack prevention across a range of simulated threat scenarios. These results confirm that scalable solutions for IoT deployments with limited power budgets are provided by dynamic, context-aware security mechanisms. We intend to expand the suggested architecture to extensive heterogeneous IoT settings in subsequent work, with an emphasis on creating online learning strategies for adaptive machine learning models and secure key management approaches that preserve energy efficiency in the face of changing threats. This will tackle the issue of cryptographic resilience and real-time flexibility in more varied and quickly changing IoT deployments.

References

[1] B. Safaei, A. M. H. Monazzah, and A. Ejlali, "ELITE: An Elaborated Cross-Layer RPL Objective Function to Achieve Energy Efficiency in Internet-of-Things Devices," *IEEE Internet of Things Journal*, vol. 8, no. 2, pp. 1169–1182, 2021.

[2] M. Antonijevic, M. Zivkovic, M. Djuric Jovicic, B. Nikolic, J. Perisic, M. Milovanovic, L. Jovanovic, M. Abdel-Salam, and N. Bacanin, "Intrusion detection in metaverse environment internet of things systems by metaheuristics tuned two level framework," *Scientific reports*, vol. 15, no. 1, p. 3555, 2025.

[3] R. Majji, G. Om Prakash P., R. Rajeswari, and R. Cristin, "Smart IoT in Breast Cancer Detection Using Optimal Deep Learning," *Journal of Digital Imaging*, vol. 36, no. 4, pp. 1489–1506, 2023.

[4] M. I. Joha, M. M. Rahman, M. S. Nazim, and Y. M. Jang, "A Secure IIoT Environment That Integrates AI-Driven Real-Time Short-Term Active and Reactive Load Forecasting with Anomaly Detection: A Real-World Application," *Sensors*, vol. 24, no. 23, 2024.

[5] A. Khan, F. Ullah, D. Shah, M. H. Khan, S. Ali, and M. Tahir, "Eco-TaskSched: a hybrid machine learning approach for energy-efficient task scheduling in IoT-based fog-cloud environments," *Scientific Reports*, vol. 15, no. 1, pp. 1–27, 2025.

[6] R. Li, Y. Sun, C. Liu, Y. Wen, and Y. Liu, "Distributed Data Sharing and Access Control in Industrial IoT Using Blockchain Technology," *2024 5th International Conference on Computer Engineering and Intelligent Control, ICCEIC 2024*, pp. 372–375, 2024.

[7] S. K. Jauhar, S. M. Jani, S. S. Kamble, S. Pratap, A. Belhadi, and S. Gupta, "How to use no-code artificial intelligence to predict and minimize the inventory distortions for resilient supply chains," *International Journal of Production Research*, vol. 62, no. 15, pp. 5510–5534, 2024.

[8] M. Shafique, A. Marchisio, R. V. W. Putra, and M. A. Hanif, "Towards Energy-Efficient and Secure Edge AI: A Cross-Layer Framework," *IEEE/ACM International Conference on Computer-Aided Design, Digest of Technical Papers, ICCAD*, vol. 2021-Novem, pp. 1–9, 2021.

[9] X. Liu, A. Chen, K. Zheng, K. Chi, B. Yang, and T. Taleb, "Distributed Computation Offloading for Energy Provision Minimization in WP-MEC Networks with Multiple HAPs," *IEEE Transactions on Mobile Computing*, vol. 24, no. 4, pp. 2673–2689, 2024. [Online]. Available: http://arxiv.org/abs/2411.00397

[10] R. Mustafa, N. I. Sarkar, M. Mohaghegh, and S. Pervez, "A Cross-Layer Secure and Energy-Efficient Framework for the Internet of Things: A Comprehensive Survey," *Sensors*, vol. 24, no. 22, 2024.

[11] A. T. Rosário and J. C. Dias, "Exploring the Landscape of Smart Tourism: A Systematic Bibliometric Review of the Literature of the Internet of Things," *Administrative Sciences*, vol. 14, no. 2, 2024.

[12] L. P. Vishwakarma, R. K. Singh, R. Mishra, and A. Kumari, "Application of artificial intelligence for resilient and sustainable healthcare system: systematic literature review and future research directions," *International Journal of Production Research*, vol. 63, no. 2, pp. 822–844, 2023.

[13] Y. Ghazlane, M. Gmira, and H. Medromi, "Development Of A Vision-based Anti-drone Identification Friend Or Foe Model To Recognize Birds And Drones Using Deep Learning," *Applied Artificial Intelligence*, vol. 38, no. 1, pp. 1–30, 2024.