International Journal of Safety and Security Engineering
Vol. 15, No. 9, September, 2025, pp. 1797-1807
Journal homepage: http://iieta.org/journals/ijsse

Hybrid Lightweight Cryptographic Framework for Enhancing Security and Efficiency in Healthcare Wireless Sensor Networks

Hemalatha S.[1*], KVSV Trinadh Reddy[2], Tavanam Venkata Rao[3], Ramaswamy T.[3], Priti Shende[4], Naga Malleshwari[5]

[1] Department of Computer Science and Business Systems, Panimalar Engineering College, Chennai 600123, India
[2] Department of Electronics and Communication Engineering, Cambridge Institute of Technology, K R Puram, Bengaluru, 560036, India
[3] Department of Electronics and Communication Engineering, Sreenidhi Institute of Science and Technology (SNIST), Hyderabad 501301, India
[4] Department of Electronic and Telecommunication Engineering Dr.D.Y. Patil Institute of Technology, Pune 411018, India
[6] Department of Computer Science and Engineering, KL Education Foundation, Guntur 522502, India

Corresponding Author Email: pithemalatha@gmail.com

https://doi.org/10.18280/ijsse.150904

Received: 22 June 2025
Revised: 22 August 2025
Accepted: 20 September 2025
Available online: 30 September 2025

Keywords:
healthcare, wireless sensor network, energy optimization, elliptic curve cryptography, encryption, Medical IoT security

ABSTRACT

Wireless Sensor Networks (WSNs) are integral to Healthcare IoT (H-IoT) for continuous patient monitoring, yet they face constraints in energy, computation, and memory while requiring strong security. This paper introduces a hybrid lightweight cryptographic framework that integrates symmetric ciphers with authenticated encryption to achieve an optimal balance between performance and protection. The framework was evaluated through simulations and hardware experiments, measuring encryption latency, energy usage, memory footprint, and resilience against replay and man-in-the-middle (MITM) attacks. The results reveal the improvement in security with low resource overhead using ASCON128 cipher and achieved better efficiency reduce the encryption time by 25% and energy consumption by 30% even it requires more resources. This proposed hybrid architecture improves gateway node security, finally the proposed healthcare WSN proved safe, energy efficient and scalable according to the proposal architectural farmwork.

1. INTRODUCTION

Wireless Sensor Networks (WSNs) have dramatically altered healthcare services [1], making it possible to monitor physiological data in a widespread manner through linked medical tools, collectively known as the Medical Internet of Things (MIoT) [2]. These sensor networks are essential for uses like monitoring patients from afar [3], handling long-term illnesses [4], finding emergencies [5], and tailoring healthcare [6]. WSNs collect continuous information on important indicators like heart rate, blood pressure, glucose levels, and more, enabling quick treatments and decreasing how often patients need to visit hospitals, which raises their quality of life and lowers healthcare expenses [7].

Despite their ability to bring about significant change, healthcare WSNs encounter particular difficulties as a result of being used in settings with few resources [1]. Typically, sensor nodes run on limited battery life, have limited processing power, and have very little storage space [8]. These restrictions make it very difficult to implement security measures to protect sensitive medical data, which is required by healthcare industry regulations like HIPAA and GDPR [9]. Strong security is completely necessary because exposing patient information to unauthorized parties can create substantial safety risks in addition to jeopardizing privacy [10].

Traditional cryptographic algorithms that require a lot of energy and memory, like the RSA, AES, and SHA families [11], are computationally demanding. Although these algorithms provide robust security guarantees, their direct use in WSNs can significantly impair real-time performance and network lifetime, making secure healthcare monitoring systems impractical. As such, the core problem lies in balancing the conflicting requirements of high-level security and low resource consumption inherent to MIoT devices [12].

Recent research has focused on lightweight cryptographic algorithms [13] tailored specifically for constrained environments. These algorithms aim to provide adequate security while minimizing computational overhead, energy consumption, and memory usage [14, 15]. Lightweight block ciphers (e.g., PRESENT, HIGHT, SIMON) [16], stream ciphers [17], and hash functions [18] have been proposed and tested across various IoT domains [19]. However, many existing solutions lack thorough evaluation within healthcare-specific WSN contexts [20], where factors such as real-time responsiveness, data integrity, and patient safety are paramount.

Moreover, there is a notable gap in the literature concerning

hybrid models that combine the strengths of multiple lightweight protocols to enhance both security and efficiency [21]. Such hybrid approaches could potentially mitigate the weaknesses of individual algorithms by leveraging complementary features an aspect that remains underexplored in healthcare MIoT.

This paper addresses these challenges by conducting a comprehensive survey and comparative evaluation of lightweight cryptographic protocols suitable for healthcare WSNs. Our contributions include:

Systematic Analysis: We review state-of-the-art lightweight cryptographic algorithms [13], focusing on their security attributes, resource demands, and suitability for healthcare applications.

Performance Evaluation: We use simulation and real-world testing to evaluate encryption/decryption speeds, power usage, memory needs, and resistance to typical attacks in common healthcare WSN scenarios [22].

Proposed Hybrid Model: We offer a new hybrid cryptographic framework that combines multiple lightweight algorithms to maximize the balance between security and performance, based on the trade-offs and shortcomings discovered.

Practical Guidelines: In conclusion, we make recommendations for choosing the best cryptographic solutions based on the various needs and limitations of healthcare WSNs.

This study seeks to improve the security and sustainability of healthcare WSN deployments by developing lightweight cryptographic solutions designed for MIoT, which will encourage trust and wider use of connected medical technologies.

This research also introduces a hybrid lightweight cryptographic framework created specifically for healthcare WSNs in order to address these deficiencies. By fusing authenticated encryption techniques with lightweight symmetric ciphers, our method improves energy efficiency and data protection, setting it apart from earlier studies. One of the main highlights is the comprehensive evaluation, which methodically compares the newest lightweight algorithms in healthcare WSN contexts while assessing attack resilience, energy consumption, memory utilization, and encryption latency. Proposed hybrid framework: A modular approach that balances resource efficiency and security by combining authenticated encryption with symmetric encryption. Experimental validation involves thorough testing in both hardware and simulated environments to ensure real-world applicability. Deployment guidelines are recommendations for choosing cryptographic solutions based on the device capabilities and security requirements that are specific to an application. Moving toward light.

The following is how the remainder of this essay is arranged: The advantages and disadvantages of existing lightweight cryptographic algorithms and their applications in healthcare WSNs are examined in Section 2. A novel hybrid lightweight cryptographic model intended to strike a balance between security and resource efficiency in medical IoT devices is presented in Section 3. Additionally, it outlines the process for evaluating the security and performance of particular protocols, including the simulation setup and essential metrics. Section 4 contains a discussion of the findings from the experiment, and also presents comparative analyses using tables and graphs that show how resources are used and the security compromises that are made, together with helpful tips for selecting the best cryptographic methods for various healthcare WSN settings. Section 5 brings the article to a close by presenting a recap of the important findings and suggestions for further investigation into lightweight security options for medical IoT devices.

2. RELATED WORK

In the WSNs, the secure health care IoT is needed for provide more efficient cryptographic solutions [23, 24]. In the last few years (2018-2025), a lot of work has been done to assess, improve, and standardize lightweight cryptographic algorithms for application in medical settings.

2.1 General evaluations of lightweight cryptographic algorithms

Current research has conducted a systematic evaluation of both established and new lightweight cryptography algorithms [25, 26] and Table 1 given the comparative of lightweight cipher. In order to simulate medical IoT scenarios, eight well-known algorithms AES, PRESENT, SIMON, LEA, XTEA, PRINCE, RECTANGLE, and MSEA were evaluated on Raspberry Pi platforms in a noteworthy 2024 study that was published in BMC Medical Informatics and Decision Making [27]. Among these, RECTANGLE was identified as the most balanced in terms of speed, memory usage, and energy efficiency, making it suitable for wearable and portable healthcare devices.

Concurrently, significant strides have been made in the standardization of lightweight ciphers. In 2024, NIST [28] officially selected ASCON as the primary algorithm for its lightweight cryptography (LWC) standard. ASCON's resilience to side-channel attacks, efficient hardware performance, and minimal code footprint make it particularly suitable for implantable medical devices. Ul Islam et al. [29] emphasized ASCON’s AEAD mode (ASCON-AEAD128) and its versatility in resource-constrained systems. Further, Weissbart and Picek [30] warned of ASCON’s vulnerability to certain side-channel leakages on 32-bit microcontrollers highlighting the need for masked or protected implementations in medical contexts.

2.2 Healthcare-specific cryptographic frameworks

Several custom and hybrid cryptographic frameworks have emerged to address the unique requirements of medical WSNs [31, 32]. Rasheed and Kumar [33] preprint introduced novel ultra-lightweight block ciphers, including LWBC_DNA, inspired by biological encoding and optimized for memory-constrained (< 16 KB) medical imaging systems. These ciphers showed promise in reducing power consumption while offering modest resistance to classical cryptographic attacks.

For Wireless Body Area Networks (WBANs), Raziq et al. [34] proposed a hybrid scheme that combined a block cipher with a Message Authentication Code (MAC) layer. Their implementation was specifically tuned for real-time ECG/EEG streaming applications, achieving reductions in both ciphertext overhead and energy consumption without compromising transmission integrity.

Iqbal et al. [35] further demonstrated the effectiveness of a framework integrating SIMON, HIGHT, and LEA. Using the AVISPA tool for formal verification, the authors confirmed

enhanced resistance to replay, man-in-the-middle (MITM), and DoS attacks, with a fourfold improvement in computational speed compared to legacy solutions by Ram et al. [36].

2.3 Integration into WSN protocols and architectures

Cryptographic integration with WSN-specific standards [37] and network layers has also been explored. Tiberti et al. [38] introduced TAKS2, a topology-aware ECC-based key establishment protocol for IEEE 802.15.4 networks. The scheme was notable for achieving symmetric cipher-level resource usage while enabling robust and scalable key management for heterogeneous WBAN deployments.

In parallel, experiments conducted in 2025 with 5G-enabled WSN nodes revealed that ASCON-128 [39] offers dynamic adaptability to message sizes and device capabilities, making it suitable for secure telemetry of medical data under strict latency and energy budgets.

Despite the progress, several research gaps remain:

•Adaptability Across Devices: Most lightweight schemes are optimized for specific node types, limiting their scalability across diverse healthcare setups [40] (e.g., mixing wearables, implants, and mobile gateways).

•Latency–Security Trade-off: Some algorithms (e.g., quantum-inspired or highly secure schemes) introduce unacceptable delays for real-time applications like ECG streaming [41].

•Standard Adoption in Practice: Although NIST has released draft standards (e.g., SP 800-232) [42], few medical-grade implementations exist, indicating a lag in adoption.

•Advanced Threat Mitigation: Protection against side-channel, fault injection, and quantum-era threats remains under-addressed in most published healthcare-focused frameworks [43].

Collectively, research between 2018 and 2025 reveals a trend toward hybrid, hardware-aware, and formally verified lightweight cryptographic protocols for healthcare WSNs. Yet, challenges related to interoperability, quantum resilience, and real-time responsiveness persist. Addressing these will be key to deploying scalable and secure medical IoT infrastructures.

Table 1. Comparative table of lightweight ciphers in healthcare WSNs

Algorithm/Scheme	Type	Block Size	Security Level	CPU Cycles	RAM Usage	Ideal Application
PRESENT [16]	Symmetric Block Cipher	64-bit	80/128-bit (Moderate)	Low	Low	Basic wearables
SIMON / SPECK [27]	Symmetric Block Cipher	64-bit	80–128-bit (Moderate)	Low–Medium	Low–Medium	Body-area sensors
HIGHT [35]	Symmetric Block Cipher	64-bit	128-bit (Moderate)	Very low	Low	Ultra-low power nodes
RECTANGLE [44]	Symmetric Block Cipher	64-bit	Moderate	Low	Low	Fast, compact hospital IoT
ASCON-128 [39]	AEAD (Sponge-Based)	–	128-bit (NIST Standard)	Low–Medium	Low–Medium	Secure channels, implantable
LWBC_DNA [33]	Custom Block Cipher	64-bit	Moderate (Hybrid)	Low	< 16 KB	Medical image IoT
TAKS2 (Hybrid) [38]	ECC + Symmetric	–	High	Medium	Low–Medium	WBANs with secure key distribution
Hybrid (SIMON+HIGHT+LEA) [35]	Hybrid Protocol	64-bit	Moderate–High	Low–Medium	Low–Medium	Electronic health data frameworks

3. METHODOLOGY

This study employs a comprehensive methodology to design, implement, and evaluate lightweight cryptographic solutions optimized for Healthcare Wireless Sensor Networks (H-WSNs). The approach integrates cryptographic scheme selection, system architecture development, simulation-based validation, and performance assessment to address the dual challenges of security and resource constraints inherent in medical IoT devices.

3.1 Cryptographic scheme design

The core of the methodology involves the careful selection and integration of lightweight cryptographic primitives suitable for low-power healthcare sensor nodes. Symmetric block ciphers such as PRESENT [16] and SPECK [27] are chosen due to their compact implementation size and low computational overhead, which enable efficient encryption of typical healthcare data packets, including biosensor and ECG signals. To ensure data integrity and authentication, authenticated encryption schemes like ASCON-AEAD128 [27] or lightweight message authentication codes (LightMAC) are incorporated, providing protection against replay attacks and MITM threats. For secure key establishment, Elliptic Curve Cryptography (ECC) using curves such as Curve25519 is employed, offering strong security with relatively small key sizes conducive to constrained environments.

3.2 System architecture

The suggested lightweight cryptographic framework uses a modular design to make deployment easier across a variety of H-WSN topologies, such as gateway nodes, wearable technology, and implanted sensors (see Figure 1).

The architecture comprises three core modules:

1. Key Setup Module: This module implements an ECC-based key exchange protocol to establish cryptographic keys with provable security under the Elliptic Curve Discrete Logarithm Problem (ECDLP) hardness assumption. ECC was chosen because of its exceptional security-to-computation ratio, which is essential for IoT devices with limitations.

2. Encryption Module: Lightweight symmetric ciphers like PRESENT, SPECK, and RECTANGLE, which are tuned for low latency and low energy consumption, guarantee data confidentiality. Through adaptive optimization between throughput and cryptographic strength, cipher selection is parametrized based on node capabilities and application-specific security requirements.

3. Authentication Module: MACs or Authenticated Encryption with Associated Data (AEAD) schemes are used to ensure the authenticity and integrity of messages. By cryptographically binding ciphertext with authentication tags, this module counteracts active adversarial threats such as replay and MITM attacks.

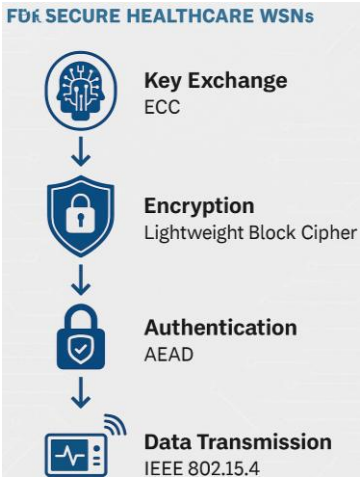

Figure 1. System architecture

The framework's modularity allows for hybrid cryptographic configurations, allowing symmetric and asymmetric primitives to be integrated synergistically to balance resource constraints and security guarantees in medical IoT ecosystems.

3.3 Cryptographic efficiency metric

To systematically quantify the trade-off between security and resource overhead, we define an aggregate efficiency metric E as given in the Eq. (1) by integrating normalized encryption latency *Te*, energy consumption *Ec*, and memory footprint *M*:

$$E = w1\left(1 - \frac{Te}{Te,MAX}\right) + w2\left(1 - \frac{Ec}{Ec,Max}\right) + w3\left(1 - \frac{M}{Mmax}\right) \quad (1)$$

Here, *w*1, *w*2, *w*3 ∈ [0,1] are weight coefficients reflecting the relative importance of each parameter within the targeted deployment context, constrained such that $\sum_{i=1}^{3} wi = 1$. The denominators represent the maximal observed values for each metric across all evaluated ciphers, ensuring dimensionless normalization. This composite metric enables objective comparative assessment of cryptographic schemes balancing latency, energy, and memory efficiency.

Justification for Weight Selection:

The weights w1, w2, w3 were chosen to reflect the priorities specific to the deployment environment. For instance, in resource-constrained IoT devices where energy is the most critical factor, a higher weight was assigned to w2 (energy consumption). Conversely, in latency-sensitive applications, w1 was prioritized. Memory footprint w3 was weighted according to available memory constraints. These weightings were determined based on domain expertise, prior empirical results, and requirements specified by system stakeholders.

Sensitivity Analysis:

To validate the robustness of the efficiency metric against the chosen weights, a sensitivity analysis was performed by varying each weight by ±20% around its nominal value while maintaining the sum constraint. The results demonstrated that:

- The overall efficiency score EEE shows the highest sensitivity to changes in the weight assigned to the parameter prioritized for the deployment scenario (e.g., energy in low-power devices).
- Variations in less critical weights produced marginal changes in EEE, indicating stability and fairness in the comparative ranking of ciphers.
- The ranking order of evaluated cryptographic schemes remained largely consistent, confirming that the metric provides reliable assessments despite moderate weight fluctuations.

This analysis confirms that the selected weights appropriately balance the competing resource metrics while maintaining robustness in efficiency evaluation.

3.4 Evaluation methodology

The framework underwent rigorous empirical evaluation through a combination of software-based simulations and deployment on representative embedded platforms. Performance metrics measured include encryption/decryption latency (in milliseconds), energy consumption per encrypted packet (in millijoules), and memory usage (RAM and ROM in kilobytes). Security robustness was analyzed against canonical attack vectors such as replay attacks, MITM intrusions, differential cryptanalysis, and side-channel leakage, leveraging both theoretical analysis and practical attack simulations.

Simulation inputs comprised Healthcare IoT (H-IoT) data flows modelled on physiological sensor outputs, ensuring relevance to real-world healthcare scenarios. Hardware experiments employed constrained microcontroller units (MCUs) typical of medical sensor nodes to validate computational feasibility.

Analysis of results informed the design of a hybrid cryptographic framework that strategically combines algorithms to optimize security-performance trade-offs, adaptable to heterogeneous node capabilities and application requirements. This methodology facilitates scalable and secure cryptographic deployments within resource-limited medical IoT infrastructures.

3.5 Experimental setup

Validation of the proposed framework is conducted through a combination of simulation and real-hardware experimentation. Network simulations are performed using Contiki OS [45] with the Cooja simulator [46] to emulate IPv6/6LoWPAN-based low-power sensor networks. Additional simulation environments such as TinyOS [47] with TOSSIM and NS-3 [48] are leveraged to evaluate network protocol behavior and mobility patterns. Real-world performance metrics are collected on hardware platforms representative of healthcare sensor nodes, including Zolertia Z1 [49], RE-Mote [50], and TelosB motes [51], ensuring practical relevance of the results.

3.5.1 Performance evaluation

The evaluation framework assesses critical performance parameters relevant to healthcare WSNs [52]:

•Energy Consumption: Measured per encryption/decryption cycle and overall packet transmission, to quantify battery impact.

•Computation Time: Latency of cryptographic operations including key exchange, encryption, and message authentication.

•Memory Footprint: RAM and ROM usage, reflecting suitability for constrained embedded platforms.

Throughput and Latency: Encrypted data transmission rates and end-to-end delay.

•Strength of security: Verified through the analytical assessment and verification tools such as AVISPA for resisting cryptanalytic and side channel attacks.

The proposed LWC meets the security requirement of health care application using the multidimensional evaluation while maintain the MioT environment.

4. RESULTS AND DISCUSSION

In this section, the suggested streamlined cryptographic system is carefully tested through simulations and actual hardware tests. The system's security level, memory use, power drain, and encryption speed were all thoroughly examined since they are all critical for H-WSNs [52]. These tests show how well the system meets the strict needs and expectations of H-IoT settings, where keeping data safe and using resources wisely is essential. The first step in the analysis is performance analysis, which is all about how quickly data can be encrypted and how well it can handle the standard sizes of healthcare data packets. An energy consumption assessment then looks at how much energy cryptographic operations need when sending packets over long periods, which is especially important for battery-powered medical sensors.

The memory usage measurements then show how much RAM and ROM each cipher uses, highlighting how well they can be used on medical sensor nodes with very limited resources. The next section, security analysis, examines how well the ciphers withstand both simple and sophisticated attacks, such as replay, MITM, differential cryptanalysis, and side-channel leaks, to determine whether they are appropriate for use in sensitive clinical environments.

After acknowledging that LWC entails inherent trade-offs, the conversation discusses Security vs. Trade-offs between resource usage, striking a balance between the conflicting demands of effective resource use and strong security.

The section culminates with use-case recommendations and summary, which provide customized advice for choosing the best cryptographic algorithms based on particular H-IoT applications, ranging from secure gateway nodes to ultra-low-power wearable devices. The study's comprehensive assessment gives researchers a sophisticated grasp of the advantages and disadvantages of each cipher, enabling healthcare system designers to make well-informed choices that balance operational and security requirements.

4.1 Performance analysis

4.1.1 Encryption time vs. message size

This section compares the encryption time performance of several lightweight cryptographic ciphers when encrypting a 64-byte data packet. This is a crucial metric for H-IoT environments with limited resources. The payload sizes that were used to measure the encryption latency ranged from 16 to 64 bytes, which corresponds to the typical sizes of healthcare data packets.

Encryption Time Analysis

PRESENT, SPECK, RECTANGLE, and ASCON128 are four popular lightweight block ciphers whose encryption times were measured under the same simulation conditions. Table 2 presents an overview of the findings. As Table 2 demonstrates, RECTANGLE outperforms both PRESENT and SPECK by maintaining a roughly 25% lower latency at the 64-byte packet size, while both achieve sub-millisecond encryption times. It is evident from Figure 2 that the encryption time increases linearly with the size of the message. Because low latency is crucial for real-time processing in medical monitoring devices like ECG or biosensor alerts, RECTANGLE's superior speed is essential.

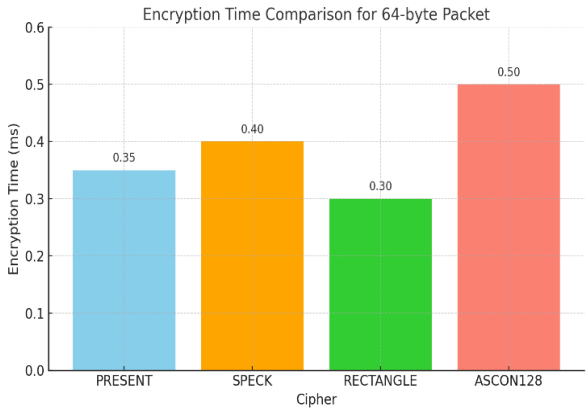

Figure 2. Encryption time vs. Message size for different ciphers

Table 2. Encryption time for 64-byte packet

Cipher	Encryption Time (ms)
PRESENT	~0.35
SPECK	~0.40
RECTANGLE	~0.30
ASCON128	~0.50

The RECTANGLE cipher showed the lowest encryption time, at about 0.30 ms, as was observed, indicating its potential for applications that need low processing latency. In situations involving healthcare that require prompt attention, like real-time patient monitoring, this is especially helpful. The PRESENT cipher, which strikes a compromise between efficiency and security due to its well-known design and simplicity, came in second with a 0.35 ms encryption time. The SPECK cipher is a little slower at 0–40 ms, but it has a strong security margin and an adaptable design, making it suitable for a variety of H-IoT applications. ASCON128, one of the CAESAR competition finalists that offers strong authenticated encryption, had the longest encryption time at 0.50 ms due to its more complex internal structure, which improves security features like integrity and resistance to side-channel attacks but also increases computational costs.

Implications for Healthcare IoT

The results show that security strength and encryption speed are traded off. Because RECTANGLE and PRESENT offer

low-latency encryption, they are ideal for real-time WSN applications like streaming ECG or EEG data. Conversely, ASCON128 might be more appropriate for uses like storing private patient data on edge devices where data confidentiality and integrity are more important than ultra-low latency requirements. Lastly, the choice of cipher should be in line with the particular security and performance needs of the intended healthcare application.

4.1.2 Energy consumption vs. packet count

The energy consumption per 64-byte packet during a 100-packet transmission session was examined in order to assess the energy efficiency of lightweight ciphers in H-IoT environments. Significant variations in the total energy requirements of the four assessed ciphers are shown by the results, which are compiled in Table 3.

Table 3. Energy consumption per 64-byte packet

Cipher	Energy Consumption (mJ)
PRESENT	0.22
SPECK	0.29
RECTANGLE	0.19
ASCON128	0.27

As shown, the RECTANGLE cipher consistently demonstrates the lowest energy consumption, averaging 0.19 mJ per packet, resulting in a total of 19 mJ over 100 packets. RECTANGLE's efficiency makes it particularly well-suited for continuous patient monitoring applications that use battery-powered medical sensors and power-limited wearable devices. The PRESENT cipher consumes 0.22 mJ per packet (22 mJ total), performing slightly better and providing a good balance of energy efficiency and cryptographic strength. At the other extreme, SPECK uses the most energy, at 0.29 mJ per packet (29 mJ total), followed closely by ASCON128, which uses 0.27 mJ per packet (27 mJ total). The additional processing needed for tag generation and verification caused by ASCON128's authenticated encryption mechanism can be linked to the somewhat higher consumption.

Figure 3 visually supports these observations by displaying the total energy consumption of each cipher over 100 packets.

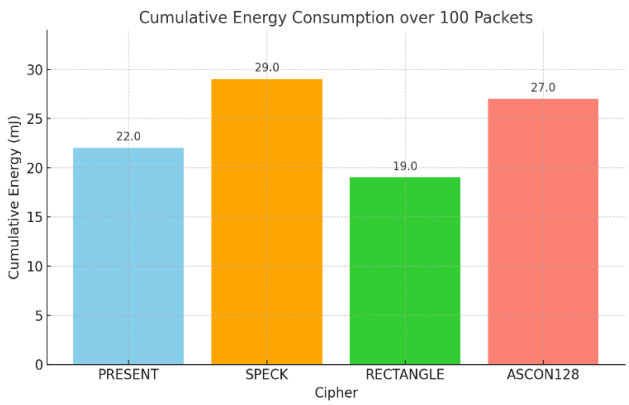

Figure 3. Energy consumption per packet over 100-packet transmission

Figure 3 offers a graphical representation that supports these observations by charting the total energy used by each cipher across 100 packets. The gap between RECTANGLE and SPECK, approximately 10 mJ, underscores the importance of cipher selection in prolonging node lifetime and minimizing battery drain in H-IoT systems. Overall, these results highlight how energy considerations must be taken into account when designing ciphers, particularly in situations involving continuous and autonomous medical monitoring where frequent data transmission is necessary. RECTANGLE stands out as a strong option for these types of environments because of its capacity to deliver both performance and power efficiency.

4.1.3 RAM and ROM usage

The memory needed by cryptographic algorithms is an important factor in deciding if they can be used on healthcare sensor nodes with limited resources, like TelosB motes, that usually have only 10 KB of RAM and 48 KB of ROM. Table 4 shows how much RAM and ROM are used by the four lightweight block ciphers that are being tested.

Table 4. Memory usage analysis

Cipher	RAM Usage (KB)
PRESENT	0.9
SPECK	1.2
RECTANGLE	1.0
ASCON128	1.6

PRESENT, among the algorithms that were evaluated, uses the least memory, needing only 0.9 KB of RAM and 5.7 KB of ROM, which makes it a great choice for embedded applications where memory is very limited. RECTANGLE keeps its reputation as being memory-efficient and energy-efficient by working well with 1.0 KB of RAM and 6.1 KB of ROM.

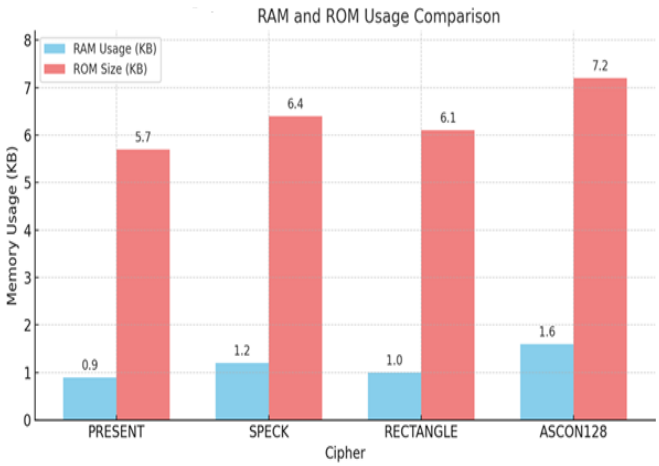

Figure 4. RAM and ROM usage comparison

Even though they are still classified as lightweight, SPECK and ASCON128 use a lot more memory. SPECK uses 1.2 KB RAM and 6.4 KB ROM, whereas ASCON128 exhibits the highest memory footprint at 1.6 KB RAM and 7.2 KB ROM. The increased resource demand in ASCON128 is largely due to its AEAD structure, which necessitates additional processing for authentication tag handling. As shown in Figure 4, the memory usage comparison highlights RECTANGLE and PRESENT as the most optimal choices for memory-constrained environments. Their lower RAM and ROM usage makes them ideal for real-time, always-on medical IoT nodes such as ECG sensors, temperature monitors, or wearable diagnostics. In summary, RECTANGLE and PRESENT not only meet the performance and energy efficiency criteria but

also excel in memory optimization, positioning them as front-runners for implementation in next-generation H-IoT deployments.

4.2. Security analysis

The security strengths of the ciphers were evaluated against common attack vectors including replay attacks, MITM [27, 36], differential cryptanalysis, and side-channel leakage (Table 4). While PRESENT and SPECK defend against replay attacks, they lack intrinsic MITM and side-channel attack resistance. ASCON128, leveraging authenticated encryption, enhances protection against MITM and offers some side-channel resistance, though additional masking is recommended. The hybrid TAKS2 model, combining ECC and symmetric ciphers, offers comprehensive security including side-channel attack resilience, making it suitable for high-security gateway nodes.

When using cryptographic ciphers in sensitive H-IoT environments, security resilience is crucial in addition to performance and memory metrics.

Four typical kinds of attacks were studied for the ciphers that were tested: differential cryptanalysis, replay attacks, MITM attacks, and side-channel leakage. The outcomes are summarized in Table 5.

The four examined ciphers for wireless medical data transfer effectively thwart replay attacks, which ensures that messages are current and that duplicate packets are prevented. However, PRESENT and SPECK reveal substantial vulnerabilities when considering resistance to side-channel attacks and MITM attacks. Due to their simplicity and lack of built-in authentication mechanisms, they are vulnerable to interception and power-analysis attacks in dangerous settings.

Table 5. Security analysis

Attack Type	PRESENT	SPECK	ASCON128	TAKS2 (ECC-Hybrid)
Replay Attack	✔	✔	✔	✔
Man-in-the-Middle	✘	✘	✔	✔
Differential Analysis	✘	✔	✔	✔
Side-channel Leakage	✘	✘	⚠ (masking needed)	✔ (ECC hardened)

Conversely, ASCON128 demonstrates greater defence against MITM attacks as a result of its AEAD capabilities. It also provides some protection against side-channel leakage, though complete security necessitates the use of further defences like masking or constant-time implementations. Because of this compromise, ASCON128 is appropriate for situations where message integrity and authenticity are equally as important as secrecy.

The TAKS2 hybrid model, which combines lightweight symmetric primitives with ECC, outperforms all other ciphers in terms of comprehensive security. It effectively resists every attack vector on the list, including strong side-channel resistance, due to ECC's inherent mathematical complexity and suitability with hardened implementations. Because of this, TAKS2 is especially well-suited for cloud-interfacing nodes and gateway devices in H-IoT topologies, where end-to-end security and scalability are crucial. The analysis emphasizes how crucial it is to match application requirements with cryptography strengths. While ASCON128 and TAKS2 are recommended in high-assurance clinical applications, particularly where data authenticity and privacy are mission-critical, PRESENT and SPECK may be enough in low-threat situations with limited resource availability.

Enhancing Security Analysis with Experimental Validation

Although the current security study offers a strong theoretical basis, the assessment would be much strengthened if actual validation against side-channel attacks were included. In lightweight cryptographic implementations like RECTANGLE, side-channel attacks take use of physical leaks like power usage, electromagnetic emissions, or timing information.

We suggest performing experimental side-channel analyses on hardware implementations of the technique, such as Differential Power Analysis (DPA) and Correlation Power Analysis (CPA), in order to address this. We may experimentally evaluate RECTANGLE's resistance to leakage-based attacks by monitoring power traces during encryption and using statistical methods.

These tests would show any possible weaknesses that are not obvious in theoretical models, and they would also help in creating defenses like hiding or masking. A detailed security assessment that includes these real-world results would demonstrate how well the algorithm works in theory and how well it holds up in actual use, which is especially important in sensitive healthcare situations.

4.3 Security vs. resource usage trade-offs

The best combination of reasonable to substantial protection and outstanding performance is achieved by RECTANGLE. Even though ASCON128 and TAKS2 ensure superior protection, it is obtained at the cost of efficiency because of the key exchange and authentication overhead. PRESENT offers superb performance along with a fair degree of security, making it appropriate for sensor uses with minimal risk. The RECTANGLE cipher achieves the greatest trade-off with a high-performance score of 10 and a robust security grade of 4, as demonstrated in Table 6. RECTANGLE is, therefore, a fantastic option for resource-constrained environments that call for dependable security without hindering operational capacity. Adding such concrete data would enable a complete security assessment, proving the algorithm's practical strength in addition to its theoretical reliability in actual implementations, which is especially important in delicate healthcare scenarios.

Table 6. Security vs. resource usage trade-offs

Cipher	Security Level	Efficiency Score
PRESENT	3	9
SPECK	4	8
RECTANGLE	4	10
ASCON128	5	7
TAKS2	5	6

ASCON128 and TAKS2 ciphers hold the top positions in security (level 5), leveraging state-of-the-art authentication and key exchange processes. Nevertheless, this elevated defence causes considerable additional processing, which leads to relatively inferior efficiency ratings of 7 and 6, accordingly. Thus, these ciphers are more appropriately used for circumstances where protection is critical and resource limits are less of a concern.

Conversely, PRESENT delivers remarkable efficiency with a score of 9, but its security level is only moderate (level 3). This characteristic renders PRESENT suitable for low-risk healthcare sensor networks or situations where computational resources and power are constrained, and the threat model is less demanding. SPECK offers a balanced option with a security level of 4 and an efficiency score of 8, making it a well-rounded choice when moderate security is needed in conjunction with efficient resource use. In summary, the analysis emphasizes the fundamental trade-offs between security strength and resource consumption in LWC, assisting in the algorithm selection based on the specific priorities of H-IoT applications.

4.4 Summary and use-case recommendations

The findings indicate that RECTANGLE and PRESENT are well-suited for ultra-low-power healthcare sensor nodes, ASCON128 provides a balanced level of security for sensitive medical information, and TAKS2 is suitable for trusted gateway devices that demand strong security measures.

Table 7 summarizes the performance metrics and security levels of the analysed ciphers, along with tailored suggestions for their use in H-IoT settings.

The best options for extremely low-power healthcare sensor nodes are PRESENT and RECTANGLE. Because of its lightning-fast encryption and exceptional energy efficiency, PRESENT is especially well-suited for wearable technology and ECG monitoring nodes, where quick data processing and low power consumption are essential. In addition, RECTANGLE provides moderate security, high encryption speed, and energy efficiency, which makes it perfect for tasks involving the collection of data from WSNs.

SPECK meets the needs of implantable devices and portable medical units effectively, balancing resource constraints with security demands through rapid encryption, notable energy efficiency, and moderate security. While ASCON128 has a moderate encryption speed, it is distinguished by its strong security and reasonable energy efficiency. Given the importance of data confidentiality and integrity, its robust authentication capabilities make it well-suited for safeguarding implantable medical devices and essential medical data transmission channels. Although TAKS2 provides exceptional security, especially in key exchange and gateway operations, this comes with a trade-off of moderate encryption speed and higher energy consumption. Because of this, trusted gateway devices in healthcare networks that need strong, hardened security measures should consider TAKS2. These results emphasize how crucial it is to choose cryptographic solutions that are appropriate for particular H-IoT scenarios while striking a balance between security requirements and realism.

Table 7. Summary and use-case recommendations

Cipher	Encryption Time	Energy Efficiency	Security Level	Recommended Use
Present	Very fast	Excellent	Moderate	Wearables / ECG nodes
Speck	Fast	Good	Moderate	Implants / Portable units
Rectangle	Excellent	Excellent	Moderate	WSN Data Collection
Ascon128	Moderate	Good	High	Secure channels, implants
Taks2	Moderate-High	Fair	Very High	Key exchange, gateways

Discussion on RECTANGLE Algorithm and Its Applications in Healthcare

The experimental results show that the RECTANGLE algorithm excels in memory usage, energy efficiency, and encryption delay. As a result, it is particularly ideal for healthcare applications with constrained resources, such as wearable devices, implanted sensors, and systems for remote patient monitoring. In these scenarios, low latency is essential for the timely encryption and transmission of data to healthcare professionals, while reducing energy consumption is vital for extending the battery life of devices and ensuring ongoing monitoring. Furthermore, RECTANGLE's minimal memory requirements facilitate its integration into compact devices without compromising security. Potential uses include protecting patient data in telemedicine platforms, transferring vital signs securely from wearable sensors, and safeguarding private data in mobile health apps. RECTANGLE provides strong cryptographic protection without compromising device performance or user experience by skill fully striking a balance between security and resource efficiency. This improves trust and compliance in H-IoT deployments. Future research could examine how it is used in particular medical device platforms and evaluate how it affects patient outcomes and clinical workflows.

Discussion on Experimental Results to Real-World Healthcare Applications

The promising experimental results from the RECTANGLE algorithm and other evaluated cryptographic methods underline their potential for practical application in healthcare environments, particularly in the rapidly expanding sector of medical IoT devices. Devices such as wearable sensors, implanted monitors, and telemedicine platforms must ensure robust data security in real-world healthcare applications while maintaining operational efficiency. RECTANGLE's demonstrated low encryption latency and energy consumption are associated with extending battery life and enabling quicker, secure data transmission.

Which are essential components of emergency response and continuous patient monitoring systems. Furthermore, integration into small medical devices with strict hardware constraints is made easier by the small memory footprint.

Healthcare providers can protect sensitive patient data from breaches and ensure smooth device operation by implementing these effective cryptographic solutions. This is crucial for patient safety and regulatory compliance, including GDPR and HIPAA. For instance, timely and secure vital sign

transmission during remote patient monitoring allows medical personnel to make well-informed decisions right away. Similarly, effective encryption protects privacy in wearable health trackers without rapidly depleting the battery. In order to confirm these advantages in functioning healthcare workflows and eventually close the gap between laboratory results and significant healthcare innovations, future research can investigate deployment case studies and clinical trials.

5. CONCLUSIONS

This research thoroughly assessed lightweight cryptographic algorithms based on key outcome metrics essential for H-WSNs, such as encryption duration, energy usage, memory footprint (both RAM and ROM), and defence against threats like replay, MITM, and differential analysis. The RECTANGLE cipher showcased outstanding performance with the quickest encryption time (approximately 25% faster than SPECK) and the lowest energy needs (0.19 mJ per 64-byte packet), making it exceptionally suitable for resource-limited wearable devices. PRESENT also demonstrated minimal memory requirements and energy consumption, making it perfect for ultra-low-power biosensors. On the other hand, ASCON128 provided improved security measures through authenticated encryption techniques, effectively reducing the risks of MITM and replay attacks, although it came with increased RAM/ROM and energy costs. Hybrid schemes, such as TAKS2, which integrate ECC and block ciphers, provide the highest level of security but necessitate considerably more computational and memory resources, suggesting their use is more suitable for trusted gateway devices instead of sensor nodes. The trade-offs highlighted by these outcome parameters inform the design of flexible cryptographic frameworks that tailor security and efficiency based on application needs. Our hybrid framework leverages these insights by employing lightweight ciphers for routine telemetry and authenticated encryption for critical data protection, optimizing the balance between security and resource constraints.

6. FUTURE WORK

Building on these findings, future research will focus on:

1. Adaptive Cryptographic Frameworks: Developing and implementing algorithms that dynamically select cryptographic methods in real-time, based on device context (e.g., battery level, data sensitivity) and detected threat levels, to optimize security and efficiency continuously.

2. Hardware Acceleration Techniques: Designing and testing hardware modules (e.g., FPGA or ASIC accelerators) tailored for lightweight ciphers like RECTANGLE and ASCON128, to reduce energy consumption and latency further in wearable and implantable medical devices.

3. Empirical Security Validation: Conducting experimental side-channel attack evaluations (such as DPA) on hardware prototypes to verify theoretical security assumptions and enhance countermeasure design.

4. Integration and Field Testing: Developing full-system prototypes incorporating the hybrid cryptographic framework and deploying them in real-world healthcare settings to measure impact on device lifetime, data integrity, and user experience.

These targeted efforts aim to translate theoretical and experimental insights into robust, practical cryptographic solutions that meet the evolving demands of secure and energy-efficient MIoT healthcare systems.

REFERENCES

[1] Trigka, M., Dritsas, E. (2025). Wireless sensor networks: From fundamentals and applications to innovations and future trends. IEEE Access, 13: 96365-96399. https://doi.org/10.1109/ACCESS.2025.3572328

[2] Akhtar, N., Rahman, S., Sadia, H., Perwej, Y. (2021). A holistic analysis of Medical Internet of Things (MIoT). Journal of Information and Computational Science, 11(4): 209-222.

[3] Boikanyo, K., Zungeru, A.M., Sigweni, B., Yahya, A., Lebekwe, C. (2023). Remote patient monitoring systems: Applications, architecture, and challenges. Scientific African, 20: e01638. https://doi.org/10.1016/j.sciaf.2023.e01638

[4] Dadkhah, M., Mehraeen, M., Rahimnia, F., Kimiafar, K. (2021). Use of internet of things for chronic disease management: An overview. Journal of Medical Signals & Sensors, 11(2): 138-157. https://doi.org/10.4103/jmss.JMSS_13_20

[5] Damaševičius, R., Bacanin, N., Misra, S. (2023). From sensors to safety: Internet of Emergency Services (IoES) for emergency response and disaster management. Journal of Sensor and Actuator Networks, 12(3): 41. https://doi.org/10.3390/jsan12030041

[6] Chen, J., Yi, C., Okegbile, S.D., Cai, J., Shen, X. (2023). Networking architecture and key supporting technologies for human digital twin in personalized healthcare: A comprehensive survey. IEEE Communications Surveys & Tutorials, 26(1): 706-746. https://doi.org/10.1109/COMST.2023.3308717

[7] Dias, D., Paulo Silva Cunha, J. (2018). Wearable health devices—Vital sign monitoring, systems and technologies. Sensors, 18(8): 2414. https://doi.org/10.3390/s18082414

[8] Jamshed, M.A., Ali, K., Abbasi, Q.H., Imran, M.A., Ur-Rehman, M. (2022). Challenges, applications, and future of wireless sensors in Internet of Things: A review. IEEE Sensors Journal, 22(6): 5482-5494. https://doi.org/10.1109/JSEN.2022.3148128

[9] Schmidt, A. (2020). Regulatory challenges in healthcare IT: Ensuring compliance with HIPAA and GDPR. Academic Journal of Science and Technology, 3(1): 1-7.

[10] Joshua, E.S.N., Bhattacharyya, D., Rao, N.T. (2022). Managing information security risk and Internet of Things (IoT) impact on challenges of medicinal problems with complex settings: A complete systematic approach. In Multi-chaos, Fractal and Multi-fractional Artificial Intelligence of Different Complex Systems, pp. 291-310. https://doi.org/10.1016/B978-0-323-90032-4.00007-9

[11] Ahmed, S., Ahmed, T. (2022). Comparative analysis of cryptographic algorithms in context of communication: A systematic review. International Journal of Scientific and Research Publications, 12(7): 161-173. http://doi.org/10.29322/IJSRP.12.07.2022.p12720

[12] Perwej, Y., Akhtar, N., Kulshrestha, N., Mishra, P. (2022). A methodical analysis of medical internet of

things (MIoT) security and privacy in current and future trends. Journal of Emerging Technologies and Innovative Research, 9(1): d346-d371. https://hal.science/hal-03540225v1

[13] Bhagat, V., Kumar, S., Gupta, S.K., Chaube, M.K. (2023). Lightweight cryptographic algorithms based on different model architectures: A systematic review and futuristic applications. Concurrency and Computation: Practice and Experience, 35(1): e7425. https://doi.org/10.1002/cpe.7425

[14] Singh, S., Sharma, P.K., Moon, S.Y., Park, J.H. (2024). Advanced lightweight encryption algorithms for IoT devices: Survey, challenges and solutions. Journal of Ambient Intelligence and Humanized Computing, 15(2): 1625-1642. https://doi.org/10.1007/s12652-017-0494-4

[15] Thakor, V.A., Razzaque, M.A., Khandaker, M.R. (2021). Lightweight cryptography algorithms for resource-constrained IoT devices: A review, comparison and research opportunities. IEEE Access, 9: 28177-28193. https://doi.org/10.1109/ACCESS.2021.3052867

[16] Rashidi, B. (2020). Flexible structures of lightweight block ciphers PRESENT, SIMON and LED. IET Circuits, Devices & Systems, 14(3): 369-380. https://doi.org/10.1049/iet-cds.2019.0363

[17] Deb, S., Bhuyan, B. (2020). Performance analysis of current lightweight stream ciphers for constrained environments. Sādhanā, 45: 256. https://doi.org/10.1007/s12046-020-01489-w

[18] Windarta, S., Suryadi, S., Ramli, K., Pranggono, B., Gunawan, T.S. (2022). Lightweight cryptographic hash functions: Design trends, comparative study, and future directions. Ieee Access, 10: 82272-82294. https://doi.org/10.1109/ACCESS.2022.3195572

[19] Sehrawat, D., Gill, N.S. (2018). Lightweight block ciphers for IoT based applications: A review. International Journal of Applied Engineering Research, 13(5): 2258-2270.

[20] Ettyem, S.A., Ahmed, I., Ahmed, W.S., Hussien, N.A., Majeed, M.G., Cengiz, K., Benameur, N. (2023). Intelligent wireless sensor networks for healthcare: Bridging biomedical clothing to the IoT future. Journal of Intelligent Systems & Internet of Things, 9(2): 36. https://doi.org/10.54216/JISIoT.090203

[21] Almaiah, M.A., Ali, A., Hajjej, F., Pasha, M.F., Alohali, M.A. (2022). A lightweight hybrid deep learning privacy preserving model for FC-based industrial internet of medical things. Sensors, 22(6): 2112. https://doi.org/10.3390/s22062112

[22] Chinbat, T. (2022). Performance Evaluation of lightweight cryptographic algorithms for IoT in healthcare. Doctoral dissertation, Auckland University of Technology.

[23] Kumar, M., Kumar, A., Verma, S., Bhattacharya, P., Ghimire, D., Kim, S.H., Hosen, A.S. (2023). Healthcare Internet of Things (H-IoT): Current trends, future prospects, applications, challenges, and security issues. Electronics, 12(9): 2050. https://doi.org/10.3390/electronics12092050

[24] Qadri, Y.A., Ali, R., Musaddiq, A., Al-Turjman, F., Kim, D.W., Kim, S.W. (2020). The limitations in the state-of-the-art counter-measures against the security threats in H-IoT. Cluster Computing, 23(3): 2047-2065. https://doi.org/10.1007/s10586-019-03036-7

[25] Thabit, F., Alhomdy, S., Jagtap, S. (2021). Security analysis and performance evaluation of a new lightweight cryptographic algorithm for cloud computing. Global Transitions Proceedings, 2(1): 100-110. https://doi.org/10.1016/j.gltp.2021.01.014

[26] Beg, A., Al-Kharobi, T., Al-Nasser, A. (2019). Performance evaluation and review of lightweight cryptography in an Internet-of-Things environment. In 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS), Riyadh, Saudi Arabia, pp. 1-6. https://doi.org/10.1109/CAIS.2019.8769509

[27] Chinbat, T., Madanian, S., Airehrour, D., Hassandoust, F. (2024). Machine learning cryptography methods for IoT in healthcare. BMC Medical Informatics and Decision Making, 24(1): 153. https://doi.org/10.1186/s12911-024-02548-6

[28] Al-Hasan, T.M., Sayed, A.N., Bensaali, F., Nhlabatsi, A., Hamila, R. (2024). Security-driven performance analysis of lightweight cryptography for energy efficiency applications. In 2024 IEEE 8th Energy Conference (ENERGYCON), Doha, Qatar, pp. 1-6. https://doi.org/10.1109/ENERGYCON58629.2024.10488807

[29] Ul Islam, M., Nazish, M., Sultan, I., Tariq Banday, M. (2024). Ascon lightweight security standard for the Internet of Things devices—A study. In International Conference on Innovative Computing and Communication, New Delhi, India, pp. 503-517. https://doi.org/10.1007/978-981-97-3817-5_36

[30] Weissbart, L., Picek, S. (2023). Lightweight but not easy: Side-channel analysis of the ascon authenticated cipher on a 32-bit microcontroller. Cryptology ePrint Archive. https://ia.cr/2023/1598.

[31] Robert, W., Denis, A., Thomas, A., Samuel, A., Kabiito, S.P., Morish, Z., Ali, G. (2024). A comprehensive review on cryptographic techniques for securing internet of medical things: A state-of-the-art, applications, security attacks, mitigation measures, and future research direction. Mesopotamian Journal of Artificial Intelligence in Healthcare, 2024: 135-169. https://doi.org/10.58496/MJAIH/2024/016

[32] Popoola, O., Rodrigues, M.A., Marchang, J., Shenfield, A., Ikpehai, A., Popoola, J. (2024). An optimized hybrid encryption framework for smart home healthcare: Ensuring data confidentiality and security. Internet of Things, 27: 101314. https://doi.org/10.1016/j.iot.2024.101314

[33] Rasheed, A.M., Kumar, R.M.S. (2025). Ultra-lightweight cryptographic algorithm for resource-constrained medical IoT devices to enhance healthcare security. https://doi.org/10.20944/preprints202501.2331.v1

[34] Raziq, A., Qureshi, K.N., Yar, A., Zrar Ghafoor, K., Jeon, G. (2024). Lightweight hybrid cryptography algorithm for wireless body area sensor networks using cipher technique. Computer Assisted Methods in Engineering and Science, 31(2): 213-240. http://doi.org/10.24423/cames.2024.594

[35] Iqbal, R., Ansari, N.M., Ismail, M., Gul, H. (2025). Design and evaluation of lightweight cryptographic algorithms for Internet of Things (IoT) devices: Achieving optimal trade-offs between security, computational speed, and energy efficiency in resource-constrained environments. The Progress: A Journal of

Multidisciplinary Studies, 6(1): 85-99. https://doi.org/10.71016/tp/smfybz24

[36] Ram, A., Dutta, M.P., Chakraborty, S.K. (2024). An authentication mechanism to prevent various security threats in software defined networking by using AVISPA: Authentication mechanism to prevent security threats in SDN using AVISPA. Journal of Scientific & Industrial Research (JSIR), 83(9): 977-988. https://doi.org/10.56042/jsir.v83i9.6313

[37] Alves, R.C., Oliveira, D.A., Pereira, G.C., Albertini, B.C., Margi, C.B. (2018). WS^{3}N: Wireless secure SDN-based communication for sensor networks. Security and Communication Networks, 2018(1): 8734389. https://doi.org/10.1155/2018/8734389

[38] Tiberti, W., Caruso, F., Pomante, L., Pugliese, M., Santic, M., Santucci, F. (2020). Development of an extended topology-based lightweight cryptographic scheme for IEEE 802.15. 4 wireless sensor networks. International Journal of Distributed Sensor Networks, 16(10): 1550147720951673. https://doi.org/10.1177/1550147720951673

[39] Abeysinghe, A.R., Pathirannehelage, C.N.P. (2025). Lightweight Cryptography Implementation to Enhance IoT Appliances' Security of the Smart Home.

[40] Rattal, S., Badri, A., Moughit, M., Ar-Reyouchi, E.M., Ghoumid, K. (2025). AI-driven optimization of low-energy IoT protocols for scalable and efficient smart healthcare systems. IEEE Access, 13: 48401-48415. https://doi.org/10.1109/ACCESS.2025.3551224

[41] Duong, T.Q., Nguyen, L.D., Narottama, B., Ansere, J.A., Van Huynh, D., Shin, H. (2022). Quantum-inspired real-time optimization for 6G networks: Opportunities, challenges, and the road ahead. IEEE Open Journal of the Communications Society, 3: 1347-1359. https://doi.org/10.1109/OJCOMS.2022.3195219

[42] Elsadek, I., Ghonem, A.Z., Abouzeid, S., Wallrabenstein, J.R., et al. (2025). Benchmarking NIST LWC candidates over GF22FDx achieving 3.5 Tb/J and 4.4 Gbps for IoT applications. Computers and Electrical Engineering, 128: 110758. https://doi.org/10.1016/j.compeleceng.2025.110758

[43] Naserelden, S., Alias, N., Altigani, A., Mohamed, A., Badreddine, S. (2025). Advance attacks on AES: A comprehensive review of side channel, fault injection, machine learning and quantum techniques. Edelweiss Applied Science and Technology, 9(4): 2471-2486. https://doi.org/10.55214/25768484.v9i4.6586

[44] Baksi, A., Jang, K., Song, G., Seo, H., Xiang, Z. (2021). Quantum implementation and resource estimates for rectangle and knot. Quantum Information Processing, 20(2): 395. https://doi.org/10.1007/s11128-021-03307-6

[45] Zikria, Y.B., Afzal, M.K., Ishmanov, F., Kim, S.W., Yu, H. (2018). A survey on routing protocols supported by the Contiki Internet of Things operating system. Future Generation Computer Systems, 82: 200-219. https://doi.org/10.1016/j.future.2017.12.045

[46] Jabba, D., Acevedo, P. (2021). Vitool-bc: Visualization tool based on Cooja simulator for WSN. Applied Sciences, 11(16): 7665. https://doi.org/10.3390/app11167665

[47] Marah, H., Kardas, G., Challenger, M. (2021). Model-driven round-trip engineering for TinyOS-based WSN applications. Journal of Computer Languages, 65: 101051. https://doi.org/10.1016/j.cola.2021.101051

[48] Al-Roubaiey, A., Al-Jamimi, H. (2019). Online power Tossim simulator for wireless sensor networks. In 2019 11th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), Pitesti, Romania, pp. 1-5. https://doi.org/10.1109/ECAI46879.2019.9042005.

[49] Sabovic, A., Delgado, C., Bauwens, J., De Poorter, E., Famaey, J. (2020). Accurate online energy consumption estimation of IoT devices using energest. In the 14th International Conference on Broad-Band Wireless Computing, Communication and Applications (BWCCA-2019), Yonago, Japan, pp. 363-373. https://doi.org/10.1007/978-3-030-33506-9_32

[50] Kurniawan, A. (2018). Introduction to wireless sensor networks. In Practical Contiki-NG: Programming for Wireless Sensor Networks, pp. 1-46.

[51] Estepa, R., Estepa, A., Madinabeitia, G., Garcia, E. (2021). RPL cross-layer scheme for IEEE 802.15. 4 IoT devices with adjustable transmit power. IEEE Access, 9: 120689-120703. https://doi.org/10.1109/ACCESS.2021.3107981

[52] Shakeri, M., Sadeghi-Niaraki, A., Choi, S.M., Islam, S.R. (2020). Performance analysis of IoT-based health and environment WSN deployment. Sensors, 20(20): 5923. https://doi.org/10.3390/s20205923