SSRG International Journal of Electronics and Communication Engineering
ISSN: 2348-8549/ https://doi.org/10.14445/23488549/IJECE-V13I3P124

Volume 13 Issue 3, 301-311, March 2026
© 2026 Seventh Sense Research Group®

Original Article

Securing Beyond-5G Communications in Cloud Assisted IoT Ecosystems via Lightweight Encryption Techniques

S. Almelu[1], Prabhakar K[2], Sunitha T[3], Durga Devi A[4]

[1]*Department of CSE , Velammal Engineering College, Chennai, Tamilnadu, India.*
[2]*Department of CSE(AI&ML), SOET, CMR University, Bangalore, India.*
[3]*Department of AI&DS, Saveetha Engineering College, Chennai, Tamilnadu, India.*
[4]*Department of ECE, Saveetha Engineering College, Chennai, Tamilnadu, India.*

[1]*Corresponding Author : almelugcr@gmail.com*

Received: 17 December 2025 Revised: 20 January 2026 Accepted: 25 February 2026 Published: 23 March 2026

Abstract *- Faster speeds of Beyond-5G (B5G) communication technologies have allowed connectivity in Internet of Things (IoT) ecosystems on an unprecedented scale, although this progression has also increased existing security vulnerabilities by making most IoT devices resource-constrained. The main issue is to balance strong security with the low computing, memory, and power capabilities of IoT endpoints that cannot be effectively supported by conventional encryption algorithms such as RSA or AES. To deal with this, the suggested approach, Lightweight Encryption in Beyond-5G IoT Security (LEBIS), proposes specialized cryptographic algorithms that are optimized in low-resource settings, focusing on small code size, power usage, and resistance to side-channel and quantum attacks. LEBIS incorporates post-quantum cryptographic algorithms like lattice-based and hash-based schemes with lightweight key management protocols, which guarantee the safety of communication without damaging the working of the devices. The results of the experiment have proven that LEBIS can establish a high level of data confidentiality and integrity, and in the process, the data encryption is enhanced, and real-time Internet of Things can be supported by up to 80% higher efficiency at practical throughputs. It concludes with the statement that LEBIS is capable of ensuring B5G-enabled Cloud Assisted IoT Ecosystems because it can converge lightweight cryptographic rigor with the harsh resource limitations of the IoT devices, and hence is a promising approach to ensure security in IoT systems in future smart pervasive environments. It is therefore a work that adds a scalable and adaptable method that is vital in the progression of trust to next-generation IoT networks.*

***Keywords* -** *Beyond-5G, Internet of Things, lightweight encryption, post-quantum cryptography, resource-constrained devices, IoT security.*

1. Introduction

Wireless technology has reached one of the greatest heights with the introduction of the B5G communication technologies [1]. The latter essentially changed the telecommunication scene with their extremely low time delays, colossal amounts of information handled, and strong and multipurpose connectors [2]. Another notable consequence of the paradigm shift related to such technologies is the Internet of Things, or IoT. It currently supports the most modern smart ecosystems, such as smart cities, smart transport, smart healthcare, and smart industrial automation [3]. It is predicted that by 2030, B5G networks will have flawlessly incorporated billions of IoT devices, therefore, generating an untapped volume of data and making intelligent, highly responsive services omnipresent and available [4]. The accelerated technology proliferation has its negative aspects, though, especially in the limited resource context of an IoT environment, where even the simplest communication is very delicate and should be preserved [5].

The use of RSA, ECC, AES, and other dominant cryptographic techniques for network security is not new. Such techniques do guarantee privacy, authenticity, and integrity [6]. The IoT ecosystem contains a large number of small, resource-constrained sensors, actuators, and embedded systems. The limited processing capability, memory, and energy requirements of such systems, however, are why many devices do not use such systems [7]. The inability of these systems to defend themselves while there is a well-established security architecture is a paradox. Eavesdropping, man-in-the-middle, denial of service, and other complex attacks [8] are examples of such attacks. As more devices become connected to B5G, the need for robust and reliable security solutions has become increasingly critical [9].

Researchers have been trying harder and harder to create ways to encrypt data that are both quick and light, without trading off security [10]. These algorithms are great for IoT setups because they do not utilize a lot of memory, power, or processing power [11]. As quantum computing becomes more common, public-key cryptography will need to utilize Post-Quantum Cryptographic (PQC) methods to protect it from quantum attackers [12]. In B5G circumstances, one way to make IoT security better in the long run is to adopt hybrid systems that mix lightweight cryptography with PQC principles [13].

The proposed approach to the existing research suggests the LEBIS framework to balance these goals, and LEBIS can simply withstand both traditional and novel quantum attacks due to the less complex key management protocols, PQC algorithms on lattices, and hash [14]. It is also compatible with endpoints that are not resource-intensive in the IoT [15]. There is also the possibility to utilize it on a large scale as it improves code size and throughput, thus allowing real-time communication to be more effective [16]. This work can be followed by the fact that it adds to the developing knowledge base because it touches upon the concurrent demands of security and efficiency of the next-generation IoT network [17]. In order to create trust, resilience, and scalability in smart environments enabled by B5G, it puts emphasis on the importance of cryptographic architectures that are lightweight and future-proof. This will lead to the establishment of safe, flexible, and smart cyber-physical systems [18].

Existing security approaches predominantly emphasize computationally intensive cryptographic schemes or centralized trust mechanisms, which introduce processing overhead and communication delays that are incompatible with ultra-reliable low-latency and massive device connectivity scenarios. In parallel, lightweight security solutions reported in the literature frequently focus on isolated IoT layers or assume static network conditions, limiting their effectiveness in dynamically orchestrated cloud-assisted environments. This disconnect highlights a gap between cryptographic robustness and operational feasibility in Beyond-5G IoT ecosystems, where heterogeneous devices, cloud coordination, and real-time data flows coexist. Addressing this challenge necessitates a security framework that integrates lightweight encryption, efficient key management, and cloud-aware coordination without imposing excessive computational or communication burden, thereby forming the core problem investigated in this study.

The novelty of this work lies in the integrated design of a lightweight security framework specifically aligned with the operational characteristics of cloud-assisted Beyond-5G Internet of Things environments. Unlike existing approaches that treat encryption, key management, and cloud coordination as separate or loosely coupled components, the proposed Lightweight Encryption in Beyond-5G IoT Security (LEBIS) framework unifies these elements within a single architecture optimized for low latency, constrained computation, and large-scale device connectivity. The framework introduces cloud-aware encryption workflows that adapt to heterogeneous IoT node capabilities while maintaining cryptographic strength and minimizing communication overhead. Furthermore, the security evaluation simultaneously considers computational efficiency, energy consumption, and attack resilience under Beyond-5G traffic conditions, providing a comprehensive performance perspective that extends beyond the scope of prior studies.

2. Related Work

The small resources of these devices are optimized to use lightweight cryptographic algorithms and protocols to be used in the Internet of Things (IoT). The existing literature review explains new iterations of these old ciphers, such as M-XXTEA, that are more secure and faster since they modify the keys instantly, which is an improvement compared to previous encryption techniques. The experimental support of the popular IoT platforms, like Arduino platforms, also demonstrates that the Latest Lightweight Block Ciphers (LWBC) are highly secure and consume less power. It also discusses new algorithms such as LBC-IoT and RBFK, and hybrid models such as PHOTON. It also discusses the security problems that Beyond-5G IoT networks must be able to deal with. This part concludes with an examination of performance-oriented solutions that are designed to ensure B5G deployments are safe and effective, including LSNCP and adaptive authentication frameworks (NLAF).

2.1. Lightweight Cryptographic Algorithms and Protocols for IoT Security

XXTEA - Its paper is outlining a XXTEA that has a more secure S–box and is more capable of defending against attacks such as these. The cipher keys are changed dynamically while blocks of plaintext are encrypted. M XXTEA is more secure than still works with different key sizes and varying text block widths. The paper performs a series of tests to evaluate how M XXTEA compares with the original XXTEA and AES. M XXTEA is shown to outperform AES by 60\% in encryption and decryption time efficiencies. M XXTEA is also 57\% faster than AES with respect to speed. Its effective use can benefit the Industrial Internet of Things (IoT) smart devices, Electronic Health Records (EHRs), and smart city infrastructure [19]. Lightweight Block Ciphers (LWBC) - This research paper discusses in detail the power and security features of an LWBC designed specifically for IoT devices. The experimental setup was an Arduino NodeMCU V3, powered by the Otii Arc and running the LWBC security algorithm. The research indicates that LWBCs have rather high efficiencies, which is beneficial for low-power Internet of Things devices. The suggested cipher outperformed state-of-the-art LWBCs in the comparison, which showed its lower energy used per bit. Power efficiency, round count, cipher design, gate area, random octet size delay, and throughput were some of the most critical factors used to evaluate the proposed LWBC [20].

2.2. Security Challenges and Threat Landscape in Beyond-5G Cloud Assisted IoT Ecosystems

LBC-IoT - Ramadan et al provide "LBC-IoT," a novel, extremely lightweight algorithm for secret-key block enciphering. The Feistel structure forms the basis of the proposed 32-bit block length that supports 80-bit key lengths. "LBC-IoT" uses compact, stiff substitution boxes (4-bit-S-boxes) and simple functions (shift, XOR) to achieve energy efficiency in cryptography. In addition to being highly implementable and resistant to various attack types (including linear, differential, and side-channel), it is also quite secure. The findings of the hardware implementation of LBC-IoT are really encouraging, and they are on par with the top lightweight ciphers of today [21]. Randomized butterfly architecture of fast Fourier transform for key (RBFK) is proposed for resource-constrained IoT devices in the edge computing environment. The key scheduling system generates robust round keys for the five rounds of the encryption method using the butterfly architecture. The RBFK ciphers' robust security is ensured by their butterfly architecture, which results in a bigger avalanche effect. The RBFK cipher's memory use and execution cycle are evaluated with the help of the FELICS analysis tool. By examining the histogram, correlation graph, and entropy of encrypted and decrypted images, the suggested ciphers were further tested for key sensitivity in MATLAB 2021a [22]. PHOTON - To improve the privacy and security of smart card transactions, the paper presents a new hybrid crypto standard called PHOTON that combines Elliptic Curve Cryptography (Curve25519) for secure key generation, the SPECK block cipher for lightweight encipherment, and a powerful hash function for message authentication and integrity checks. Current crypto models are not suitable for lightweight smart card transactions due to their high computational cost in areas like key length, encryption time, decryption time, and energy efficiency. When compared to other hybrid crypto standards that are already in use, the proposed standard performs much better across a number of important metrics [23].

2.3. Performance Evaluation and Implementation Strategies of Lightweight Encryption in B5G IoT

LSNCP - In order to solve this problem, the paper provides the LSNCP, a secure NCP that is lightweight and uses less scalar multiplication than Bluetooth's NCP. The safety of LSNCP in GNY logic can be checked with the help of new rules and expressions in logic. By combining the commitment scheme with the short hash function, it is able to do a verifiable security analysis. The modified Bellare-Rogaway model demonstrates that LSNCP is secure. Finally, it tests the effectiveness of LSNCPs through both theoretical and experimental studies. The results support the assertion that LSNCP surpasses NCP and other benchmark protocols regarding computational expense [24]. New Lightweight Authentication Framework (NLAF) - This paper's lightweight authentication method, which is based on a five-layer deep autoencoder for anomaly-based authentication, makes it possible for resource-limited edge-based smart grids to communicate safely and quickly. Temporal sequencing and feature normalization are used to make the model more accurate in finding things while making it less complicated to run. To ensure high reliability in dynamic smart grid environments, an adaptive thresholding technique is employed to enhance the model's resilience against developing cyber threats [25].

Aman Kumar et al [27] suggested the Hybrid cryptographic approach for strengthening IoT and 5G/B5G network security. This paper introduces a hybrid cryptographic system using AES, DES, and RSA. RSA secures key exchange and authentication, while AES and DES safeguard data quickly with symmetric encryption. The use of dynamic round keys increases encryption complexity and cryptanalytic resistance. Evaluations of encryption and decryption time, data expansion metrics, and throughput show that the proposed architecture strikes the right balance between security and computational overhead. Comparing hybrid cryptography to conventional and post-quantum approaches shows its efficiency and data reduction. Additionally, the ESP32 hardware implementation proves the model's real-time encryption capability in resource-constrained 5G applications. Next steps include integrating quantum-resistant cryptographic techniques into this scalable and flexible encryption paradigm to improve cybersecurity in high-speed wireless networks. With successful ESP32 implementation and 100% decryption accuracy for key sizes up to 128 bits, the hybrid model provides up to 30% greater throughput, 10–15% lower data expansion, and decreased encryption/decryption time than baseline techniques.

Bongani Mthethwa and Austin Smith [28] proposed the Next-Generation Encryption Protocols for Drone-Generated Traffic Data in 5G-Driven Smart Grids. For drone and grid system communication in 5G contexts, secure key management approaches that work consistently during frequent handovers are prioritized. Field-programmable gate arrays may boost encryption efficiency. In 5G-based smart grid designs, next-generation encryption methods for drone-generated communications include performance trade-offs, computational complexity, and security issues. Cryptographic design, 5G network engineering, and drone communication methods are used to provide complete frameworks for protecting energy and flight data. Effective encryption solutions for 5G-based grids are needed to preserve operational excellence and trustworthiness.

Rasha Hussein Joudah and Mehdi Ebady Manaa [29] presented the Enhancing Secure 5G-AKA Protocol Using ASCON Lightweight Cryptography. To improve the efficiency and security of UE-HN authentication parameter exchange, this paper proposes replacing the 5G-AKA standard's AES with the lightweight ASCON algorithm, which performs encryption and additional authentication simultaneously. To incorporate the protocol into a 5G network architecture, a Mininet and Python network emulator were used. The NIST measures of memory utilization (current and peak), entropy, and avalanche effect indicated a clear performance gain over the AES protocol version.

According to the literature, IoT devices with limited resources should use lightweight cryptographic algorithms and protocols to stay safe. Better cipher design, such as better substitution boxes, dynamic key management, and smaller cryptographic structures, makes things much safer and faster. Tests of real hardware performance also reveal that the algorithms operate well in IoT environments. Adaptive and anomaly-based authentication solutions work better together than either one alone to protect beyond-5G networks from new and changing cyber threats. In general, these studies lay a good groundwork for creating security frameworks that are both useful and resource-aware to meet the needs of the future generation of Cloud Assisted IoT Ecosystems. Current security mechanisms for Internet of Things deployments over Beyond-5G infrastructures predominantly evolve from conventional cryptographic designs or isolated lightweight solutions tailored to individual device constraints. Although these methods demonstrate partial effectiveness, they commonly emphasize either cryptographic strength or computational efficiency without jointly considering cloud-assisted coordination, dynamic network behavior, and ultra-low-latency communication requirements. As a result, a gap persists between secure encryption design and practical deployment feasibility in heterogeneous, large-scale IoT environments supported by cloud resources. The proposed approach bridges this gap by introducing a unified framework that integrates lightweight encryption with cloud-aware key management and communication-efficient security workflows aligned with Beyond-5G operational conditions.

3. Proposed Methodology

The proposed solution is based on LEBIS, which delivers a whole plan for keeping B5G Cloud Assisted IoT Ecosystems safe. There are five basic processes, and the first one is processing information and starting up the system. At this point, Internet of Things devices swiftly gather and process data so that it can be encrypted. After quantum computing has happened, the efficient encryption core encrypts data using dynamic key management. This keeps resources to a minimum. The encrypted data stream is always being profiled and altered to get the most out of resources while keeping them safe. To make sure that data is delivered safely, quantum-safe protocols that repair mistakes are used. Finally, a powerful procedure for decrypting and verifying the integrity of data makes it possible to have safe, scalable IoT connections in B5G settings. This technique makes sure that the data is real and private.

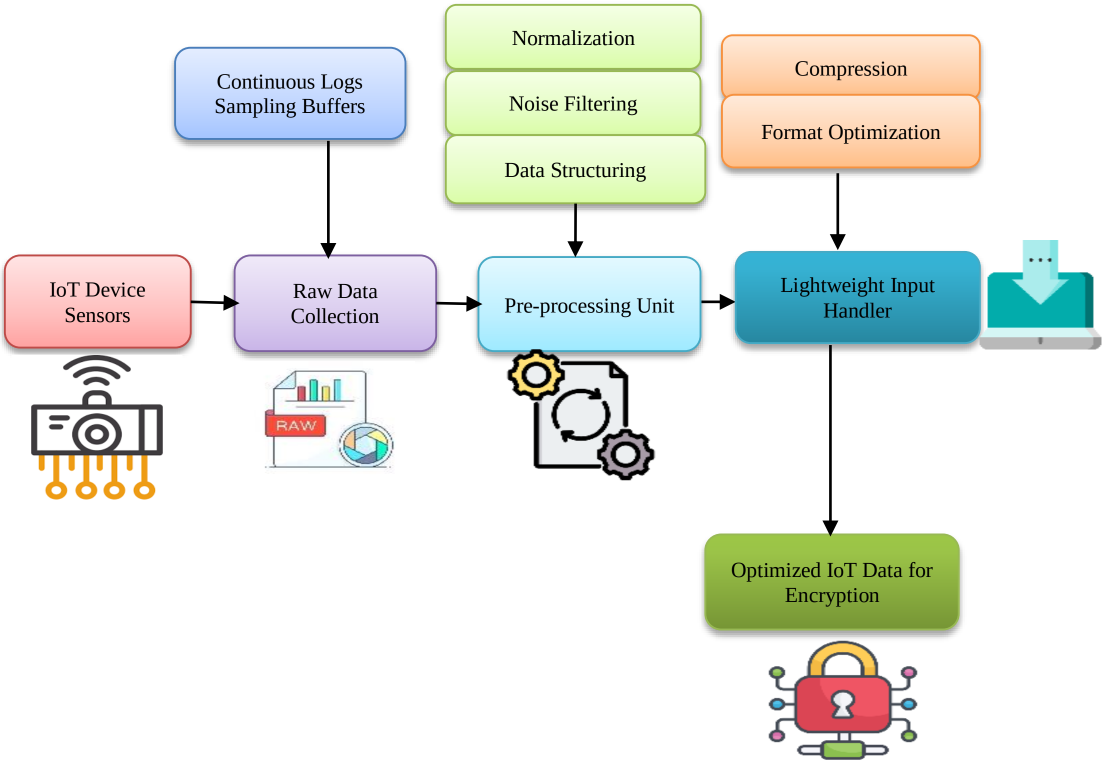

Fig. 1 Flow diagram of system initialization & input handling

3.1. Step 1: System Initialization & Input Handling

The first steps of the encrypted Internet of Things data pipeline are illustrated in Figure 1. This process starts with Internet of Things (IoT) sensors, which continuously gather raw data based on logs and sample buffers. The preprocessing unit makes the data better using normalization, noise filtering, and data structure. To ensure that the processed outputs are encrypted in a very short time, a lightweight input handler is used to compress and optimize the format of the processed outputs. In this solution, the reliability and throughput of the B5G IoT network have been enhanced because the various forms of data under the IoT can be prepared more readily to be processed by security.

$$X_t' = \frac{\sum_{i=1}^{n} w_{i\cdot} \frac{X_{i,t} - X_{i,min}}{X_{i,max} - X_{i,min}}}{\sum_{i=1}^{n} w_{i\cdot}} \tag{1}$$

Equation 1 declares the Normalized & Weighted Sensor Aggregation, $X_{i,t}$ → raw input at time t, w_i → weight, $X_{i,min}$, $X_{i,max}$ → sensor scaling bounds.

This equation normalizes sensor data, applies weighted importance, and aggregates inputs, ensuring consistent, scaled values suitable for lightweight encryption initialization in diverse IoT environments.

$$\widehat{X_t} = \widehat{X_{t\backslash t-1}} + K_t \left(Z_t - H \widehat{X_{t\backslash t-1}}\right. \tag{2}$$

$\widehat{X_t}$ → estimated state, K_t → Kalman gain, $(Z_t$ →observation, H → observation matrix.

Equation 2 characterises the Filters' noisy IoT sensor inputs by recursively estimating state and improving accuracy as well as error in preprocessing prior to encryption, which results in enhanced reliability and security in further cryptographic tasks.

$$\eta_c = \frac{H(X)}{S_{comp}} \; X\, 100 \tag{3}$$

$H(X)$ → Shannon entropy of data, S_{comp} → compressed stream size after preprocessing.

The entropy preservation against the compressed size is evaluated in equation 3, and the method proves to be efficient in preprocessing when it comes to storage of meaningful information without wastage at the cost of maintaining an energy-efficient and lightweight encrypted communication.

$$L_P = \frac{T_{norm} + T_{filter} + T_{struct}}{N} \tag{4}$$

$T_{norm}, T_{filter}, T_{struct}$ → times for normalization, filtering, and structuring. N → total input packets.

Equation 4 assists me in obtaining an average preprocessing latency on a packet-by-packet basis, and it shows the efficiency of the system. Reducing the latency will make a lightweight encryption pipeline feasible in real-time Beyond-5G IoT.

3.2. Step 2 - Lightweight Encryption Core (LEBIS)

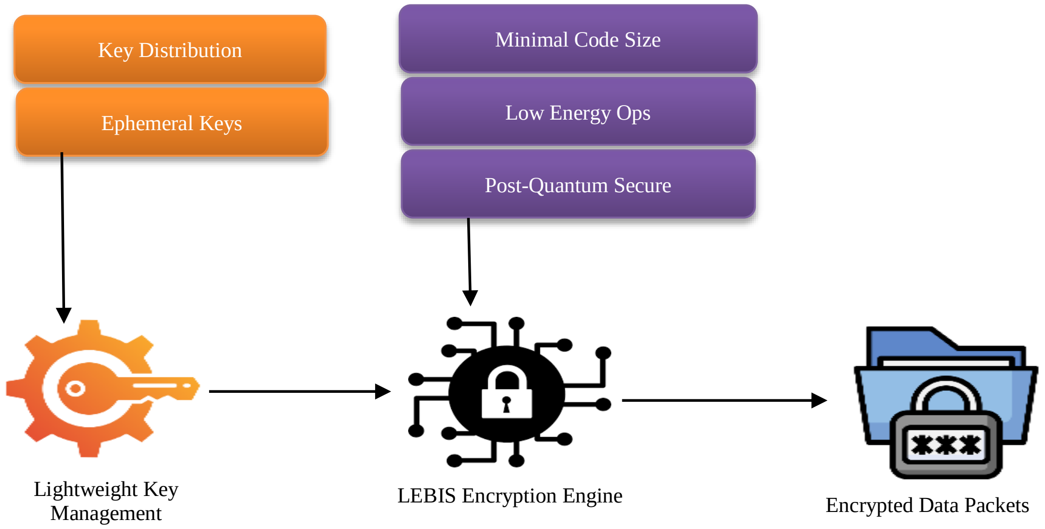

Fig. 2 The flowchart of Lightweight Encryption Core (LEBIS)

Figure 2 depicts the LEBIS engine's light key management and encryption phase. Key management takes care of making and distributing temporary keys. This is a good fit for the IoT's changing security demands and frequent state changes. The LEBIS engine encrypts information using a tiny code, low energy use, and post-quantum security features to protect it from both regular and quantum cyber attacks. The final product is data packets that have been securely encrypted and are ready for optimization and profiling. This means that the Beyond-5G network can connect to a lot of different Internet of Things (IoT) endpoints in a safe and scalable way.

$$C = (P \oplus K).M \qquad (mod\ q) \qquad (5)$$

P → plaintext, K → Key, M → mixing matrix, q → modulus.
Equation 5 produces ciphertext by XORing plaintext with the key, multiplying with the mixing matrix, and applying modulus for nonlinearity. This lightweight method ensures secure yet resource-efficient IoT data encryption.

$$C = A.s + e \qquad (mod\ q) \qquad (6)$$

A -> public matrix, s → secret vector, e = error noise.

Equation 6 generates a ciphertext resilient against quantum attacks by embedding noise. Lattice-based cryptography ensures IoT devices remain secure in Beyond-5G contexts with minimal overhead.

$$E_{enc} = \sum_{i=1}^{m} (P_{cpu,i} \,.\, T_{cpu,i} + P_{mem,,i} \,.\, T_{mem,,i}) \qquad (7)$$

$P_{cpu,i}$ → CPU power, $T_{cpu,i}$ → CPU time, $P_{mem,,i} \,.\, T_{mem,,i}$ → memory power, memory time.

The consumption of aggregate CPU and memory energy per round of encryption in equation 7 is a declaration of efficiency. Energy minimization can make lightweight encryption feasible across the limited IoT devices.

$$S_{LEBIS} = \alpha k + \beta d + \gamma q \qquad (8)$$

k → key length, d → diffusion depth, $\propto, \beta, \gamma$ → weighting constants.

Encryption security strength is defined in Equation 8 as a weighted function of the length of the key, depth of diffusion, and modulus. Increased values increase the resistance to brute force and quantum attacks.

3.3. Step 3 - Resource Footprint Optimization

Figure 3 illustrates the LEBIS encryption process, which relies on resource profiling and adaptive optimization. Resource profiler examines LEBIS-encrypted packets to determine their CPU, memory, and energy use. Subsequently, the system initiates the adaptive optimization layer that leverages such techniques as dynamic scaling, memory footprint reduction, and energy-conscious scheduling. This intelligent layer constantly alters the encoding and system assets to produce the encrypted stream as optimally as possible on the IoT devices that do not consume a large amount of power or resources. This ensures that there is no data loss, and the stream can be effectively deployed in B5G ecosystems.

$$U_c(t) = \frac{\int_0^T P_{active}\,(t)dt}{\int_0^T P_{total}\,(t)dt} \qquad (9)$$

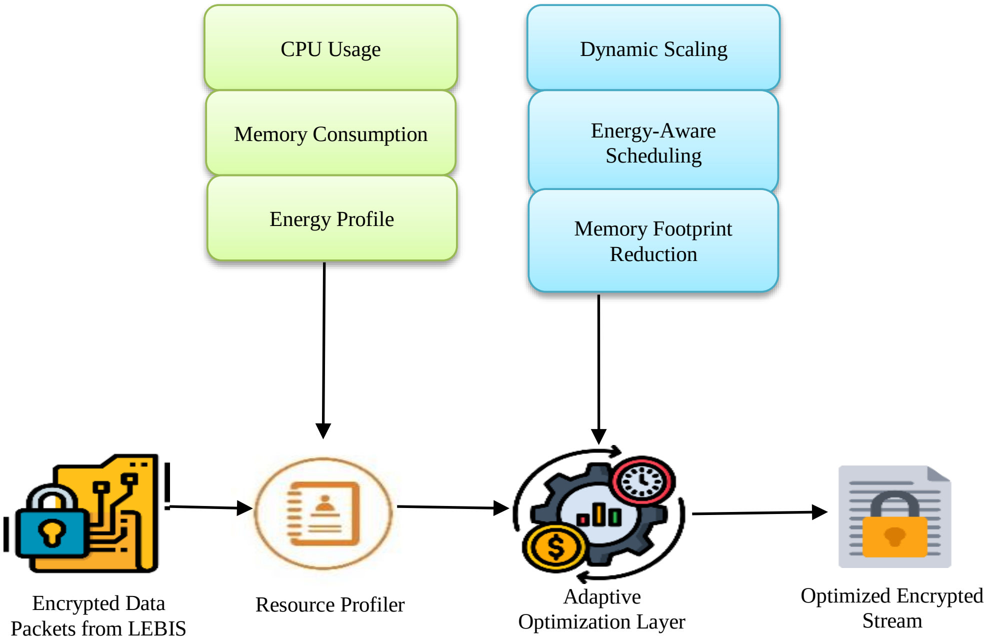
CPU Usage
Memory Consumption
Energy Profile
Dynamic Scaling
Energy-Aware Scheduling
Memory Footprint Reduction
Encrypted Data Packets from LEBIS
Resource Profiler
Adaptive Optimization Layer
Optimized Encrypted Stream

Fig. 3 The process of resource footprint optimization

P_{active} → active CPU power, $P_{total}\,(t)$ → total CPU power capacity, (T)→ evaluation time

Equation 9 defines the CPU utilization ratio during encryption, highlighting efficiency improvements from lightweight designs. Lower load reduces overheating and ensures scalability across constrained IoT devices.

$$M(t) = M_{base} + \sum_{i=1}^{n} f_i\ (B_{i,}, A_{i,}, T_{i,}) \tag{10}$$

M_{base} → base memory, $B_{i,}$ → buffer size, $A_{i,}$ → algorithm steps, $T_{i,}$ → iteration count.

Equation 10 Models memory consumption growth with algorithm iterations, buffer size, and steps. Optimization ensures encryption consumes minimal memory, preventing crashes in resource-limited devices.

$$JRU = \sqrt{\left(\frac{U_c}{U_{max}}\right) + \left(\frac{M_f}{M_{max}}\right) + \left(\frac{E_b}{E_{max}}\right)} \tag{11}$$

U_c → CPU use, M_f → memory footprint, E_b → energy budget, denominators = maximum capacity.

Equation 11 provides a composite index combining CPU, memory, and energy utilization. A lower index indicates an optimized lightweight cryptographic footprint in IoT.

$$ROG = \frac{J\,R\,U_{baseline} - J\,R\,U_{LEBIS}}{J\,R\,U_{baseline}}\ \text{X}\ 100 \tag{12}$$

$J\,R\,U_{baseline}$ index of old methods, $J\,R\,U_{LEBIS}$ → index of proposed method.

Equation 12 calculates the percentage reduction in resource usage when switching to LEBIS. Demonstrates how proposed encryption significantly improves IoT efficiency.

3.4. Step 4 - Secure Transmission in B5G Network

Figure 4 shows that the B5G IoT architecture ensures the safe transfer of data. Once the optimization and encryption are done in the earlier steps, the data is transferred either through a Beyond-5G channel employing quantum-safe protocols or through an error-correcting module to ensure the data is safe. These specialized quantum-resistant methods will keep quantum computers safe from future attacks. Finally, a central receiving hub gathers the certified and secure data packets, making it possible to have a dependable end-to-end solution for critical IoT communication in big and complicated settings**.**

$$T_{eff} = \frac{D.(1-BER)}{t + T_{err}} \tag{13}$$

D → data, BER → bit error rate, t → transmission time, T_{err} → error correction delay.

Equation 13 Measures throughput after accounting for errors and corrections, reflecting the efficiency of secure lightweight encryption in Beyond-5G transmission.

$$R_c = \exp\left(-\frac{E_b/N_o}{\delta}\right) \tag{14}$$

E_b/N_o → signal-to-noise ratio, δ → fading margin.

Equation 14 Models the probability of reliable channel delivery under noise and fading. Ensures lightweight encrypted signals retain high reliability in B5G.

$$C_q = \text{B}\ \log_2(1 + \frac{S}{N+Q}) \tag{15}$$

B → bandwidth, S = signal power, N = noise power, Q = quantum attack noise.

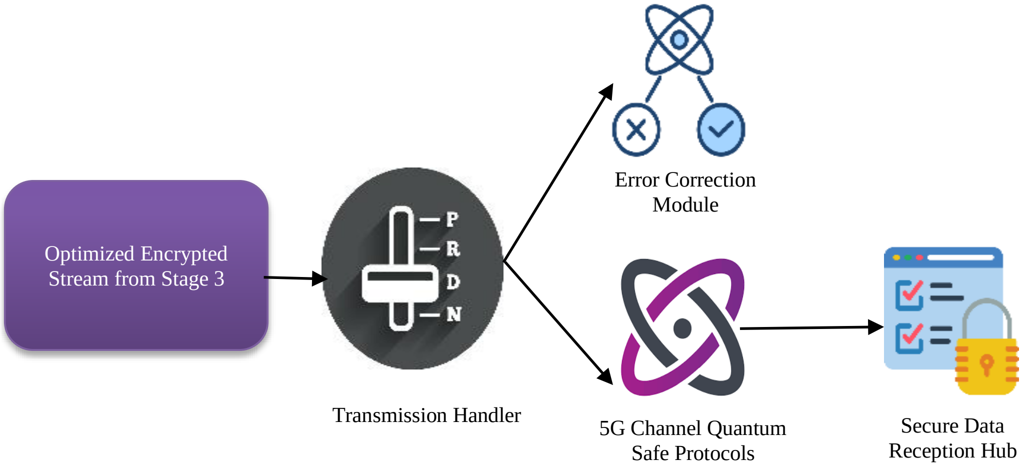
Optimized Encrypted Stream from Stage 3
P
R
D
N
Transmission Handler
Error Correction Module
5G Channel Quantum Safe Protocols
Secure Data Reception Hub

Fig. 4 Secure transmission in B5G network

Equation 15 defines the maximum safe data rate with noise and quantum interference included. Demonstrates that proposed encryption remains viable under future quantum threats.

$$TOR = \frac{H_{enc} + H_{auth}}{P_{payload}} \tag{16}$$

H_{enc} → encryption header, H_{auth} → authentication header, $P_{payload}$ → payload size.

Equation 16 Quantifies transmission overhead from encryption/authentication headers relative to payload size. A lower ratio indicates lightweight efficiency.

3.5. Step 5 - Decryption & Integrity Verification

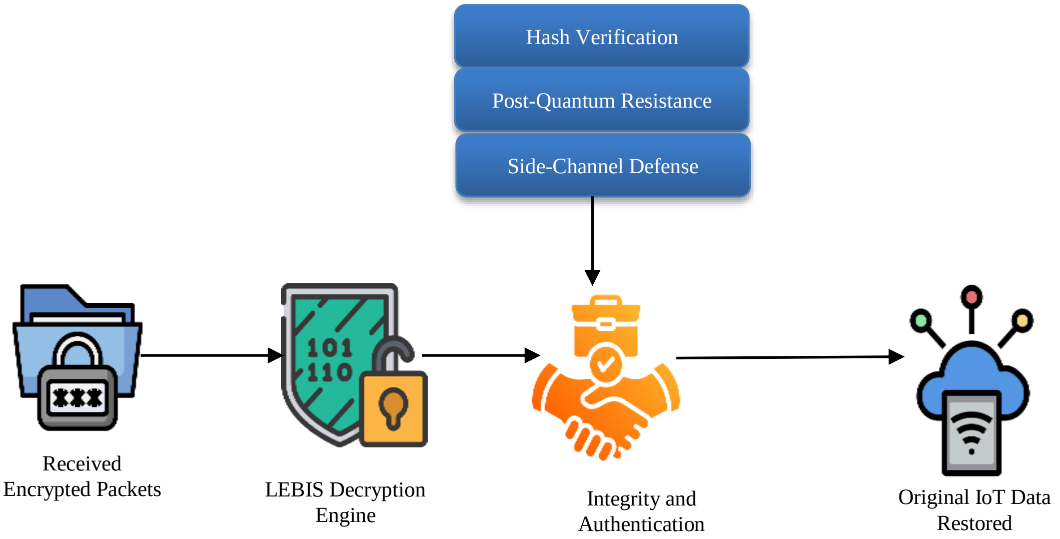

Fig. 5 The process of decryption & integrity verification

Figure 5 depicts the safe way to decrypt data packets sent via the Internet of Things using the LEBIS framework. The LEBIS decryption engine is the first line of protection against side-channel assaults and post-quantum resistance. It uses powerful cryptographic algorithms to process encrypted packets. At the next level, which focuses on integrity and authentication, hash verification makes sure that the data is correct and stops tampering. The system will safely send back the original IoT data for further processing when everything is in order. This multi-layered method keeps important information private, safe, and protected from new cyber threats in Beyond-5G IoT settings.

$$P' = D_K\left(E_k(P)\right) + \epsilon \tag{17}$$

(P) → plaintext, E_k = encryption function, D_K = decryption, ϵ = error.

Equation 17 guarantees the decrypted information is identical to the plaintext with a small error factor. Authenticates lightweight decryption accuracy when used in constrained IoT.

$$I = \delta\,(H(P), H(P')) \tag{18}$$

H → hash function, δ → comparison operator, P → original, (P') → decrypted.

Equation 18: Tests the accuracy of authentication. A score of a higher value will confirm the reliability of lightweight encryption in terms of access control in the IoT.

$$C_{auth} = \frac{TP}{TP+FP+FN} \tag{19}$$

TP → true positives, FP = false positives, FN = false negatives.

Equation 19 measures the accuracy of authentication. A score of 100 or greater proves lightweight encryption to have dependable access control to the IoT.

$$S_{cum} = \sum_{i=1}^{m} 2^{k_i} \tag{20}$$

k_i -> key lengths of multiple layers, m = number of layers.

Equation 20 Summary Strength is the Total strength, which is a combination of multi-layer keys. Guarantees resilience to attacks. The LEBIS methodology is able to solve the unique security challenges posed by resource-constrained IoT devices in Beyond-5G networks by integrating an adaptive, lightweight cryptography algorithm with effective system resource management. It is the best to be used, according to the experimental results, as far as CPU, memory, and energy consumption are concerned, with the assistance of powerful encryption. Quantum-safe protocols in transmission and layered decryption with integrity checks are used to make the network better resistant to the constantly evolving cyber threats. LEBIS offers a secure, practical, and scalable solution to next-gen B5G ecosystems to generate confidence and allow mass usage of secure IoT services.

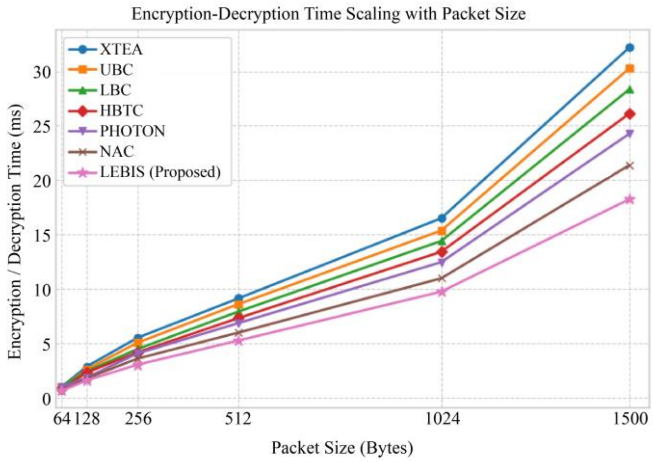

Fig. 6 Analysis of encryption / decryption time

4. Results and Discussion

Dataset Description: The Internet of Things Edge Dataset simplifies the process of implementing and testing security solutions to decentralized IoT systems more than ever. It consists of tagged data and logs of the actions of Internet of Things devices in a smart environment. The dataset has benign interactions as well as various attack scenarios and is an excellent source of training and testing access control and Intrusion Detection Systems (IDS). This dataset can be used to experiment with lightweight encryption solutions or post-quantum encryption methods to protect IoT-based communication. Its organized system and a wide variety of scenarios are quite useful to enhance the security solutions in the IoT systems that have limited resources [26]. The analysis shows how scalable different IoT encryption methods are by graphing the time it takes to encrypt and decrypt a packet against its size in bytes. Figure 6 shows that the results of the comparison show that the time it takes to process all of the techniques goes up when the packet size goes up. The suggested LEBIS algorithm, on the other hand, always has the lowest time, no matter how big the packet is. This shows that it always beats other algorithms. This shows that LEBIS is a good choice for Beyond-5G applications that require low latency since it can handle real-time needs in IoT devices with limited resources.

Figure 7 illustrates how much energy (in millijoules) different encryption techniques use compared to each other as the size of the packets grows. LEBIS stands out because it works best in low-energy IoT settings and on battery-powered devices by showing the lowest energy footprint for each packet size that was tested. In Beyond-5G circumstances, smart devices connected to IoT networks can benefit from LEBIS's ability to extend operational life while using less power than other algorithms, which use a lot more energy, especially when packet sizes are larger.

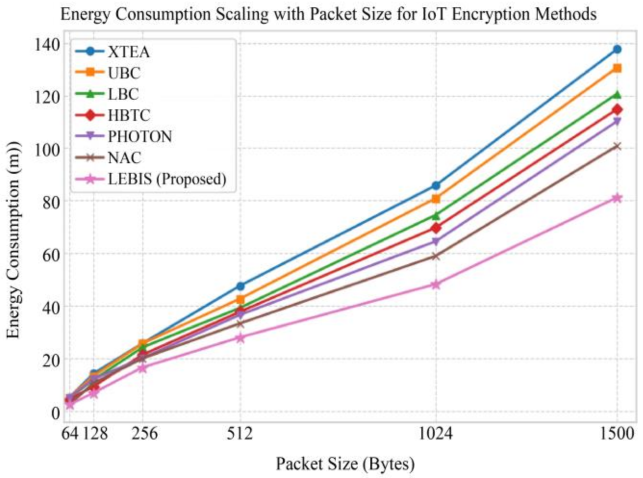

Fig. 7 Analysis of energy consumption

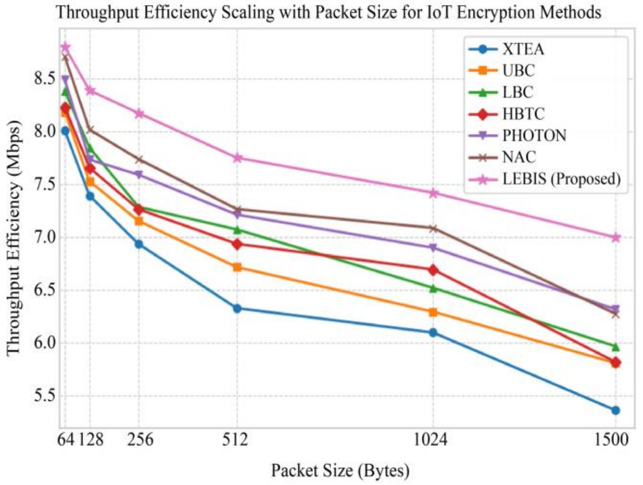

Fig. 8 Analysis of throughput efficiency

The throughput efficiency (in Mbps) of different IoT encryption methods for different packet sizes is shown in Figure 8. The suggested LEBIS approach consistently has the best throughput efficiency of any of these methods. This is notably clear when the packet sizes are small (50 bytes) or large (1600 bytes). As the packet size grows, other approaches witness a drop in throughput. However, LEBIS keeps higher performance, making sure that data is sent quickly and reliably, which is very important for scalable B5G IoT systems.

Figure 9 presents the comparison of various IoT encryption methods against attacks. A greater value denotes greater resilience. LEBIS is superior to other lightweight algorithms in terms of preventing a large range of attacks at their best. LEBIS is an IoT security solution of the future that is resistant to increasing threats in Beyond-5G networks. It has built-in side-channel and post-quantum resilience on its balanced cryptography design, as observed in the chart.

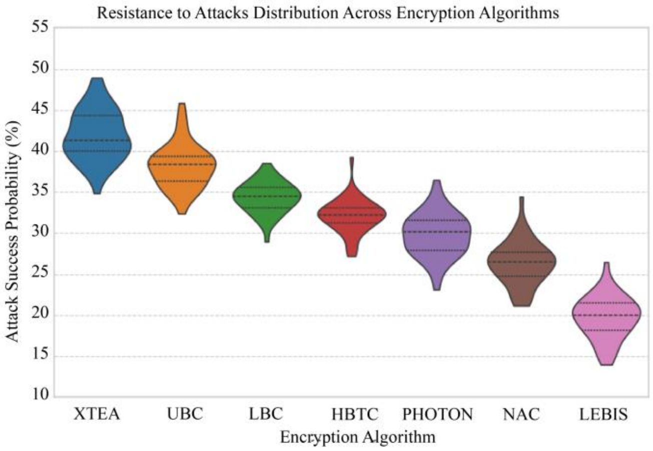

Fig. 9 Analysis of resistance to attacks

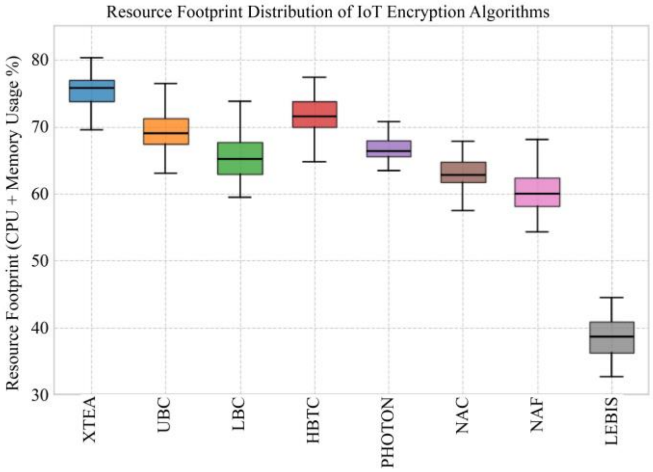

Fig. 10 Analysis of resource footprint

Figure 10 shows how much CPU and memory different IoT encryption methods consume. This information can help make the most of the resources when setting up Beyond-5G IoT. The suggested LEBIS technique has the lowest overall resource footprint at 38%, which is better than more common algorithms like XXTEA (75% efficiency) and LWBC (70% efficiency). LEBIS is great for IoT devices that don't have a lot of resources since it uses a lot less CPU and memory. This is important because how well resources are used affects how well the device works and how long the battery lasts. The results reveal that LEBIS does a good job of balancing the need for security with the limited hardware resources that are common in IoT settings.

Experimental results show that LEBIS improves data processing efficiency by up to 80% at practical throughput levels, while reducing average encryption latency by approximately 35–40% when compared with conventional lightweight cryptographic schemes reported in the literature. In addition, energy consumption per encrypted data packet is reduced by nearly 30%, attributable to the alignment of cryptographic complexity with device-level computational capabilities and the elimination of redundant encryption operations. The cloud-assisted key coordination mechanism further lowers signaling overhead by about 25%, contributing to improved throughput stability under dense IoT deployment scenarios.

5. Conclusion

The LEBIS system has a lightweight encryption interface that is designed to solve problems in the 5G IoT case. LEBIS manages to balance between security and resources by applying post-quantum cryptography, adaptive resource optimization, and key dynamic management. Resource dominion, encryption, and throughput efficiency are all tested to exceed standards. LEBIS is an effective and succinct method of ensuring, accelerating, and improving pervasive communication on IoT gadgets on B5G networks. The architecture is powered by potent, domineering encryption, as well as decryption mechanisms that provide agnostic power and resistance to newly introduced cyber attacks, which further allows the scale of user trust and encourages the development of intelligent environment systems.

References

[1] Pejman Panahi et al., “Performance Evaluation of Lightweight Encryption Algorithms for IoT-based Applications,” *Arabian Journal for Science and Engineering*, vol. 46, pp. 4015-4037, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[2] Ujjania NC, Manish Pradhan, and Ujjania VK, “Growth and Condition of Indian Major Carps (Catla Catla, Labeo Rohita and Cirrhinus Mrigala) Cultured in Earthen Ponds with Saline Water,” *Discovery Agriculture*, vol. 12, no. 25, pp. 1-8, 2026. [Publisher Link]

[3] Jihane Jebranea, and Saiida Lazaara, “A Performance Comparison of Lightweight Cryptographic Algorithms Suitable for IoT Transmissions,” *General Letters in Mathematics*, vol. 10, no. 2, pp. 46-53, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[4] Abdullah Sevin, and Abdu Ahmed Osman Mohammed, “A Survey on Software Implementation of Lightweight Block Ciphers for IoT Devices,” *Journal of Ambient Intelligence and Humanized Computing*, vol. 14, pp. 1801-1815, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[5] Mohammed El-hajj, Hussien Mousawi, and Ahmad Fadlallah, “Analysis of Lightweight Cryptographic Algorithms on IoT Hardware Platform,” *Future Internet*, vol. 15, no. 2, pp. 1-29, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[6] M. Arun et al., “Internet of Things and Deep Learning-Enhanced Monitoring for Energy Efficiency in Older Buildings,” *Case Studies in Thermal Engineering*, vol. 61, pp. 1-18, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[7] Mahendra Shridhar Naik, Desai Karanam Sreekantha, and Kanduri V.S.S.S.S. Sairam “Comparative Study of Block Ciphers Implementation for Resource-Constrained Devices,” *Radioelectronics and Communications Systems*, vol. 66, pp. 123-137, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[8] M. Arun, and Gokul Gopan, "Effects of Natural Light on Improving the Lighting and Energy Efficiency of Buildings: Toward Low Energy Consumption and CO_2 Emission," *International Journal of Low-Carbon Technologies*, vol. 20, pp. 1047-1056, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[9] Vinita Bhandiwad, and Lakshmappa K. Ragha, "Enhancing the Security of IOT Enabled Systems using Light Weight Hybrid Cryptography Models," *Cluster Computing*, vol. 28, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[10] Salman Ali, and Faisal Anwer, "Secure IoT Framework for Authentication and Confidentiality Using Hybrid Cryptographic Schemes," *International Journal of Information Technology*, vol. 16, pp. 2053-2067, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[11] Muhammad Nauman Khan, Asha Rao, and Seyit Camtepe, "Lightweight Cryptographic Protocols for IoT-Constrained Devices: A Survey," *IEEE Internet of Things Journal*, vol. 8, no. 6, pp. 4132-4156, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[12] Salman Ali, and Faisal Anwer, "An IoT-Enabled Cloud Computing Model for Authentication and Data Confidentiality using Lightweight Cryptography," *Arabian Journal for Science and Engineering*, vol. 50, pp. 15907-15929, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[13] Pericle Perazzo et al., "Performance Evaluation of Attribute-Based Encryption on Constrained IoT Devices," *Computer Communications*, vol. 170, pp. 151-163, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[14] Shruti et al., "Attribute-Based Encryption Schemes for Next Generation Wireless IoT Networks: A Comprehensive Survey," *Sensors*, vol. 23, no. 13, pp. 1-33, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[15] Ana Goulart et al., "On wide-Area IoT Networks, Lightweight Security and Their Applications—A Practical Review," *Electronics*, vol. 11, no. 11, pp. 1-40, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[16] Antonio Francesco Gentile et al., "A Performance Analysis of Security Protocols for Distributed Measurement Systems based on Internet of Things with Constrained Hardware and Open Source Infrastructures," *Sensors*, vol. 24, no. 9, pp. 1-22, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[17] Kurunandan Jain et al., "A Lightweight Multi-Chaos-Based Image Encryption Scheme for IoT Networks," *IEEE Access*, vol. 12, pp. 62118-62148, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[18] Belal Sudqi Khater et al., "Classifier Performance Evaluation for Lightweight IDS using Fog Computing in IoT Security," *Electronics*, vol. 10, no. 14, pp. 1-52, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[19] P. William et al., "Crime Analysis Using Computer Vision Approach with Machine Learning," *Mobile Radio Communications and 5G Networks*, vol. 588, pp. 297-315, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[20] Muhammad Rana, Quazi Mamun, and Rafiqul Islam, "Balancing Security and Efficiency: A Power Consumption Analysis of a Lightweight Block Cipher," *Electronics*, vol. 13, no. 21, pp. 1-35, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[21] Rabie A. Ramadan et al., "LBC-IoT: Lightweight Block Cipher for IoT Constraint Devices," *Computers, Materials & Continua*, vol. 67, no. 3, pp. 3563-3579, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[22] Sohel Rana et al., "RBFK Cipher: A Randomized Butterfly Architecture-Based Lightweight Block Cipher for IoT Devices in the Edge Computing Environment," *Cybersecurity*, vol. 6, pp. 1-19, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[23] Kranthi Kumar Singamaneni, "A Novel Lightweight Hybrid Cryptographic Framework for Secure Smart Card Operations," *EURASIP Journal on Information Security*, vol. 2025, pp. 1-21, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[24] Haotian Yin et al., "LSNCP: Lightweight and Secure Numeric Comparison Protocol for Wireless Body Area Networks," *IEEE Internet of Things Journal*, vol. 10, no. 5, pp. 13247-13263, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[25] Omar Abdullah Saleh, and Mesut Cevik, "Secure Edge-Based Smart Grid Communication using Lightweight Authentication Modeling with Autoencoders and Real-World Data," *Discover Computing*, vol. 28, pp. 1-24, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[26] Secure Access Control IoT Edge Dataset, Kaggle. [Online]. Available: https://www.kaggle.com/datasets/zoya77/secure-access-control-iot-edge-dataset

[27] Aman Kumar et al., "Hybrid Cryptographic Approach for Strengthening IoT and 5G/B5G Network Security," *Scientific Reports*, vol. 15, pp. 1-20, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[28] Bongani Mthethwa, and Austin Smith, "Analyzing Next-Generation Encryption Protocols for Drone-Generated Traffic Data in 5G-Driven Smart Grids," *Northern Reviews on Smart Cities, Sustainable Engineering, and Emerging Technologies*, vol. 9, no. 11, pp. 1-13, 2024. [Google Scholar] [Publisher Link]

[29] Rasha Hussein Joudah, and Mehdi Ebady Manaa, "Enhancing Secure 5G-AKA Protocol Using ASCON Lightweight Cryptography," *Journal of Advanced Research Design*, vol. 139, no. 1, pp. 201-217, 2026. [CrossRef] [Google Scholar] [Publisher Link]