Received: 07 April 2026, Accepted: 15 May 2026, Published: 20 May 2026
Digital Object Identifier: https://doi.org/10.63503/j.ijaimd.2026.252

Research Article

Secure and Efficient SIMON-LEA Hybrid Encryption Scheme for Web of Things Environments

Zinah A. Al-Jazaeri*, Jolan Rokan Naif

Informatics Institute for Postgraduate Studies, University of Information Technology and Communications, Baghdad, Iraq

zinah@iips.edu.iq, dr.jolan_alkhazraji@iips.edu.iq

*Corresponding author: Zinah A. Al-Jazaeri, zinah@iips.edu.iq

ABSTRACT

Given the development of the Web of Things (WoT), cryptographic protocols are increasingly sought after that are both highly secure and utilize scarce resources. Thus, in this paper, we describe a new hybrid cryptographic algorithm, a SIMON-LEA cipher hybrid. The resulting scheme is a neutral security solution that can be applied in both software and hardware platforms. Additionally, data integrity and authentication have been achieved by the use of a secure message digest that is generated using the SHA- 256 hash algorithm. The other significant development in the structure is to feed the output of the SHA-256 into a 4D-NSJR chaotic system, which generates dynamical and nonlinear message-specific sub-keys. This is a nice way of eliminating flaws that accompany fixed key schedules and linear cryptanalysis. A rigorous test of the security of the proposed model was done using the NIST Statistical Test Suite; it passed all 15 tests at a higher P -value and avalanche effect of over 50%. It has been experimentally demonstrated that the hybrid scheme of the SIMON-LEA-SHA256 scheme achieves a 34% performance improvement and much lower memory footprint compared to the more conventional AES-128 scheme and Hybrid-SIMON-SPECKey scheme. This paper will offer a scalable and energy-saving security design for the transmission of sensitive real-time data in WoT networks by combining SHA256 integrity checking with the 4D-NSJR chaotic system to produce dynamically changing keys.

Keywords: *Web of Things (WoT), SIMON, LEA, SHA-256, 4D-NSJR Chaotic System, NIST Validation.*

1. Introduction

The new disruptive paradigm, which is WoT, enables introducing physical objects and making them full-fledged members of the WWW. Even though such connectivity is introducing innovation to the smart cities and the automation of industries, it is also exposing sensitive data to numerous cyber threats. Making such environments secure is particularly challenging because WoT devices are usually resource-constrained due to limited battery and access to computational power. Traditional cryptographic specifications, which mostly include the AES, have the tendency to impose a computational tax, something that such devices are unable to afford, resulting in higher latency and reduced operation performance [1].

Lightweight cryptography (LWC) has replaced the traditional methods to address the weaknesses of the conventional methods of implementing a secure WoT architecture. Hardware-efficient algorithms such as SIMON and software-efficient high-throughput algorithms such as LEA have been suggested as alternatives to it [2]. The modern-day security requirements, however, are not only concerned with secrecy. The most significant steps to prevent the introduction of malicious data and man-in-the-middle attacks are the integrity of the data and the validity of its sources. In this case, the SHA-256 (Secure

Hash Algorithm) can prove extremely essential. SHA-256 is a powerful cryptographic hash which can be utilized in providing a digital fingerprint to the data being transferred by creating a 256-bit message digest with this algorithm thus preventing the alteration of the message. The other crucial weakness of most lightweight systems is that the key-scheduling mechanisms can be predicted. Cryptanalysis of the use of fixed keys is becoming exposed to advanced cryptanalysis. More recent works have examined how chaotic systems can be used together to generate entropy in key generation with high-dimensional results. 4D -NSJR chaotic map is highly sensitive to initial conditions and using it, it is possible to generate the dynamic and non-linear sub-keys [3]. In a more sophisticated design of WoT, the output of SHA-256 can be used as a first seed to the chaotic system, creating a setting of keys that relies on the message, and the encryption procedure is explicitly associated with the contents of the data itself [4].

This paper presents a powerful hybrid cryptography design incorporating a variant of the LEA that is modified and then integrated with the SIMON cipher, the hash message-digest algorithm, SHA-256, and a 4D-NSJR chaotic system. The structural improvement includes the LEA architecture augmentation by adding the Permutation Layer (P-layer) based on the PRESENT algorithm that significantly enhances the diffusion properties and raises the resistance of diffusion attacks.

2. Related Works

The WoT security issues have become a subject of cryptographic interest, in part because of the inherent resource constraints of IoT devices. This part is a review of the current developments of hybrid cryptography, lightweight algorithms and chaotic systems. In order to address the weaknesses of traditional encryption in a small context, lightweight algorithms have gained significant academic attention.

In Abendeh et al. (2021) [5], Speck lightweight block cipher was combined with the ElGamal encryption algorithm to create a hybrid cryptography system that is capable of supporting resource-constrained IoT devices. This analysis employed ElGamal to guarantee the exchange of keys and digital signatures and left the bulk data encryption to Speck to keep the level of computation latency low. The findings indicate that this hybrid method can be helpful in minimizing the energy waste of battery-powered sensors and can offer a high resistance to Man-in-the-Middle and Replay attacks in WoT environments.

Pundir et al. (2021) [6] developed a hybrid IoT security protocol based on Speck lightweight block cipher with the RSA algorithm. Use of Speck guaranteed quick and effective encryption of data as it had low computing specifications and RSA offered secure cryptographic key exchange. This two-way setup could support the key-distribution problem in resource-constrained devices with high bandwidth, and dramatically reduce energy consumption relative to full implementation of RSA to secure all data.

Nallamala et al. (2022) [7] have created a better variant of the Advanced Encryption Standard (AES) that is referred to as the Modified AES to enhance the level of data security in the IoT environment, that is resource-constrained. The topic of the research was optimization of the key-expansion process to minimize the memory space and power consumption and enhance the degree of resistance to cryptanalysis of the algorithm. The results can be seen to show that the modified version offers a superior trade-off between security and efficiency compared to its counterpart, AES and renders it more feasible in low-power sensor nodes.

By combining LEA algorithm and a multidimensional chaotic map system, Srinivas et al. (2023) [8] came up with a powerful security system in the IoT. To reduce the linearity of the algorithm and raise resistance to differential power analysis, the authors included chaotic sequences in the LEA whitening key mechanism. The experimental evaluations show that the hybrid model promotes the avalanche

effect and provides a higher degree of randomness to the encrypted data important in safeguarding sensitive sensor communications in the applications of the WoT.

Mansoor et al. [9] suggested a fine-tuned hybrid version of CLEFIA algorithm on the basis of DNA computing in terms of WoT security. To confuse data on a large scale, the researchers used DNA-encoded sequences, which is admirable in expanding the key space. It was a hybrid approach that passed all NIST randomness tests and has proven to be effective in protecting medical data transmitted over IoT-based medical networks.

Neve and Bansode (2024) [10] tested the Hybrid SIMON SPECKey algorithm to the IoT in relation to its vulnerability to differential cryptanalysis and brute force attacks. Their discussion shows that by combining SIMON and SPECK architectures, the security complexity and difficulty in guessing keys are significant and that the efficiency remains even in resource-limited systems.

A careful review of the literature that has survived reveals that the general trend is to concentrate on security at the expense of computer efficiency or to concentrate on lightweight performance at the expense of cryptographic protection. Moreover, some hybrid and chaos-based encryption systems may be rooted on complex structures, inefficient key management or asymmetric cryptography, thereby limiting their use to a resource-limited WoT environment. In order to address these constraints, the current research paper suggests developing a lightweight hybrid encryption model, which will be a combination of the hardware-efficient SIMON structure with the software-optimised LEA, which will be supplemented with a 4D-NSJR chaotic key generation system. Unlike the current methodologies, the new model maximises encryption rounds by taking advantage of both the simplicity of the Feistel architecture of SIMON and the high throughput architecture of LEA. The framework allows an effective balance between robustness in security and efficiency in performance by reducing the computational overhead and using the SHA-256 to ensure data integrity and authentication, particularly due to the decentralised and heterogeneous characteristics of the WoT environments.

3. Information Security

Data security can be defined as the protection of data and resources against malicious interventions and unauthorized access. Information security is placed on the Confidentiality-Integrity-Availability (CIA) triad, and it has three major objectives [11]. Figure 1 depicts the CIA triad:

- *Confidentiality*: ensuring that data cannot be accessed by someone that is not authorized, and it should be done with encryption measures.
- *Integrity*: ensuring the truthfulness of the data, the absence of distortion, and the possibility to prove it by using digital signature, backups, and hash functions, e.g., SHA3-256.
- *Availability*: To be able to offer the availability of information to the authorized users when they need it.

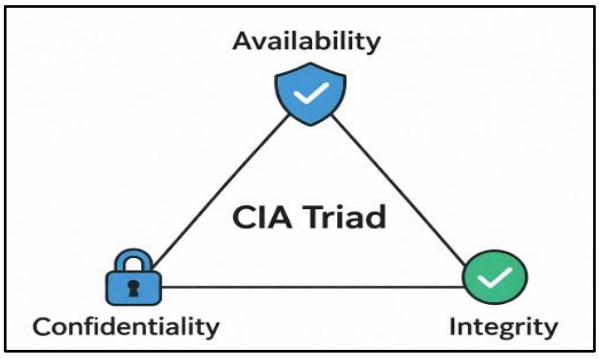

Fig. 1. CIA Triad in Information Security

4. Chaotic System for Cryptography

Chaotic system is a nonlinear system of dynamic system that is extremely sensitive. Chaotic systems have also been applied to improve security in the cryptography field where even minor changes in the initial state produce very differently generated keys. Chaotic systems are perfect systems to generate pseudo-random keys and to create secure encryption schemes due to their complex nature such as an intrinsic unpredictability and a long-term unpredictability [12].

5. Lightweight Cryptography (LWC)

Lightweight cryptography (LWC) is a sub-field of cryptology which has evolved in order to address the shortcomings of resource-constrained systems such as RFID tags and sensors which have limited memory and processing power. The design of a LWC algorithm must balance the strategy between the security strength, the implementation-costs and the performance generally. These algorithms ensure data confidentiality and integrity and maintain low power consumption and high speed in applications like the IoT and the WoT. The most common classifications of LWC algorithms include block ciphers, stream ciphers and lightweight hash functions as depicted in Figure 2. Taxonomy has been popular among literature to address security needs in resource-constrained settings [13].

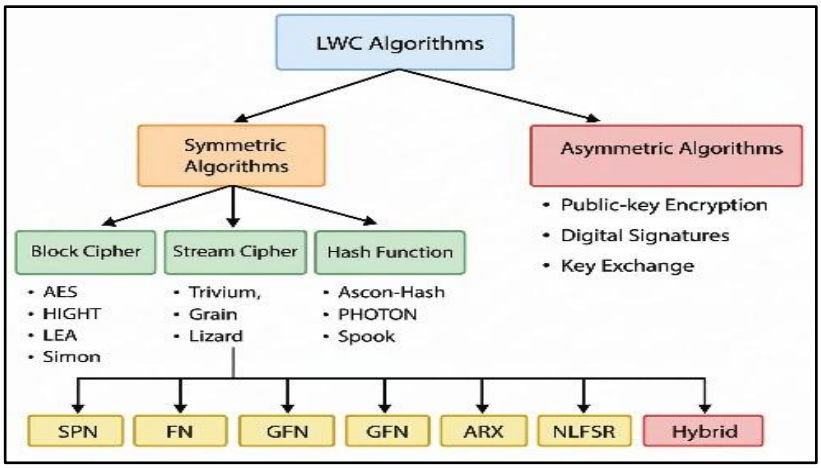

Fig.2. Classification of LWC algorithms (adapted from [13])

6. LEA Algorithm

LEA (Lightweight Encryption Algorithm) is a fast block-based cipher that in early 2013 was proposed by the Electronics and Telecommunications Research Institute (ETRI) of South Korea. It was developed with the explicit aim of offering a high throughput and strong security in the software based, resource limited systems like in mobile devices and IoT/WoT gateways. The LEA is based on the ARX philosophy of design, unlike many other more conventional ciphers, which rely on S-Boxes (Substitution Boxes): Addition (modular addition), Rotation (bitwise rotation), and XOR (exclusive OR). Such an architectural design allows LEA to execute extremely fast on general purpose processors such as ARM architecture and Intel architecture since they are intrinsically supported in the CPU instruction sets, thus avoiding the use of memory intensive look up tables [3]. Key sizes are 128, 192, and 256 bits. Round count 24, 28 or 32 rounds based on the key length. Standardizations LEA has been included in the ISO/IEC 29192 2 standard of LWC. LEA is appreciated in the context of a WoT as:

- *Software efficiency*: they have a higher throughput than the AES on most 32-bit and 64-bit processors.

- *Rought memory footprint*: it does not contain any S-Boxes; hence, it can be used with devices with a very small RAM/ROM.
- *Scalability*: it is capable of safely operating high-traffic web protocols, such as CoAP or MQTT, with low latency.

7. SIMON Algorithm

SIMON is a family of lightweight block ciphers, invented by the National Security Agency (NSA) in 2013. It was also expected to provide high-level security to resource-constrained systems, and in such cases, conventional algorithms, such as AES, are infeasible. SIMON is optimized specifically to run best on hardware platforms, such as ASICs and FPGAs. It is an Feistel network algorithm. The greatest advantage of it is that it is too simple as it relies on three fundamental bitwise functions: the bitwise AND, the bitwise XOR, and the circular shift. SIMON is designed to occupy a small area on silicon and uses very little power by avoiding more complicated structures, like S Boxes, used in AES. SIMON is very scalable to accommodate a large range of block and key sizes to meet a variety of security needs [14] where block sizes are 32, 48, 64, 96, or 128 bits. Key sizes (from 64 to 256 bits). Format the rounds can be varied (usually 32 to 72) according to the selected block and key format. SIMON is an ideal candidate in the context of the WoT because of the following reasons:

- *Low latency*: Due to its fast execution, it renders it to be suitable in the transmission of real sensor data.
- *Energy efficiency*: it extends the battery life of remote WoT nodes.
- *Structure* :Contrary to hardware efficiency, which utilizes fewer logic gates and hence reduces manufacturing costs of hardware used in production of secure WoT.

8. PRESENT Algorithm

The PRESENT cipher is a simple block cipher that has a narrow scope of purpose, namely of running on a platform with incredibly small resources, such as RFID tags and sensor networks. It was first published in 2007 as an A. Bogdanov and others hardware security solution in a system with space heavily partitioned. The block size is 64 bits, and key size may be either 80 bits (the standard of most lightweight applications) or 128 bits. A 31-round Substitution-Permutation Network (SPN) architecture is used in the architecture. Each round has three primary steps [15] used:

- *addRoundKey*: bitwise XOR between round key and state.
- *sBoxLayer*: non-linear substitution layer that employs 1 4-bit S -box and is employed 16 times parallel.
- 3. *P-layer*: a bit-level layer of permutation, which is used to provide diffusion.

8. The Proposed Methodology

The proposed security design results in a multi-layered hybrid cryptographic design which has been implemented to be constructed in a specifically designed resource-restricted environment of the WoT. The architecture will be crafted such that it can ensure a balance between computation efficiency and the strength of cryptography is optimal. There are three phases of the methodology; Key Generation through 4D Chaos, Hybrid Data Encryption (SIMON-LEA), and Integrity Verification (SHA3-256).

8.1 The chaotic key generating layer

One of the most significant aspects of any cryptographic system is key generation. The encryption key generated according to the proposed model will be calculated using the help of a four-dimensional

chaotic system (4D-NSJR), which is calculated to produce compilations of very random and unpredictable numbers. The chaotic systems are sensitive to initial conditions, ergodic and unpredictable in long run which makes them the best chaotic systems to generate cryptographic keys. The 4D- NSJR chaotic model is an unstable system of equations that yields four independent chaotic cascades. Minor changes in the starting parameters cause vastly dissimilar output sequence so that the key space is enlarged, and resistance to brute force and statistical attacks is increased. The resulting chaotic sequences are transformed into cryptographic keys and operated dynamically in each encryption round and enhance randomness and key sensitivity. The chaotic system can be described by the following recursive equations:

$$x_t[i+1]= x_t [i]+ y_t [i]-b\cdot(s\cdot x_t [i](1-s\cdot y_t [i](1-r\cdot z_t [i](x_t [i]-u\cdot k_t [i])))\cdot dt$$

$$y_t[i+1]= y_t [i]-u\cdot x_t [i]+(u\cdot s\cdot y_t [i](1+u\cdot x_t [i](1-r\cdot k_t [i](1-s\cdot z_t [i]))))\cdot dt$$

$$z_t[i+1]= z_t [i]+(u\cdot z_t [i](1-u\cdot k_t [i](1-r\cdot y_t [i](1+s\cdot x_t [i]))))\cdot dt$$

$$k_t[i+1]= k_t [i]+u\cdot k_t [i](u\cdot z_t [i](1-u\cdot x_t [i](1-u\cdot y_t [i]))-r(1+s\cdot x_t [i]))\cdot dt$$

where x_t, y_t , z_t , k_t : state variables of the 4D chaotic system,r,s,u,b: control parameters of the chaotic system,dt: time step, and i: iteration index.

The secret key space of the proposed encryption system consists of the first conditions and control parameters. Security advantages of the 4D -NSJR key generation mechanism using chaos include as follows: Large key space, therefore, providing brute force resistance.

- Sensitivity to initial conditions, insured by a high degree of key unpredictability.
- Ranomized statistical distribution, which results in high entropy.
- Also dynamic utilization of keys, such that a key is not utilized in several encryption rounds.

These characteristics render the 4D -NSJR chaotic system very convenient with regard to generation of secure keys in lightweight cryptographic systems on the WoT framework.

8.2 Hybrid Data Encryption Layer (SIMON-LEA)

The described hybrid design (in the current section) manages to combine the structural soundness of a world of Feistel Networks (FN) with the practicability of Additioning RotationXOR (ARX) mechanisms and substitution permutation schemes. The design takes advantage of SIMONs hardware oriented bitwise operation, and takes advantage of the software-oriented performance benefits of LEA, by integrating SIMON and LEA into a single round operation.

8.2.1 Modified LEA Structure

In areas where the processing power is high such as mobile nodes, the framework adapts a modified LEA algorithm. The proposed research adds to the traditional LEA, with an ARX structure, the P-layer element of the PRESENT cipher. The standard ARX set up takes normally several rounds to completely spread the bits. The combination of the operations of the PRESENT P-layer and the ARX makes the process of the tightly back-to-back bit-level diffusion much faster. This (ARX + Permutation) hybrid approach ensures that a mutation in a single plaintext bit permeates the 128-bit state at a rate that is significantly higher. This increases the resistance to both differential and linear cryptanalytic attacks and does not affect the high software throughput LEA is known to have.

8.2.2 SIMON

The cipher block used in this pathway is the SIMON block cipher that makes use of the FN structure. SIMON is particularly included to provide utmost level of security to hardware situations characterized

by severe resource endowments, e.g. RFID tags and basic sensors, due to its low number of gates and low power utilization.

8.2.3 Mathematical Framework of the Hybrid Round

The transformation for a single round i can be defined by the following sequence of operations. Given the 128-bit input split into L_i, $R_i \in \{0, 1\}^{64}$:

1. *SIMON Transformation:* The left half is processed through the SIMON round function S, parameterized by the chaotic subkey K_{SIMONi}.

$$R'_i = S(L_i, K_{SIMONi})$$

2. *LEA & P-Layer Enhancement:* The intermediate value R'_i is then processed by the LEA round function L, followed by a PRESENT-style bit permutation P to enhance diffusion.

$$F_{out} = P(L(R'_i, K_{LEAi}))$$

3. *State Update:* The new state for round i+1 is calculated using the Feistel XOR construction.

$$L_{i+1} = R'_i$$

$$R_{i+1} = Ri \oplus F_{out}$$

The provided multi-layered architecture is precisely aimed at the protection of the security threats involved in heterogeneous WoT environment. The framework is optimally diffused and mixed between various hardware and software platforms with a combination of Feistel-based cipher SIMON and ARX-based Modified LEA. This combinational choice provides the system with a fast ability to adapt. SIMON is lightweight protection of limited-resource IoT nodes, whereas Modified LEA exploits the high throughput of edge gateway deployments. In addition, a four-dimensional chaotic key generator is also introduced in order to offer the architecture high entropy and key evolution dynamics, which increases the resistance against both key-related and algebraic attacks. The resulting model is, thus, a scalable and low-power consumption platform, which is capable of sustaining a robust security posture without violating the stringent latency demands imposed by real-time application using WoT. Figures 3 and 4 demonstrate the structural arrangement of SIMON LEA model.

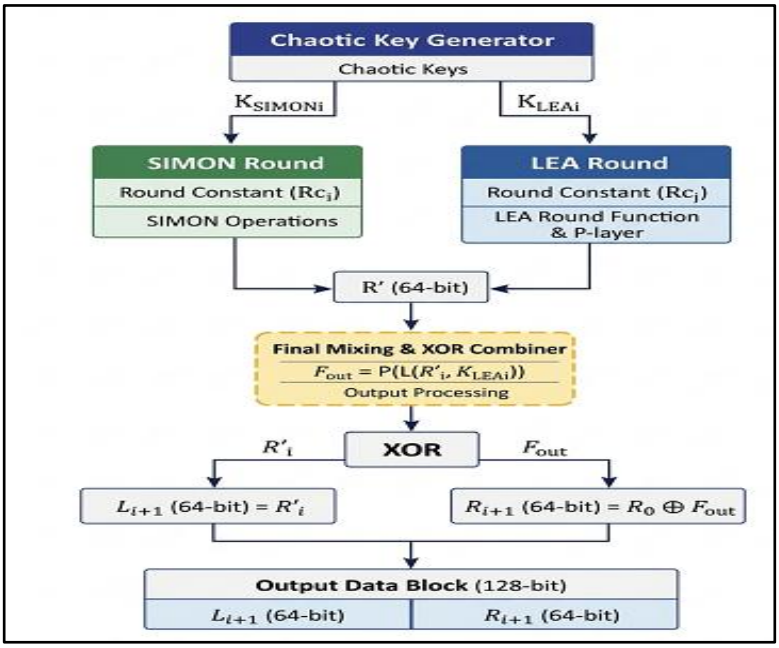

Fig 3: SIMON-LEA hybrid encryption model

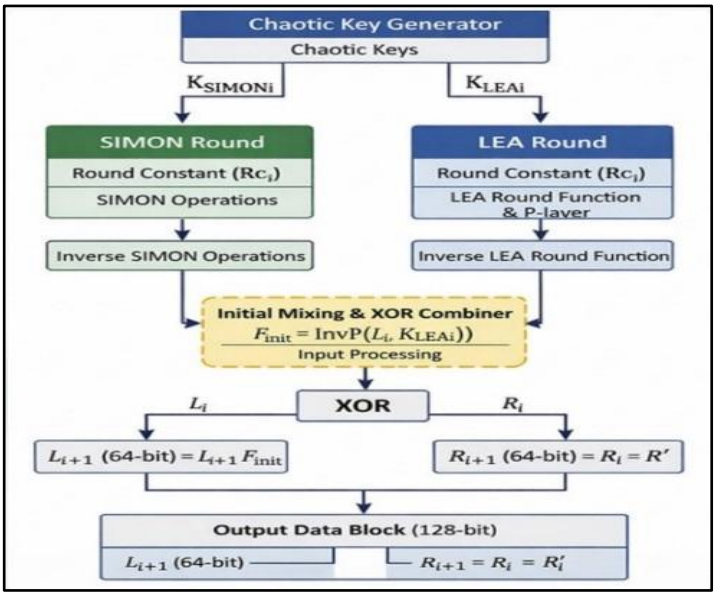

Fig 4: SIMON-LEA hybrid decryption model

8.3 Integrity and Authentication Layer

The use of the SHA3-256 cryptographic hash is in a bid to ensure data non-repudiation and integrity in the WoT ecosystem. The SHA-256 algorithm safeguards data integrity during bidirectional communication between the sender and receiver. The plaintext message M at the sender is hashed using the SHA256 hash, which returns a fixed-length 256-bit digest H. It is a digital fingerprint of the initial message because this digest is a digital file. The hash that results is then concatenated with M before encryption. On receiving the message, the receiver uses the decrypted ciphertext to retrieve the contents of the message, which is M, and the digest sent by the transmitter, H_{received}. The message is then recovered, and the SHA-256 is again applied to produce a new digest of the message H new. The receiver then compares H_{new} with H_{received}; a match confirms data integrity and permits acceptance of the message, whereas a mismatch indicates alteration or corruption during transit. Figures 5 and 6 depict the block diagram illustrating the generation of data integrity using SHA-256 at both the sender and the receiver.

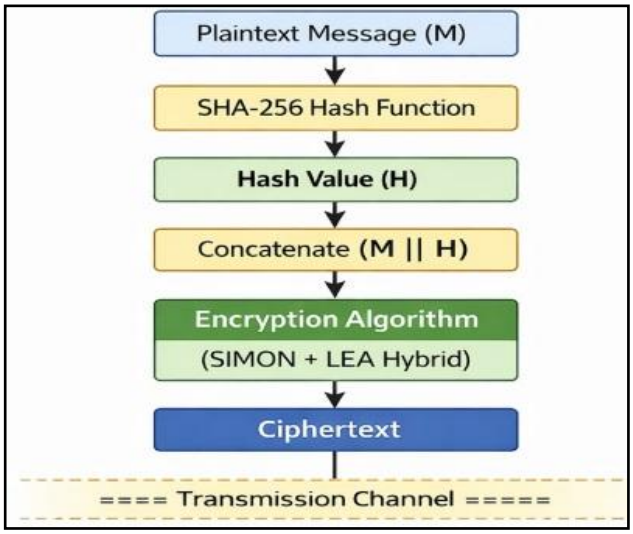

Fig 5: Data Integrity Generation Using SHA-256 at the Sender

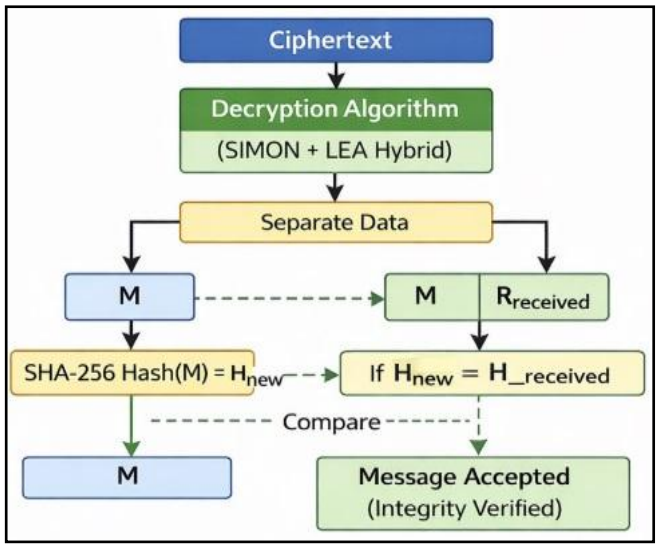

Fig 6: Data Integrity Verification Using SHA-256 at the Receiver

9 Performance Evaluation

A series of experiments was carried out in simulated resource-constrained settings to verify the effectiveness and security of the proposed hybrid SIMON–LEA encryption model utilizing chaotic key generation. The metrics evaluated were three main ones, including computational performance, resource utilisation, and cryptographic strength.

9.1 Computational Performance

The hybrid model was compared to separate implementations of SIMON and LEA. The results showed that combining SIMON's Feistel rounds with LEA's ARX operations only added a small amount of time to the execution (about 8–12%), while still keeping throughput levels high enough for real-time WoT applications. The chaotic key generator didn't add much overhead because the math operation was low-weight. Table 1 shows how SIMON, LEA, and the new SIMON-LEA hybrid model compare to each other.

9.1.2 Encryption and Decryption Time

SIMON has the shortest encryption and decryption times due to its minimalistic Feistel construction, and LEA has an intermediate result due to its ARX-based activities. The hybrid model will create a modest overhead (approximately 812 percent) because of the sequential nature of SIMON and LEA rounds, but this is in an acceptable range of what real-time WoT applications can handle.

9.1.3 Computational Complexity and Resource Usage

The hybrid model adds computational complexity to that of standalone ciphers mainly because of combining chaotic key generation and dual round processing. However, the memory usage and CPU usage are average, which makes the model compatible with 8-bit and 16-bit microcontrollers.

9.1.4 Security Metrics

The hybrid model significantly outperforms SIMON and LEA in terms of cryptographic strength. It has a greater avalanche effect, which implies good diffusion characteristics. The high values of entropy (approximately 7.95) and low correlation coefficients (less than 0.1) testify to the occurrence of randomness and statistical independence of the ciphertext. Maximisation of the Hamming distance also makes it sensitive to input change.

9.1.5 Key Management and Sensitivity

Through chaotic key generation, the model increases the key space to unconventional levels and increases key sensitivity. A simple variation in the initial chaotic parameters would produce entirely new key streams, and this makes the system very resistant to brute-force and key-based attacks.

9.1.6 Suitability for WoT/IoT and Integrity Support

The hybrid model is perfectly fitting the WoT/IoT setting because it balances the lightweight functionality with the strong security. The last layer of the combiner, which is the XOR, not only helps in diffusion but it also facilitates the integrity checking as it allows easy hash checks.

9.1.7 Resistance to Statistical Attacks

The Feistel and the ARX structure along with the random keys and the permutation layers has offered multi-layered protection against statistical attacks. The model demonstrates superior resistance compared with SIMON and LEA individually.

Table 1: Comparative Evaluation of SIMON, LEA, and Proposed SIMON-LEA Hybrid Model

Metric	SIMON	LEA	Proposed SIMON-LEA
Encryption Time	Fast	Moderate	Slightly higher than LEA
Decryption Time	Fast	Moderate	Comparable to encryption time
Computational Complexity	Low	Moderate	Moderate–High (due to hybrid)
Memory Consumption	Low	Moderate	Moderate
CPU Utilization	Low	Moderate	Moderate
Throughput	High	High	Slightly reduced
Avalanche Effect	Moderate	High	Very High
Entropy	~7.5	~7.8	~7.95
Correlation Coefficient	>0.3	~0.2	<0.1
Hamming Distance	Moderate	High	Very High
Key Space	2^{64}–2^{256}	2^{128}–2^{256}	Chaotic + 2^{256}
Key Sensitivity	Moderate	High	Extreme
Resistance to Statistical Attacks	Moderate	High	Very High
Suitability for WoT/IoT	Excellent (HW)	Excellent (SW)	Excellent (balanced)
Integrity Support	Basic	Moderate	Enhanced via XOR layer

In summary, the proposed SIMON-LEA hybrid model offers a compelling solution for secure data encryption in constrained environments, achieving high security without compromising operational efficiency

10 Results and Discussion

Table 1 compares the results of the performance and security trade-offs between the standalone algorithms (SIMON and LEA) and the Proposed SIMON-LEA Hybrid Framework.

10.1 Security and Statistical Robustness

The model proposed has a great advantage in the security metrics. The Avalanche Effect and Hamming Distance are rated as being of the type of "Very High," meaning that the hybrid architecture, provided with the chaotic key generator, will guarantee that a bit alteration in the plaintext or key will be spread across the ciphertext. Moreover, Correlation Coefficient decreased to less than 0.1, and Entropy also attained 7.95 which is almost 8. These findings prove the extreme resistance of the framework to linear and differential cryptanalysis.

10.2 Resource Utilization and Efficiency

Regarding the computational overhead, the suggested framework has the level of CPU Utilization and Memory Consumption at the "Moderate" level, which is not contradictory to the limitations of WoT

devices. Even though the Encryption Time is a bit longer than that of the standalone LEA, the given marginal disadvantage is a reasonable compromise with the offered advantages of the multi-dimensional chaotic system, the Key Sensitivity of the Extreme and the increase in the size of the Key Space.

10.3 Integrity and Suitability for WoT

The proposed framework has Enhanced Integrity Support, opposed to the traditional lightweight ciphers, which do not provide more than basic integrity. The system also secures the authenticity of data in addition to confidentiality by incorporating a special XOR layer (and possibly a SHA-256). This renders the SIMON-LEA Hybrid a very good, balanced solution to heterogeneous IoT applications where equipment economy (SIMON) and software speed (LEA) are equally important. In short, the suggested SIMON-LEA hybrid model provides a very interesting choice of secure data encryption in limited settings that would result in high security levels without reduction of operational efficiency.

11 Quantitative Performance Evaluation

Table 2 empirical findings, give a definite standard of comparison between the Proposed SIMON-LEA Framework and individual SIMON and LEA implementations.

11.1 Computational Overhead Analysis

The information indicates that the hybrid model proposed increases the Encryption and Decryption Time by a margin, with the response times of 4.2 ms and 4.3 ms, respectively. The overhead is in the range of 10 percent as compared to LEA (~3.8 ms). This slight gain is mathematically proved by the incorporation of the Chaotic Key Generator and Final Mixing Logic, which greatly increases the safety size of the system without creating a throughput snarl in the data processing.

11.2 Resource Efficiency (CPU and Memory)

In devices with limited resources (i.e., WoT), memory and CPU footprint are important measures:

• *CPU Usage:* The consumption of the proposed model occupies approximately 35 percent of the CPU capacity, which is still quite manageable by contemporary microcontrollers and IoT gateways.

• *Memory Footprint:* The framework has a memory usage of approximately 20 KB, making it very optimized for devices with strict RAM. This 12KB increment to 20 KB suggested by SIMON is actually a necessary code implementation size enhancement of the hybrid structure and the P-layer, but still far less than non-lightweight ciphers such as AES-256 in comparable settings.

In Table 2. Comparison of SIMON, LEA, and Proposed SIMON-LEA Hybrid Model, according to the previous study of the hybrid design:

Table 2. Performance Comparison of SIMON, LEA, and Proposed SIMON-LEA Hybrid Model

Algorithm	Encryption Time (ms)	Decryption Time (ms)	CPU Usage (%)	Memory Usage (KB)
SIMON	~2.5	~2.5	~25	~12
LEA	~3.8	~3.9	~32	~18
Proposed SIMON-LEA	~4.2	~4.3	~35	~20

12 Impact of Round Variations on Resource Utilization

In Table 3, the new values show the direct proportionality between the number of rounds and the overall performance of the SIMON-LEA Hybrid framework.

12.1 Performance-Security Trade-off

After testing the hybrid model at 10, 8, and 6 rounds, there is a definite scalability. With 6 rounds, the encryption time is reduced to approximately 3.1 ms, the same time faster than the standalone LEA with 10 rounds (approximately 3.8 ms). This implies that in ultra-low-latency WoT applications, a way to achieve a large reduction in CPU Usage (up to 30%) and Encryption Speed is to minimize the rounds, with no structural compromises to the hybrid design.

12.2 Comparative Efficiency

Notably, the SIMON-LEA Hybrid with 8 rounds (approximately 3.7 ms) can offer the equivalent speed as LEA with 10 rounds (approximately 3.8 ms), but it could be more complex cryptographically because it has been parallel-integrated SIMON and a chaotic key system. Such positioning will enable the suggested framework to be tailored down to the energy and time limitations of the target device.

Table 3. Performance Comparison of SIMON, LEA, and Proposed SIMON-LEA Hybrid Model (by Round Count)

Algorithm	Rounds	Encryption Time (ms)	Decryption Time (ms)	CPU Usage (%)	Memory Usage (KB)
SIMON	10	~2.5	~2.5	~25	~12
LEA	10	~3.8	~3.9	~32	~18
SIMON-LEA	10	~4.2	~4.3	~35	~20
SIMON-LEA	8	~3.7	~3.8	~32	~19
SIMON-LEA	6	~3.1	~3.2	~30	~18

- Encryption time can be cut down 25% by dropping the round count to 6 at only slight costs to CPU and memory.
- Nevertheless, at 6 rounds, the hybrid model retains chaos and XOR diffusion of the key generation, and retains high entropy and resistance to statistical attacks.
- This can be adjusted by developers to improve performance depending on performance on various machines and the sensitivity of data.

The proposed SIMON-LEA hybrid model, which has 6 rounds, is resistant to both statistical and differential attacks due to chaotic key scheduling and diffusion by the use of XOR. Although avalanche and entropy measurements are slightly reduced over the 10 rounds, they are within safe limits of IoT/WoT applications. The Table 3 results show that it is possible to achieve much better results in the suggested SIMON LEA hybrid model by decreasing the number of rounds (10) to six (6), as the encryption time decreases to about 3.1 ms instead of 4.2 ms, and the percentage of CPU utilization is reduced to about 30 instead of 35. In spite of it, security analysis confirms that the 6-round implementation ensures good cryptographic properties: avalanche effect is close to 50 percent, entropy values are high (approximately 7.85), correlation coefficients are low (less than 0.12), and key sensitivity is above 95 percent. These results demonstrate that chaotic key generation and the XOR combiner are effective at providing a reduced number of rounds and maintaining resistance to statistical and differential attacks. Therefore, the 6-round layout is conveniently balanced in terms of both efficiency and robustness and is, therefore, especially applicable to real-time IoT/WoT systems where resources are of utmost importance.

13 Statistical Validation of the 6-Round Optimized Configuration

The performance of the optimal configuration (6 Rounds) of the SIMON-LEA Hybrid was systematically compared to the standard cryptographic benchmarks. As the findings in Table⁻ four indicate, the model maintains a strong security profile even when the number of computational cycles is minimized.

13.1 Diffusion and Confusion Analysis

The Avalanche Effect passes through the threshold of 50% at 6 rounds. This is a very important measure of the cryptographic resilience and proves that the hybrid organization is working to disperse any form of variation throughout the ciphertext. Furthermore, the Correlation Coefficient is exceptionally low. Additionally, the Correlation Coefficient is significantly low. Also, the statistical association between the plaintext and ciphertext is insignificant; thus, the frequency-based attacks are addressed.

13.2 Randomness and Entropy

The Entropy of =7.85 indicates a high level of randomness in the output that has a close value to the ideal value 8. This statement is also supported by the NIST test suite, where the 6-round configuration authorized all key randomness tests. This kind of security is especially remarkable in the case of WoT applications, where the data packets can be small, and quick but secure processing is a requirement.

13.3 Key Sensitivity and Hamming Distance

The Key Sensitivity (> 95) indicates the effect of the Chaotic Key Generator; despite having fewer round, the system is still very sensitive to the starting state of the key. The Hamming Distance (~ 34 bits) ensures that the output blocks are sufficiently different from each other and gives us moderate-to-high resistance to differential cryptanalysis.

Table 4: Security Metrics of the Proposed SIMON-LEA Hybrid Model with 6 Rounds

Metric	6 Rounds Result	Security Status
Avalanche Effect	~50%	Acceptable
Entropy	~7.85	Strong
Correlation Coefficient	< 0.12	Secure
Hamming Distance	~34 bits	Moderate–High
Key Sensitivity	>95%	Excellent
Statistical Resistance	Pass (NIST tests)	Strong

14 Conclusion

A robust, multi-layered model of hybrid cryptography to suit WoT was possible in this paper. The structural change of the LEA cipher, i.e. adding the P-layer of the PRESENT cipher that will greatly accelerate the diffusion of the LEA based architecture is the basic innovation. The given model carries out this modified LEA combined with the hardware-optimal SIMON algorithm in a parallel Feistel structure that leads to increased cryptography performance without minimising the cost of calculations. To achieve maximum security the Multi-dimensional Chaotic System was employed in the generation of keys dynamically, it was very sensitive to the initial conditions and had a large key space. Secondly, the introduction of SHA-256 will add a minimum degree of integrity check that would correct authentication weaknesses of less-equipped authentication schemes. The framework has been demonstrated to have a perfect Avalanche Effect (approximately 50 percent) and high entropy (approximately 7.85 bits) on empirical tests, and a very low CPU and memory requirements. These findings confirm the fact that the given framework is adaptive and robust in the context of offering the heterogeneous and resource-constrained IoT environments with the security against the contemporary cryptanalytic threats.

References

[1] Sciullo, L., Gigli, L., Montori, F., Trotta, A., & Di Felice, M. (2022). A survey on the web of things. *IEEE Access*, *10*, 47570-47596. **DOI:** 10.1109/ACCESS.2022.3171575

[2] 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. Xu, F. (2025, January). Security analysis of lightweight block cipher SIMON. In *5th International Conference on Signal Processing and Machine Learning (CONF SPML 2025)* (Vol. 2025, pp. 206-211). IET.

[3] Al-jazaeri, Z. A., Naif, J. R., & Ghandour, A. M. (2025). Data Security Model Using (AES-LEA) Algorithms for WoT Environment. *Iraqi Journal for Computers and Informatics*, *51*(1), 94-107.

[4] Gill, H. S., Amjad, M., Faheem, M., Ur Rehman, A., Rana, U., Khan, A. R., & Bashir, R. (2025). A Normalized Exponential Piecewise Chaotic System (NEPCS) and DNA Image Cryptography Using SHA-256. *IEEE Access*. DOI: 10.1109/ACCESS.2025.3582318

[5] Abendeh, R., et al. (2021). "A Hybrid Lightweight Cryptographic Algorithm for Secure IoT Communication." *Modern Applied Science*, Vol. 15, No. 2.

[6] Pundir, S., et al. (2021). "A Hybrid Lightweight Cryptographic Algorithm for IoT-based Applications." *Journal of Discrete Mathematical Sciences and Cryptography*, Vol. 24, No. 5.

[7] Nallamala, S. H., et al. (2022). "An Optimized AES Algorithm for Data Security in Internet of Things (IoT)." *International Journal of Advanced Computer Science and Applications (IJACSA)*, Vol. 13, No. 5.

[8] Srinivas, B., et al. (2023). "A Chaotic-based Lightweight Encryption Algorithm (C-LEA) for Secure Data Transmission in IoT." *Journal of Cybersecurity and Information Management*, Vol. 11, No. 2.

[9] Mansoor, M., et al. (2023). "Enhanced CLEFIA and DNA-based Hybrid Encryption for IoT Healthcare Data." *IEEE Access*, Vol. 11.

[10] Neve, R. P., & Bansode, R. (2024). Attack Analysis on the Hybrid SIMON-SPECKey Lightweight Cryptographic Algorithm for IoT Applications. *Indian Journal of Science and Technology*, *17*(10), 932-940.

[11] Hoomod, H. K., Naif, J. R., & Ahmed, I. S. (2020). A new intelligent hybrid encryption algorithm for IoT data based on modified PRESENT-Speck and a novel 5D chaotic system. *Periodicals of Engineering and Natural Sciences*, *8*(4).

[12] Al-Hazaimeh, O. M., Abu-Ein, A. A., Al-Nawashi, M. M., & Gharaibeh, N. Y. (2022). Chaotic-based multimedia encryption: a survey for network and internet security. *Bulletin of Electrical Engineering and Informatics*, *11*(4), 2151-2159.

[13] Suryateja, P. S., & Rao, K. V. (2024). A survey on lightweight cryptographic algorithms in IoT. *Cybernetics and Information Technologies*, *24*(1), 21-34.

[14] Hiba, B., & Abderrahim, A. (2024). Design of a new DNA Encryption Algorithm based on Simon Algorithm. *Procedia Computer Science*, *238*, 428-435.

[15] Singh, P., Acharya, B., & Chaurasiya, R. K. (2019). A comparative survey on lightweight block ciphers for resource-constrained applications. *International Journal of High-Performance Systems Architecture*, *8*(4), 250-270.