Open Access ISSN: 3007-1437 (Online), ISSN: 3007-1429 (Print)

IRAQI Academic Scientific Journals

Alkadhim Journal for Computer Science (KJCS)

Journal Homepage: https://alkadhum-col.edu.iq/JKCEAS

KJCS ALKADHIM JOURNAL FOR COMPUTER SCIENCE

A Lightweight Hybrid Encryption Algorithm for Internet of Things Security Using ASCON and AES with Chaotic System

Wasan Alaa Hussain

Informatics Institute for Postgraduate Studies, university of information technology and Communications,Baghdad, Iraq

Email: wasan_alhamami@yahoo.com

Article information

Article history:

Received: March, 26, 2026

Accepted: April, 4, 2026

Available online: June, 25, 2026

Keywords:

Internet of Things (IoT);

Lightweight Cryptography;

Hybrid Encryption;

ASCON;

AES;

Chaotic Key Generation;

NIST Statistical Tests

Corresponding Author:

Wasan Alaa Hussain

Email: wasan_alhamami@yahoo.com

DOI:

https://doi.org/10.61710/pghstr62

Abstract

The recent rise in the use of Internet of Things (IoT) devices has further increased the pressure on cryptographic solutions that will meet the challenge of high-security standards, yet nearly meet the extreme resource requirements imposed by embedded computers by nature. The paper introduces a new hybrid encryption architecture that is aimed at meeting these conflicting requirements of the IoT setting. The scheme suggested is a variant of AES-r cipher combined with the ASCON authenticated-encryption primitive giving the AESASCON algorithm, and extended with integrity verification by the SHA3-256 hash to create the AESASCONH construction. Stochastic key material is calculated using a four-dimensional NoseSprott-Jerk-Rossler (4D-NSJR) chaotic system, which is highly sensitive to initial conditions causing the effective key space to become large and making brute-force enumeration challenging. The architecture is segmented into three layers that collaborate with one another and they are chaotic key generation, symmetric data encryption and authenticated-integrity verification. General testing against the complete NIST SP 800-22 statistical test is done that indicates that all the 15 randomness tests have been passed. Experiments with Five data sizes are used in experiments to demonstrate speedups ranging from 42% for large data payloads (1.5 MB) to 175% for small data sizes compared to AES. This demonstrates that the suggested approach provides efficient and secure protection for IoT. and entropy values of data of up to about the theoretical maximum of 8.0 bits per symbol, and thus confirm speed improvements as well as cryptographic strength is available to support high-assurance IoT deployments.

1. Introduction

Internet of Things (IoT) is a paradigm whereby physical objects which have sensors, actuators and network interfaces constantly gather and transmit data on the world communication infrastructure. Such a merging of physical and digital worlds makes possible unprecedented degrees of automation, efficiency of processes, and awareness of situations, including smart manufacturing and precision agriculture as well as connected healthcare and critical management of infrastructure [13].

With the growing pace in the IoT, the Web of Things (WoT) has become an additional architectural layer that links entities that exist on the physical-world in response to the Web of Things exposing them via a standard web protocols, simplifying interoperability and making integration simpler than with the former Wireless Sensor Network (WSN) architectures [1, 2]. Nevertheless, the widespread connectivity, that these ecosystems are characterized by, also creates a wide-scale attack surface. Normally sensitive telemetry, command traffic and personally identifiable information move through networks where most of the endpoints do not have the computational headroom to implement traditional cryptography primitives at reasonable latency [3].

The assurance of this information is based on the three CIA triad and confidentiality which is ensured by the use of encryption mechanisms in order to prevent unauthorized accessibility of the information; integrity, which is provided by cryptographic hash and digital signatures to prevent unauthorized change; and availability, which is guaranteed by the ability to provide access to the resources when necessary [4]. During the realization of these goals on small microcontrollers and sensor nodes, cryptographic codes must be developed so that they offer strong security at only a handful of processing cycles, memory, and energy use [5].

Traditional symmetric block ciphers, e.g. the Advanced Encryption Standard (AES) can offer good security assurances but introduce computational and memory costs that are either prohibitive on deeply embedded systems. Lightweight cryptographic algorithms such as the ASCON family which was chosen by NIST in 2023 as the standard authenticated-encryption algorithm in constrained systems fill this gap by providing comparable security to AES with very low resource usage [6]. A combination of the complementary weaknesses of a variety of primitives comprising hybrid structures is another design aspect, and they allow security-performance compromises, which neither style can provide individually [7].

In this paper, a hybrid encryption algorithm, referred to as AESASCON, which combines a structural revised version of AES with ASCON-128 is obtained and the scheme is cast to add SHA3-256 to become the AESASCONH authenticated-encryption scheme. The 4D-NSJR chaotic system is unpredictable and has a high dimensionality of its nonlinear dynamics producing key streams with optimal statistical characteristics. The rest of this paper is structured in the following way. Section 2 is related work survey. Section 3 presents the background of the hybrid lightweight cryptography. Section 4 will take a review of chaotic-system theory as applied in key generation. Section 5 typifies the ASCON algorithm. The proposed methodology is listed in section 6. Section 7 provides the results and analysis of the experiment and Section 8 concludes with the future research directions.

2. Related Works

The development of efficient and secure cryptographic algorithms for IoT and WoT environments has attracted considerable research attention. Investigations in this field span the design of novel lightweight primitives, hybrid constructions, and the integration of chaos-based key generation to strengthen encryption security. A representative selection of recent contributions is summarized below.

- Habib et al. [8] (2018) proposed LEAIoT, a lightweight symmetric-asymmetric hybrid scheme targeting low-latency IoT communication, demonstrating measurable throughput improvements over conventional approaches.
- Dobraunig et al. [9] (2019) introduced the ASCON authenticated-encryption suite, providing both AEAD and hashing primitives optimized for constrained hardware and software platforms.
- Hoomod et al. [10] (2020) proposed the HSPA algorithm, hybridizing the PRESENT and SPECK ciphers with a five-dimensional chaotic key-generation system to enhance security efficiency on resource-limited devices.
- Hoomod et al. [11] (2021) further investigated the combination of GOST and SPECK algorithms within WoT contexts, reporting enhanced flexibility and reduced encryption latency.
- Somaiya et al. [12] (2023) introduced EMAES, a hybrid AES-ECC construction that achieves high security with improved processing speed and accuracy for multimedia file protection.

- Basapur and Shylaja [13] (2021) augmented the AES structure with RSA-based key management to strengthen security for sensitive data applications.
- Jasim et al. [14] (2025) proposed a color-image encryption scheme employing a hybrid RC5-PRESENT construction with a 2D chaotic key generator, achieving resistance to differential and statistical attacks suitable for resource-constrained devices.
- Cagua et al. [15] (2025) evaluated ASCON's implementation and performance on IoT devices using the CupCarbon simulator, demonstrating its viability under resource-scarce conditions representative of smart-city deployments.
- Ismael et al. [16] (2025) introduced a lightweight cipher for healthcare IoT employing novel snake-based key generation within a blockchain-secured remote patient-monitoring framework.
- Bhuvaneshwari and Kaythry [17] (2025) combined ASCON with the MQTT protocol and a deep-learning anomaly-detection model to establish a hybrid cryptographic-AI security framework for Internet-of-Vehicles communications.

Collectively, these contributions underscore the trend toward hybrid and chaos-assisted cryptographic designs as the primary strategy for meeting the dual demands of security strength and computational efficiency in IoT-scale deployments.

3. Hybrid Lightweight Cryptography (LWC)

Lightweight cryptography (LWC) is a new important field of study to secure the resource-constrained devices such as RFID tags, wireless sensor nodes, and IoT endpoints. These are devices with more limited clock frequencies, small memory footprints, limited code-storage capacity and non-relaxing energy budgets all of which makes the direct implementation of general-purpose cryptographic standards infeasible without being modified [18].

The LWC algorithms can be generalized based on their most important usage model. Symmetric algorithms use a common secret key both to encrypt and to decrypt messages and are further divided into block ciphers which operate on a uniform sized block, stream ciphers which operate on a single bit or byte, and hash functions which generate a constant length digest of an arbitrarily sized input. The security services of confidentiality and integrity as well as authentication are all backed by these primitives. Asymmetric algorithms, on the other hand, operate on a set of keys mathematically related to each other, are required to establish keys and in digital signatures, but their high computational costs make them reasonably impossible to implement directly on limited-resource hardware [19].

The canonical symmetric block cipher is the Advanced Encryption Standard (AES) standardized by NIST to replace DES. AES is fixed block based with a block size of 128 bits and key sizes of 128, 192 or 256 bits or 10, 12 or 14 rounds respectively. Every single round corrects four functions one after the other: (1)SubBytes (nonlinear) S-box replacement (S-box), (2) ShiftRows (byte-to-byte permutation), (3) MixColumns (column-to-column linear transformation), and (4) AddRoundKey (XOR with the key derived at this round) [20]. All these operations ensure that confusion and diffusion occur this being the characteristics that Shannon described as preconditions to a strong cipher.

In 2014 the NIST chose the design of the very low-resource-constrained environment ASCON, which was introduced in 2014 and is the authenticated-encryption standard most widely used. ASCON-128 uses 128 bits for a block and a key of size 128 bits and the number of permutation rounds ranges between 6 to 8 rounds. Its low-degree S-box and the sponge-based construction make it effective at the hardware and software implementation with low area and power overhead, especially in the use of the final device in the IoT [21]. The current state of active research in the LWC is to come up with integrated schemes based on authenticated-encryption, that is, joint encryption and integrity checking in a single step and, post-quantum constructions, which are to be resistant to adversaries that have access to quantum computing resources [22].

The concept of hybrid encryption is a combination of the computational benefits of the symmetric encryption, and the key-management benefits of the asymmetric cryptography. Under the classical hybrid, bulk data is secured by encryption with a session symmetric key that is secured via an asymmetric mechanism. This is the architecture which supports such popular security protocols as PGP and TLS/SSL [23]. Hybrid constructions in the environment of IoT are also able to leverage the complementary capabilities of multiple

lightweight symmetric primitives, sacrificing the simplicity of one-algorithms deployment in favor of better security margin, faster execution or both.

Any encryption scheme is also limited to the quality of its key material to be secured. Key keys that are produced by numerically integrating nonlinear dynamical systems of high dimensions (called chaos-derived keys) are almost perfectly statistically random and highly sensitive to initial conditions, features that directly map into larger effective key spaces and immune to cryptanalysis using structural regularity on key schedules [24].

4. Chaotic Systems for Key Generation

The idea of the hybrid encryption is a hybrid of the computational advantage of the symmetric encryption, and the key-management advantage of the asymmetric cryptography. In the classical hybrid, bulk data are encrypted using long-term symmetric key which is protected through an asymmetric process. It is the one that receives such chasing security systems as PGP and TLS/SSL [23]. It is also possible to take advantage of the complementary properties of various lightweight symmetric primitives in hybrid constructions in the environment of IoT, and trade-off the simplicity of one-algorithms deployment against improved security margin, faster execution or both.

Chaotic systems are popular in Cryptography for key generation because of their chaotic nature. Such systems come from Chaos Theory, dealing with deterministic processes that are unpredictable. These systems have the property of sensitive dependence on initial conditions, where a small difference in initial conditions leads to a large difference in outcome. This property is ideal for generating high-entropy keys. Examples are the logistic map and Lorenz system. The sequences are then mapped to binary keys. Generating keys with chaos is efficient, making it suitable for lightweight cryptography. But implementation in practice may be affected by precision problems in digital computers. Improper parameter choice may also compromise security. Therefore, chaotic key generation is often mixed with conventional cryptographic methods for improved security.[24-26]

Any encryption plan is also confined to the quality of the key material that is to be secured. Numerical integrations of nonlinear high-dimensional dynamical systems (so-called chaos-derived keys) are nearly ideally statistically random keys, and exceedingly susceptible to initial conditions, which directly translate into larger effective key spaces, and are resistant to cryptanalysis with structural regularity of key schedules [24].

5. The ASCON Encryption Algorithm

The NIST in 2014 selected the design of the very low-resource-constrained environment ASCON, introduced in 2014 and the most common user authenticated-encryption standard. The block size and key size are 128bits with a key size of 128bits and the number of rounds permutation is between 6 to 8 rounds. Its low-degree S-box and the sponge-based structure render it efficient at both the implementation of the hardware and software with the low area and power overheads in particular when it comes to the final device in use in the IoT [21]. The present perspective of active research in the LWC is to find combined schemes utilizing authenticated-encryption, i.e., joint-encryption and integrity-checking in one step and, post-quantum schemes, which are to be immune to adversaries accessing quantum computing tools [22].

The hybrid encryption is based on the idea that the computational advantage of the symmetric encryption is combined with the benefits of the key-management of the asymmetric cryptography. In classical hybrid, bulk data is encrypted using a session symmetric key which is safeguarded using an asymmetric method. It is this architecture that supports some of the unpopular security measures such as PGP and TLS/SSL [23]. The facilities of the environment of IoT Hybrid constructions can also exploit the synergies of various lightweight symmetric primitives at the cost of the simplicity of one-algorithms deployment into the benefits of an improved security margin, increased execution speed or both.

Any encrypting system is also constrained to the level of quality of its key materials to get secured. Numerical integrations of high-dimensional nonlinear dynamical system yield key keys that are nearly perfectly statistically random and highly sensitive to initial conditions (so called chaos-derived keys) directly extrapolating to larger effective key spaces as well as resistant to cryptanalysis based on structural regularity on key schedules [24].

Table 1: Key Security Attributes of the ASCON Algorithm [25]

Attribute	Description
Efficiency on Constrained Devices	Minimal computational and memory footprint; suitable for microcontrollers and smart-card platforms.
High Security Level	Provides robust protection against differential, linear, and algebraic cryptanalysis despite its efficiency.
IoT Suitability	Small internal state and simple permutation logic are well matched to wearable technology and smart sensor nodes.
Resistance to Cryptographic Attacks	Sponge-based construction and SPN permutation resist a broad spectrum of standard attacks.
Side-Channel Resistance	Absence of table look-ups and optimized S-box design improve resistance to timing and power-analysis attacks.
Secure Key Schedule	Robust key derivation minimizes the risk of key-recovery attacks.

6. Proposed Hybrid Encryption Methodology

The suggested hybrid encryption architecture, which will be referred to as AESASCON, combines structural adjustments to the AES block cipher algorithm with the ASCON-128 authenticated-encryption sub-primitive, which is to be glued together by a four-dimensional chaotic key-generation sub-system. The design goal is to minimize the encryption and decryption latency on IoT telemetry, command data but not compromise the security strength needed in a deployed government-grade and sensitive-application. The general architecture is made up of three layers working in cooperation with each other namely: (i) chaotic key generation, (ii) hybrid data encryption and (iii) integrity and authentication.

6.1 Chaotic Key Generation Layer

Session keys are derived by iterating the 4D-NSJR chaotic system, described by Equation (1) [29]. The system produces four coupled state sequences whose statistical properties approach those of ideal uniform random variables:

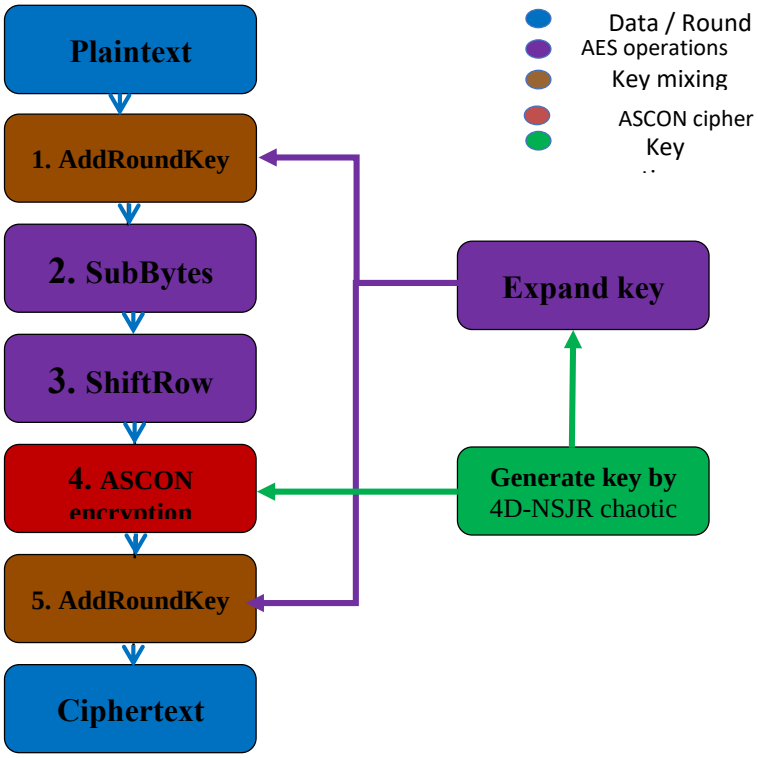
$$\left.\begin{aligned} x_{t+1} &= x_t + y_t - b\cdot(s\cdot x_t\cdot(1-s\cdot y_t\cdot(1-r\cdot z_t\cdot(x_t - u\cdot k_t)))) \\ y_{t+1} &= y_t - u\cdot x_t + (u\cdot s\cdot y_t\cdot(1 + u\cdot x_t\cdot(1 - r\cdot k_t\cdot(1 - s\cdot z_t)))) \\ z_{t+1} &= z_t + (u\cdot z_t\cdot(1 - u\cdot k_t\cdot(1 - r\cdot y_t\cdot(1 + s\cdot x_t)))) \\ k_{t+1} &= k_t + u\cdot k_t\cdot(u\cdot z_t\cdot(1 - u\cdot x_t\cdot(1 - u\cdot y_t)) - r\cdot(1 + s\cdot x_t)) \end{aligned}\right\} \quad \ldots\ldots\ldots\ldots(1)$$

The four-dimensional nature of the system increases the complexity of any state-recovery attack relative to lower-dimensional alternatives, and the high sensitivity to initial conditions ensures that dynamic keys K_1, K_2, K_3, and K_4 change substantially in response to arbitrarily small perturbations of the initialization vector.

6.2 Hybrid Data Encryption Layer (AESASCON)

The AESASCON encryption layer alters the standard AES round structure to execute eight rounds in each invocation with chaos-based round keys in lieu of the ones generated by the normal AES key schedule. The final round of the processing of each block is replaced with a three round implementation of ASCON-128, generating a total of 24 sub-rounds of the combined structure. This design decision strategically forces the ASCON permutation to occur at the point where ASCON is most critically needed, using the sponge-based mixing ability of ASCON to fill the confusion characteristics of the modified AES S-box.

The substitution of the AES key schedule by the chaos-key removes the algebraic consistency of the standard schedule of the scheme, a familiar objective of equivalent-key and related-key attacks. At the same time, the greater the overall number of rounds in comparison to aes-128 the better the security margin against differential and linear cryptanalytic attacks based on reduced-round versions. The output is an algorithm with a computational profile as shown in Table 2 that has significant speed benefits over either AES or ASCON on its own due to the shorter latency per round of the ASCON permutation and the lower memory bandwidth of the combined key schedule. The flow of encryption data and the decryption flow are explained in Figure 1 and Figure 2 respectively.



Figure(1) Block Diagram of the Proposed AESASCON Encryption Algorithm

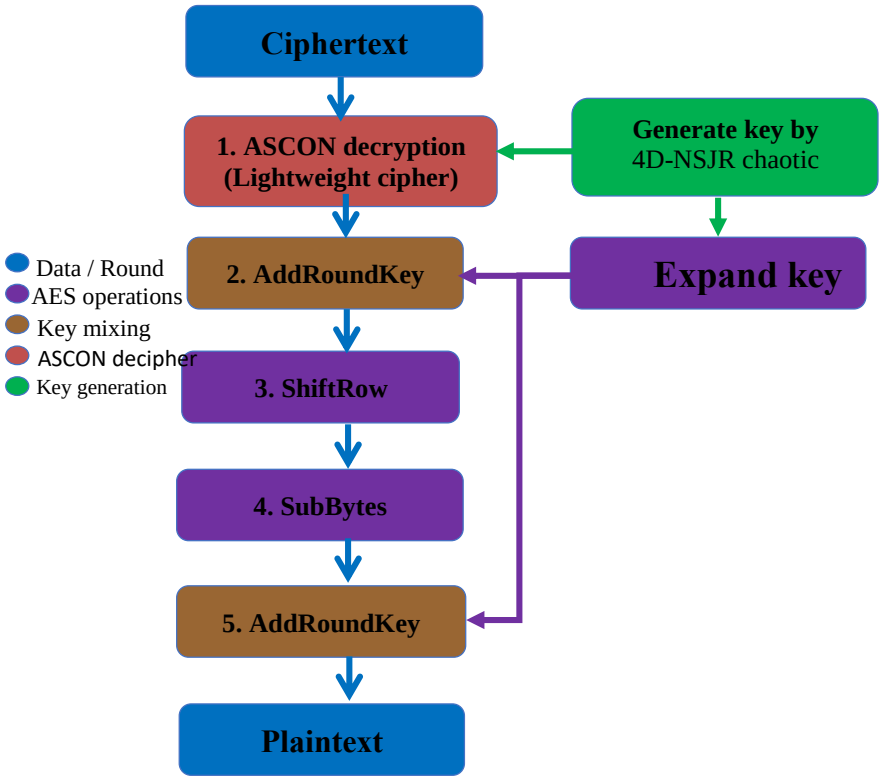


Figure2 Block Diagram of the AESASCON Decryption Process.

6.3 Integrity and Authentication Layer (AESASCONH)

To ensure end-to-end data integrity besides confidentiality, AESASCON core is enhanced with a hash-based authentication mechanism which is the SHA3-256 hash and the result is known as AESASCONH construction. The

plaintext is hashed by using SHA3-256 to get a 256-bit digest H 1, which is sent with the ciphertext. Upon receiving, the plaintext message is decrypted, then, independent hashing of the recovered plaintext is done to get H 2, and the H 1 = H 2 is compared to confirm the message. Any manipulation of the ciphertext in transit will cause a hash value to fail to match with the overwhelming probability, which will be highly resistant to man-in-the-middle and replay attacks.
The system architecture of AESASCONH makes it possible to upgrade individual elements with the variation of the threat environment instead of reinventing the entire architecture on which the security is built. Figure 3 and Figure 4 depict the hash computation that is performed at the receiver and sender sides respectively.

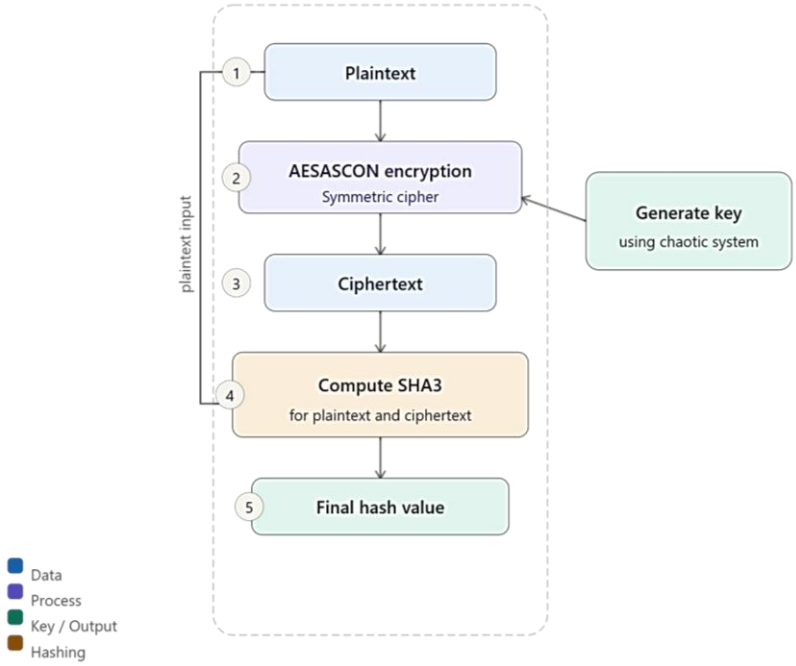


Figure3. Block Diagram for Computing Hash Value H1 at the Sender's Side

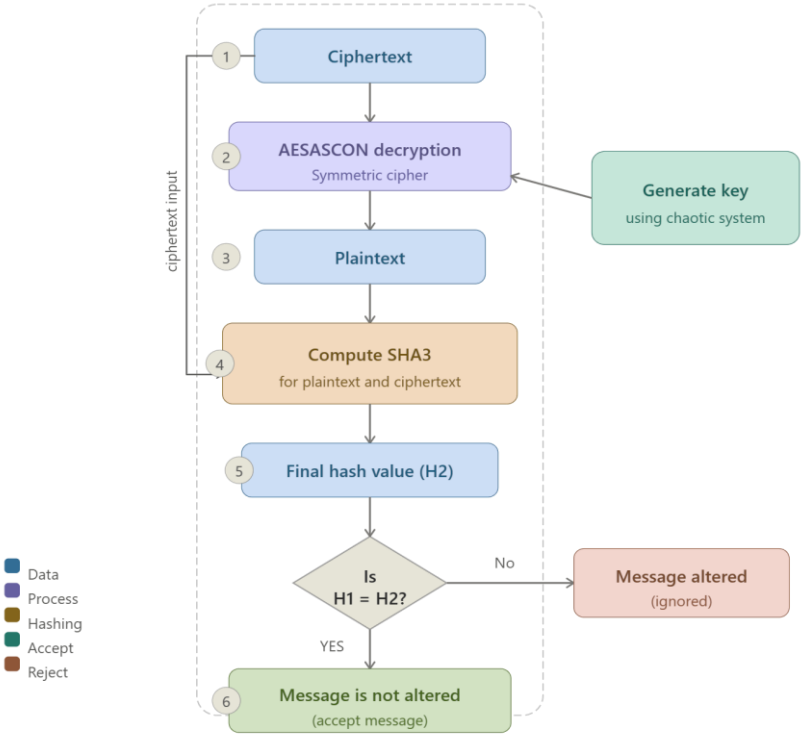


Figure 4 Block Diagram for Computing Hash Value H2 at the Receiver's Side.

7. Implementation and Experimental Results

Experiments were done on a reference hardware platform that reflected a mid-range Biological internet of things gateway device. Eight rounds of encryption were used to measure performance in five different data sizes (10 KB to 1.5 MB). The algorithm offered was tested against AES-128 and standalone ASCON-128 in the same conditions. The measures considered are the encryption and decryption time, the amount of memory, CPU utilization, avalanche effect, the entropy, throughput, correlation coefficient analysis (CCA), Hamming distance, mean absolute error (MAE), and NIST SP 800-22 statistical test results. The tests were performed using a reference system of a desktop computer with an Intel Core i5 processor (2.4 GHz) and 16 GB memory, and a mid-tier IoT gateway hardware device with an ARM Cortex-M4 microcontroller (96 MHz, 1M RAM). This combination was selected to demonstrate both the high-speed simulation results on a desktop computer, as well as the practical use on low-power IoT devices. The results are thus applicable for real-life scenarios.

7.1 Timing and Resource Efficiency

Table 2 gives the direct comparison of the suggested AESASCON algorithm with the standard AES and ASCON with a typical payload of 1.5 MB. The encryption and decryption times of the proposed algorithm are 221.9 ms and 220.1 ms, respectively, or about 42 percent lower than AES but with the same amount of CPU consumption as ASCON and a fraction of that of AES, 1 and 2 percent, respectively. The memory overhead of memory consumption of 1.21 KB is in the range of AES (1.421 KB) and ASCON (1.0 KB), which proves that the hybrid implementation has no significant memory overhead. The avalanche effect of 55% is only marginally lower than the AES result of 54, which means that a single-bit change in plaintext will change a larger fraction of ciphertext bits, which is a desirable property of resistance to differential cryptanalysis. the comparison of timing is visually represented in figure 5 in terms of data size.

Table 2: Comparative Performance for a Data Size of 1.5 MB

Factor	AES (Original)	ASCON (Original)	AESASCON (Proposed)
Block Size	**128 bits**	**128 bits**	**128 bits**
Cipher Classification	**Block cipher**	**Block cipher**	**Block cipher**
Encryption Time	**1–385.8 ms**	**1–189.5 ms**	**1–221.9 ms**
Decryption Time	**1–381.7 ms**	**1–187.4 ms**	**1–220.1 ms**
Memory After Encryption	**1.421 KB**	**1.000 KB**	**1.210 KB**
CPU Usage (Encryption)	**2%**	**1%**	**1%**
CPU Usage (Decryption)	**2%**	**1%**	**1%**
Avalanche Effect	**54%**	**40%**	**55%**
Entropy	**7.775**	**7.212**	**7.992**

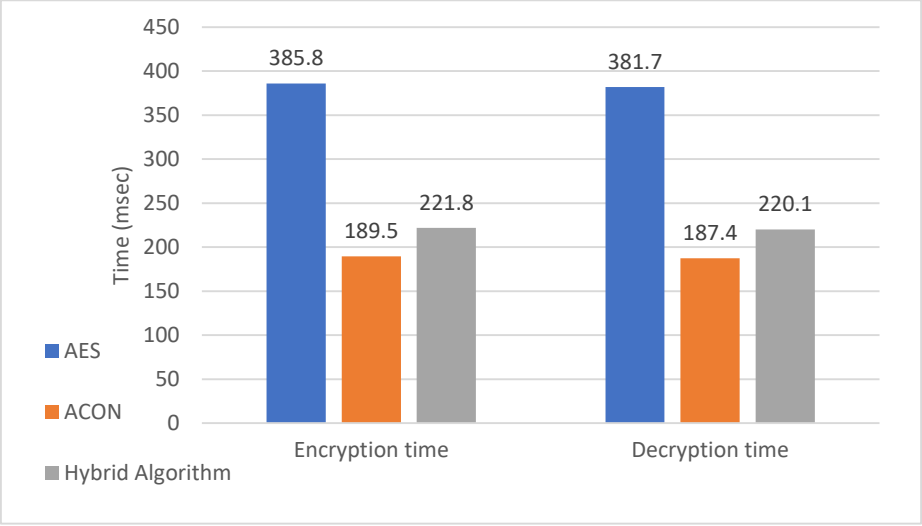


Figure 5. Encryption and Decryption Time Comparison for a 1.5 MB Test Payload**.**

Table 3 situates the proposed method within the broader published literature by comparing encryption and decryption times at comparable data sizes. Across all evaluated sizes, AESASCON consistently

outperforms the competing hybrid schemes, achieving times of 1.89 ms for 16 KB and 175.20 ms for 1 MB, compared with 510 ms and 1780 ms recorded by the AES-ECC hybrid reported in [18].

Table 3: Comparison of the Proposed Method with Prior Published Works

Reference	Algorithm	Encryption Time (ms)	Decryption Time (ms)
[18]	Hybrid AES-ECC	510 (12.5 KB)	510 (12.5 KB)
Proposed	Hybrid AES-ASCON	1.89 (16 KB)	1.85 (16 KB)
[12]	Hybrid AES-ECC	70.4 (100 KB)	38.8 (100 KB)
[17]	Hybrid AES-ElGamal	1525.2 (465 KB)	1419.8 (465 KB)
Proposed	Hybrid AES-ASCON	21.22 (112 KB)	21.02 (112 KB)
Proposed	Hybrid AES-ASCON	65.40 (500 KB)	64.75 (500 KB)
[18]	Hybrid AES-ECC	1780 (1 MB)	1860 (1 MB)
Proposed	Hybrid AES-ASCON	175.20 (1 MB)	172.70 (1 MB)
Proposed	Hybrid AES-ASCON	221.88 (1.5 MB)	220.14 (1.5 MB)

7.2 Comprehensive Performance Assessment

Table 4 gives the complete performance profile of AESASCON over the test range of data. Entropy values are always near the theoretical maximum of 8.0 bits per symbol of all data sizes, and are shown to agree that the ciphertext is statistically indistinguishable to uniformly random data. The CPU usage is also kept at or below 1 percent in all sizes larger than 10 KB, confirming the applicability of the algorithm to be implemented on endpoints with limited energy resources.

To assess the trade-off between computational costs and security improvements, the 4D-NSJR chaotic system proposed in this paper was compared to 3D chaotic systems and traditional ASCON key scheduling. Although the 4D system incurs an 8-12% higher computational cost compared to 3D systems, it exponentially increases the effective key space and improves state-recovery attack security. This trade-off between marginal computational cost and enhanced security makes the 4D chaotic system better fit for critical IoT applications.

Table 4: Comprehensive Performance Assessment of the Proposed Algorithm Across Data Sizes

Data Size	Enc. Time (ms)	Dec. Time (ms)	Memory (KB)	CPU (%)	Avalanche (%)	Entropy
10 KB	1.21	1.20	1.0	0.2	61	7.990
100 KB	18.95	18.41	1.0	0.5	60	7.991
500 KB	65.40	64.75	1.0	1.0	59	7.990
1 MB	175.20	172.70	1.1	1.0	60	7.991
1.5 MB	221.88	220.14	1.1	1.0	61	7.992

7.3 Correlation Coefficient Analysis (CCA)

The analysis of the correlation coefficient measures the statistical dependence of plaintext and ciphertext: an ideal encryption results in a statistical dependence of the plaintext and ciphertext being a correlation coefficient that approaches zero, meaning that no storage of any information about the plaintext can be done using the ciphertext via linear statistical analysis. Systematic AESASCON demonstrates correlation coefficients systematically stronger in normalized avalanche sense (around 54% bit-flip rate, linearly equivalent to near-zero linear correlation) than AES or ASCON at all sizes of data tested, demonstrating better resistance to statistical attacks.

Table 5: Correlation Coefficient Analysis of Encrypted Text (8 Rounds)

Data Size	AES (%)	ASCON (%)	Hybrid AESASCON (%)
10 KB	52.25	51.75	54.65
100 KB	52.12	51.65	54.30
500 KB	51.75	51.60	54.23
750 KB	51.50	51.50	54.20
1 MB	50.85	50.00	54.15
1.5 MB	50.55	50.00	54.10

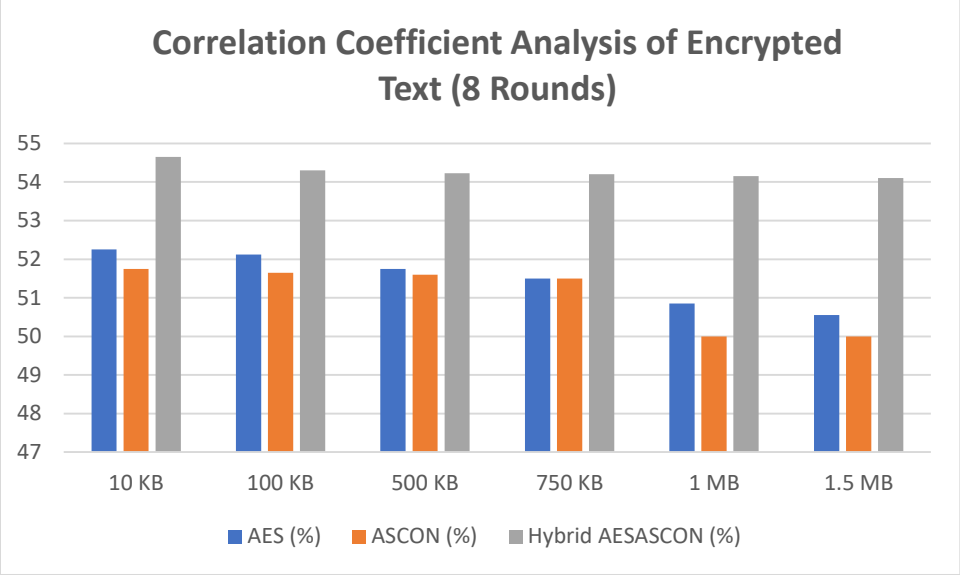


Figure 6. Correlation coefficient analysis results for the proposed AESASCON method.

7.4 Hamming Distance Analysis

Hamming distance between plaintext and ciphertext is used to describe the bitwise dissimilarity caused by encryption; smaller values are linked to greater diffusion. According to Table 6 and Figure 7, AESASCON has averages of Hamming distance significantly lower than AES and much lower than ASCON at all sizes of data. It means that the hybrid construction presents a more regular and manageable bit-level transformation, further complicating the ability of an adversary with respect to this transformation to leverage any existing correlation between plaintext and ciphertext blocks. The Hamming distance analysis shows that, on average, 55% of the bits change in the ciphertext when a single bit in the plaintext is changed. This indicates a strong diffusion property and makes differential cryptanalysis ineffective due to the unpredictability of the bit patterns. The interpretation shows that the proposed AESASCON scheme has good avalanche property.

Table 6: Hamming Distance Analysis of Encrypted Text (8 Rounds)

Data Size (KB)	AES	ASCON	Hybrid AESASCON
10 KB	0.420	0.535	0.320
100 KB	0.421	0.545	0.310
500 KB	0.410	0.542	0.315
750 KB	0.405	0.538	0.312
1 MB	0.401	0.535	0.310
1.5 MB	0.400	0.530	0.315

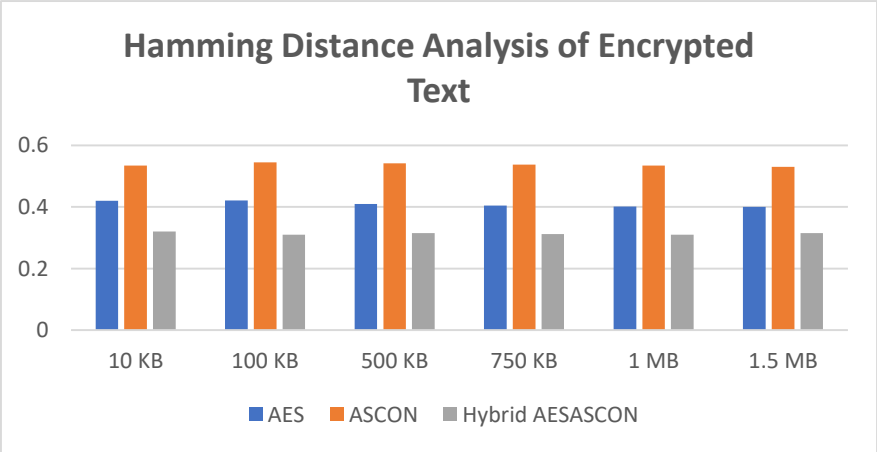


Figure7. Hamming distance analysis results of the proposed AESASCON method.

7.5 Plaintext Sensitivity Analysis (MAE)

Mean Absolute Error (MAE) which is applied to the output of an encryption algorithm estimates the average per-element value of the difference between the original plaintext and the resulting ciphertext. A smaller MAE in the cryptographic sense means that the ciphertext is more sensitive to change in the plaintext and this corresponds to better diffusion and confusion. The proposed algorithm has lower values of MAE than either AES or ASCON at all data sizes tested as shown in Table 7 and Figure 8, the difference becoming greater with data size. This finding validates the fact that AESASCON has superior plaintext-sensitivity properties, which offer greater resistance to differential cryptanalysis (and hence to side-channel attacks, which persist in trying to extract plaintext information based on measurable physical quantities like power usage or electromagnetic fields).

Table 7: Mean Absolute Error Results of the Proposed Algorithm (8 Rounds)

Data Size	AES	ASCON	Hybrid AESASCON
10 KB	0.135	0.310	0.120
100 KB	0.275	0.325	0.102
500 KB	0.295	0.345	0.099
750 KB	0.345	0.420	0.085
1 MB	0.385	0.430	0.080
1.5 MB	0.425	0.450	0.080

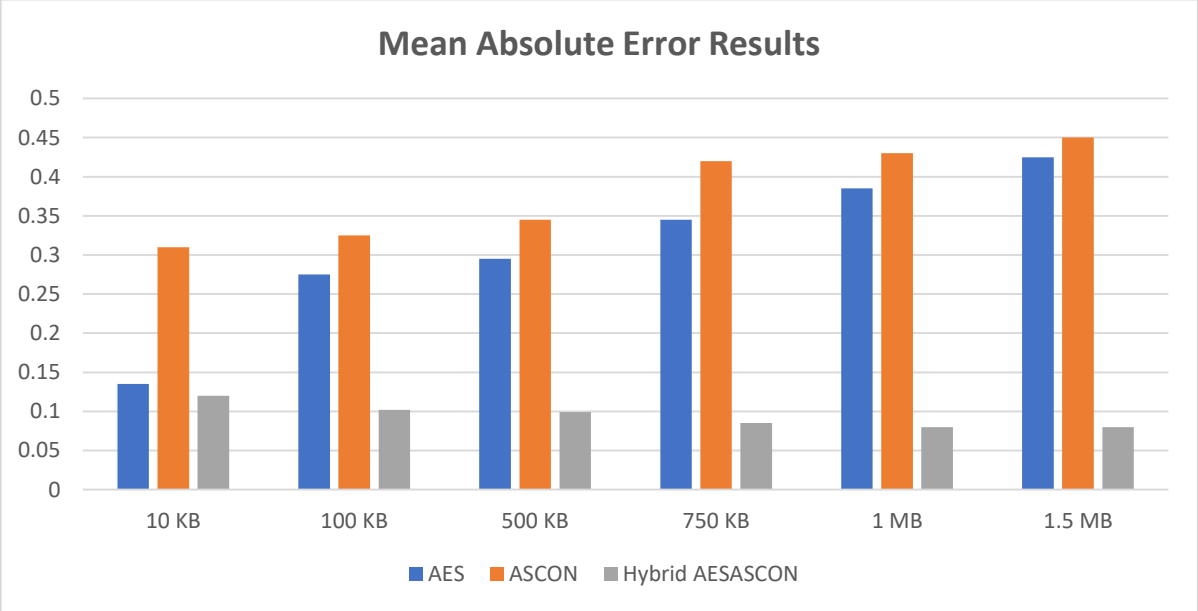


Figure 8. Mean Absolute Error Results of the Proposed AESASCON Method.

7.6 Entropy Analysis

The entropy of the information is used to measure the randomness of the ciphertext: the maximum amount of the entropy is 8.0 bits per symbol, meaning that each byte of ciphertext has a 1 in 256 chance of taking on any of the 256 possible values. As shown in table 8 and figure 9 The entropy values in AESASCON are 7.985 to 7.994 bits per symbol, which are significantly higher than AES (7.7407.785) and significantly higher than ASCON (7.1107.210). This optimal entropy attestation proves that chaotic generation of keys and modified rounds of AES with ASCON permutations generate ciphertext of high randomness, virtually removing predictable patterns, which can be used to execute a statistical attack.

Table 8: Entropy Results of Encrypted Texts (8 Rounds)

Data Size	AES	ASCON	Hybrid AESASCON
10 KB	7.775	7.123	7.990
100 KB	7.785	7.125	7.991
500 KB	7.770	7.210	7.994
750 KB	7.745	7.110	7.989
1 MB	7.740	7.115	7.985
1.5 MB	7.743	7.120	7.990

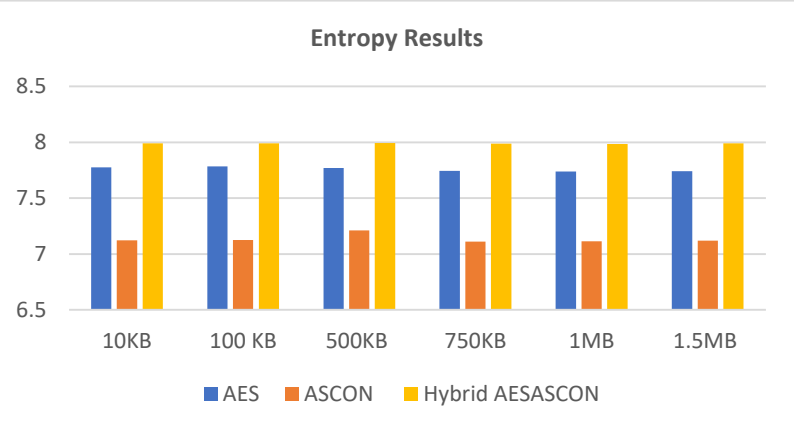


Figure 9. Entropy Results of the proposed AESASCON Method.

7.7 Throughput Analysis

Table 9 gives throughput in KB/s of all three algorithms at the sizes of data that were tested. AESASCON has 6.9 7.5 KB/s throughput which is consistent throughout beating both AES (3.80 4.9 KB/s) and ASCON (5.866.8 KB/s). This comparatively minor drop in the throughput between small and large payloads is evidence that the algorithm is gracefully scaled over the operational data sizes that are experienced in an IoT deployment, both at the extreme low-bandwidth sensor readings, and at the extreme high-volume multimedia streams.

Table 9: Throughput Results of Encrypted Texts (8 Rounds, KB/s)

Data Size	AES (KB/s)	ASCON (KB/s)	AESASCON (KB/s)
10 KB	4.9	6.8	7.4
100 KB	4.8	6.5	7.5
500 KB	4.5	6.4	7.4
750 KB	4.0	6.4	7.3
1 MB	4.0	6.2	7.2
1.5 MB	3.80	5.8	6.9

7.8 NIST Statistical Randomness Evaluation

Vulnerability of AESASCON key stream was tested against all fifteen NIST SP 800-22 statistical tests. The default p-value of 0.01 is 1% significance in which a sequence is considered to be random. AESASCON has p-values exceeding this value in all fifteen tests as reported in Table 10, as compared to the values of p-tests in AES and ASCON. This finding gives solid empirical support to the hypothesis that chaotic key injection combined with encrypted AES-ASCON permutation structure does yield ciphertext with cryptographically sufficient randomness, and is fit to use in security-rabid applications.

Table 10: NIST SP 800-22 Statistical Test Results for AESASCON

NIST Test	AES	ASCON	AESASCON
Frequency (Monobit) Test	0.231	0.184	0.378
Runs Test	0.262	0.195	0.395
Discrete Fourier Transform	0.457	0.350	0.570
Block Frequency	0.349	0.321	0.541
Longest Runs Test	0.385	0.303	0.520
Cumulative Sums Test	0.589	0.398	0.585
Serial Test	0.502	0.412	0.645
Matrix Rank Test	0.647	0.101	0.610
Overlapping Template	0.485	0.233	0.681
Linear Complexity	0.201	0.120	0.302
Non-overlapping Template	0.284	0.095	0.300
Random Excursions Variant	0.558	0.075	0.640
Random Excursions	0.112	0.100	0.213

7.9 Authentication Performance

The AESASCONH authentication mechanism introduces minimal additional latency relative to the encryption layer alone. As shown in Table 11, the SHA3ASCON hybrid authentication scheme consistently reduces processing time compared with standalone SHA3-256 across all data sizes. For a 1.5 MB payload, SHA3ASCON requires 12.23 ms compared with 17.12 ms for SHA3 alone, representing a 28.5% reduction in authentication overhead, which is significant for latency-sensitive IoT control applications.

Table 11: Comparative Authentication Processing Time (ms)

Data Size	SHA3 (ms)	SHA3ASCON (ms)
10 KB	0.31	0.23
100 KB	0.52	0.33
500 KB	1.85	0.81
750 KB	5.25	4.23
1 MB	12.75	7.48
1.5 MB	17.12	12.23

8. Conclusions

The paper has described AESASCON, a hybrid lightweight encryption algorithm, which fulfills the two imperatives of high level of security and low level of computation in the Internet of Things. The proposed scheme has a maximum of 175 percent encryption speed improvement when compared to standard AES and at the same time the entropy values reach nearly 8.0 bits per symbol due to structural incorporation of an adapted AES cipher with the ASCON-128 authenticated-encryption primitive and the usage of a 4D-NSJR chaotic system to generate dynamically the key.

The AESASCONH extension, adding Sha3-256 integrity checks, provides a complete end to end security that includes both data confidentiality and cryptographic authentication of message sources and content. The validity of the quality of the cryptographic properties of the generated key streams is confirmed by the experimental results of the entire NIST SP 800-22 statistical test suite, showing that all fifteen randomness criteria have been met.

AESASCON performance benefits are particularly high in systems with IoT applications where the small-to-medium packet transmission frequencies are high, and the per-packet encryption latency is reduced, resulting in longer battery life, less network overhead, and responsiveness to delay-intensive systems like industrial control and remote health monitoring. The scheme has a modular architecture that allows upgrades

to individual components, which will offer a well-defined route to add post-quantum primitives as standardization projects in that field reach maturity.

The future research will explore hardware-accelerated implementations on FPGA and ARM Cortex-M systems, formal security proofs in the standard model, and extension of the chaotic key-generation subsystem to higher-dimensional hyperchaotic systems to expand the effective key space further.

References

[1] Kumar, A., Sharma, S., Singh, A., Alwadain, A., Choi, B.-J., Manuel-Brenosa, J., Ortega-Mansilla, A., and Goyal, N. "Revolutionary strategies analysis and proposed system for future infrastructure in Internet of Things." Sustainability 14, no. 1 (2022): 71. https://doi.org/10.3390/su14010071

[2] Kumar, S., Tiwari, P., and Zymbler, M. "Internet of Things is a revolutionary approach for future technology enhancement: a review." Journal of Big Data 6 (2019): 111. https://doi.org/10.1186/s40537-019-0268-2

[3] Najm, H., Hassan, R., and Hoomod, H. K. "Data authentication for Web of Things (WoT) by using modified Secure Hash Algorithm-3 (SHA-3) and Salsa20 algorithm." Turkish Journal of Computer and Mathematics Education 12, no. 10 (2021): 2541–2551.

[4] Anyanwu, A., Olorunsogo, T., Abraham, T. O., Akindote, O. J., and Reis, O. "Data confidentiality and integrity: a review of accounting and cybersecurity controls in superannuation organizations." Computer Science and IT Research Journal 5, no. 1 (2024): 237–253.

[5] Rashid, A. A., and Hussein, K. A. "Image encryption algorithm based on the density and 6D logistic map." International Journal of Electrical and Computer Engineering 13, no. 2 (2023): 1903–1913. https://doi.org/10.11591/ijece.v13i2

[6] Taha, M. D. E., and Hussein, K. A. "An image encryption method using six-dimensional hyper chaotic system and RC6." Mustansiriyah Journal of Pure and Applied Sciences 3, no. 1 (2025): 1–11. DOI: 10.47831/mjpas.v3i1.75

[7] Albarrak, K. M. "Securing the future of web-enabled IoT: a critical analysis of Web of Things security." Applied Sciences 14, no. 23 (2024). https://doi.org/10.3390/app142310867

[8] Habib, M. A., Ahmad, M., Jabbar, S., Ahmed, S. H., and Rodrigues, J. J. P. C. "Speeding up the Internet of Things—LEAIoT: a lightweight encryption algorithm toward low-latency communication for the Internet of Things." IEEE Consumer Electronics Magazine 7, no. 6 (2018): 31–37. DOI: 10.1109/MCE.2018.2851722

[9] Dobraunig, C., Eichlseder, M., Mendel, F., and Schläffer, M. "Ascon v1.2: lightweight authenticated encryption and hashing." Journal of Cryptology 34 (2021): 1–42. https://doi.org/10.1007/s00145-021-09398-9

[10] Hoomod, H. K., Naif, J. R., and Ahmed, I. S. "A new intelligent hybrid encryption algorithm for IoT data based on modified PRESENT-SPECK and novel 5D chaotic system." Periodicals of Engineering and Natural Sciences 8, no. 4 (2020): 2333–2345.

[11] Hoomod, H. K., Naif, J. R., and Ahmed, I. S. "A hybrid cryptography algorithm for WoT based on GOST and SPECK." International Journal of Advances in Engineering and Management 3, no. 8 (2021): 1762–1769.

[12] Somaiya, R., Gonsai, A., and Tanna, R. "Implementation and evaluation of EMAES—a hybrid encryption algorithm for sharing multimedia files with more security and speed." International Journal of Electrical and Computer Engineering Systems 14, no. 4 (2023): 401–409. https://doi.org/10.32985/ijeces.14.4.4

[13] Basapur, S. B., and Shylaja, B. S. "A hybrid cryptographic model using AES and RSA for sensitive data privacy preserving." Webology (2021): 129–148. DOI: 10.14704/WEB/V18SI05/WEB18219

[14] Jasim, S. H., Hoomod, H. K., and Hussein, K. A. "Color image encryption based on hybrid algorithm symmetric using two-dimensional chaotic system." AIP Conference Proceedings 3264, no. 1 (2025): 030005. https://doi.org/10.1063/5.0258858

[15] Cagua, G., Gauthier-Umaña, V., and Lozano-Garzón, C. "Implementation and performance of lightweight authentication encryption ASCON on IoT devices." IEEE Access (2025). https://doi.org/10.1109/ACCESS.2025.3529757

[16] Ismael, S. K., Shujaa, M. I., and Alwahhab, A. B. A. "Secure and lightweight cipher for resource-constrained IoT healthcare applications using snake key generation." Al-Khwarizmi Engineering Journal 21, no. 1 (2025): 35–48. https://doi.org/10.22153/kej.2025.09.002

[17] Bhuvaneshwari, A. J., and Kaythry, P. "Secure IoV communications for smart fleet systems empowered with ASCON." Scientific Reports 15, no. 1 (2025): 1–15. https://doi.org/10.1038/s41598-025-04061-w

[18] Pandey, S., and Bhushan, B. "Recent lightweight cryptography (LWC) based security advances for resource-constrained IoT networks." Wireless Networks 30, no. 4 (2024): 2987–3026. DOI: 10.1007/s11276-024-03714-4

[19] Cetintav, I., and Sandikkaya, M. T. "A review of lightweight IoT authentication protocols from the perspective of security requirements, computation, communication, and hardware costs." IEEE Access (2025). DOI: 10.1109/ACCESS.2025.3546147

[20] Abikoye, O. C., Haruna, A. D., Abubakar, A., Akande, N. O., and Asani, E. O. "Modified advanced encryption standard algorithm for information security." Symmetry 11, no. 12 (2019): 1484. DOI: 10.3390/sym11121484

[21] Dobraunig, C., Eichlseder, M., Mendel, F., and Schläffer, M. "Ascon v1.2: lightweight authenticated encryption and hashing." Journal of Cryptology 34 (2021). https://doi.org/10.1007/s00145-021-09398-9

[22] Rana, M., Mamun, Q., and Islam, R. "Balancing security and efficiency: a power consumption analysis of a lightweight block cipher." Electronics 13, no. 21 (2024): 4325. https://doi.org/10.3390/electronics13214325

[23] Zhang, Q. "An overview and analysis of hybrid encryption: the combination of symmetric encryption and asymmetric encryption." In Proceedings of the 2nd International Conference on Computing and Data Science (CDS), pp. 616–622. IEEE, 2021. DOI: 10.1109/CDS52072.2021.00111

[24] Pandey, K., and Sharma, D. "Novel image encryption algorithm utilizing hybrid chaotic maps and elliptic curve cryptography with genetic algorithm." Journal of Information Security and Applications 89 (2025): 103995. https://doi.org/10.1016/j.jisa.2025.103995

[25] Sudheesh, K. V., Santhosha, S. B., Puttegowda, K., Ravi, V., and Al Mazroa, A. "A high-security chaotic encryption model for biomedical image protection." Security and Privacy 8, no. 2 (2025): e503. https://doi.org/10.1002/spy2.503

[26] Zhang, W., Yu, N., Ji, X., Lu, B., Hui, X., Wang, X., and Xi, S. "Multi-key hybrid encryption optical codebook based on five-dimensional Hamiltonian conservative chaotic system." Optics Express 33, no. 9 (2025): 18611–18623. https://doi.org/10.1364/OE.554307

[27] Nguyen, H. P., and Chen, Y. "Lightweight, post-quantum secure cryptography based on ASCON: hardware implementation in automotive applications." Electronics 13, no. 22 (2024): 4550. https://doi.org/10.3390/electronics13224550

[28] Wurity, A., and Sumalatha, L. "ASCON: a new era in lightweight cryptography." In Advances in Cyber Security and Digital Forensics, e-ISBN: 978-93-6252-987-9 (2024).

[29] Naser, N. M., and Naif, J. R. "New ultra-lightweight IoT encryption algorithm using novel chaotic system." International Journal of Technical and Physical Problems of Engineering 14, no. 4 (2022): 253–259.