International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

OPTIMIZATION OF CRYPTOGRAPHIC MODEL UTILIZING MODERN BALANCING SWARM ALGORITHM

Swathika P[1*], Vinoth Kumar. B[2]

([1] Assistant Professor, Department of Artificial Intelligence and Data Science, Mepco Schlenk Engineering College, Sivakasi, Tamil Nadu, India. Email id: swathikap192@gmail.com) (* - Corresponding author)

([2] Assist`ant Professor, Department of Computer Applications, Ayya Nadar Janaki Ammal College, Sivakasi, Tamil Nadu, India. Email id: vinothkumaranjac@gmail.com)

Abstract

The quick development of cloud computing (CC) in recent decades has raised questions regarding the energy and security needs of cloud data centers. This article proposes a new combined paradigm to address the issues of data security and energy consumption. For efficient data security, the lightweight cryptography (LWC) technique can be offered. To increase the well-secured concept by optimizing task balancing, the new augmented LWC (ALWC) technique is submitted. The new key is optimized well through balancing swarm optimization algorithm (BSOA). It also generates a public key with a new pseudo-random key. A 32-bit plaintext is encrypted using a 64-bit key in a cipher, which is then put into practice and examined. The cipher model is implemented using the MATLAB software implementation tool, and its entropy and histogram can be examined.

Keywords: Cloud computing, light weight cryptography, compression, encryption, balanced optimizer, performance analyses.

1. INTRODUCTION

Over the past few decades, internet-based user communication has seen a significant increase. As a result, more customers are utilizing data, leading to a rise in the sharing of sensitive and private information. However, ensuring the security of this data, especially when stored in the cloud, remains a critical issue. The evolution of distributed computing technology has given rise to various architectures and infrastructures, including cloud computing, which provides remote internet-dependent services such as applications, data storage, and infrastructure [1].

Cloud computing offers several advantages, including pay-as-you-go services, dynamic scaling, and reduced upfront capital and overhead costs. Security in cloud service providers (CSPs) is often ensured through encryption techniques, especially symmetric encryption methods [2]. However, despite its benefits, cloud infrastructure still faces challenges related to scalability, multi-tenancy, and interoperability, with security being a primary concern [3].

Cryptography demonstrates a vital role in addressing security issues in CC, as it involves encrypting plaintext data to guarantee secured storage and transmission. By employing encryption and decryption processes, cryptography guarantees that only authorized

Received: August 13, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

individuals can access sensitive facts [4–6]. As cloud environments are susceptible to various security threats, such as network attacks and unauthorized access, cryptography emerges as a successful method for securing data transfer [7].

Cloud services encompass a wide range of applications, including email, online file storage, business applications and social networking. Key features comprise controlled access, and on-demand self-service extensive network connectivity and resource pooling [8] of CC. Despite its advancements, the security of cloud infrastructure remains a significant concern, particularly regarding data outsourced to the cloud. Network security and secure connections between CSPs and users are critical areas of focus, with cryptography being a primary solution [9, 10].

The development of LWC has become essential, particularly for cloud-based Internet of Things (IoT) devices. The devices may often have less memory, and battery life, creating sophisticated encrypting skills challenging to implement. LWC algorithms, such as symmetric key encryption with smaller key sizes, offer a solution to this challenge, ensuring data protection and secure communication in resource-constrained devices. Additionally, LW encryption techniques are proposed for encrypting multimedia data generated by IoT devices, further enhancing data security [12-14].

- ***Problem Description and Motivation***

The complexity of encryption techniques, coupled with resource constraints in IoT devices, poses challenges for ensuring data security in cloud environments. Limited processing power, memory, and battery life hinder the implementation of sophisticated encryption methods. To address these challenges, LW encryption techniques are proposed, leveraging algorithms optimized for resource-constrained devices [15]. Also, an uneven task that causes SLA (service level agreement) violations and performance deterioration is caused by the erratic and unstable pace of client requests and the virtual machines (VM)s' varying resource usages. Moreover, the unbalanced cloud servers result in poor resource usage, higher power consumption, slower reaction times, and lower throughput. Therefore, to balance the load on cloud servers and enhance their overall performance, an efficient load balancing technique is needed [8]. Furthermore, by examining the weaknesses present in the cloud modules, the outsourced data are the vital components in the cloud computing environment that are subject to several risks and attacks. Compression-related concepts are also explored to mitigate memory consumption and enhance data security in cloud-based IoT devices [16, 32].

- ***Main Contribution***

This study introduces a new LWC to enhance data security in cloud computing environments. ALCA employs symmetric cryptography for data encryption and introduces a novel key generation technique. Additionally, data compression techniques, such as principal component analysis (PCA), are employed to reduce memory storage and transmission costs. The proposed algorithm, coupled with efficient key generation procedures, aims to improve network security and outperform existing encryption methods in cloud environments [17-19].

Received: August 13, 2025

International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

This application requires a strong cryptography or encryption technique to safeguard the cloud data that is being outsourced. In this article, a novel paradigm is proposed to address the problems with cloud data security that are outsourced. The following is a list of this study's primary contributions:

- To develop BSOA technology boosts system resource usages while significantly lowering energy consumption.
- To effectively guarantee the privacy and integrity of cloud data, the developed ALWC algorithm creates pseudorandom keys with a public key for encryption and decryption of outsourced data.
- To balance the tasks among high and low tasks in VM for effective resource allocation.
- To analyse encryption-decryption comparison time, energy consumption, and execution time are all taken into consideration while examining the effectiveness of the suggested ALWC model.

The following part briefly explains the related concepts of LWC in various environment with the current estimations.

2. LITERATURE SURVEY

Cloud computing has revolutionized modern information technology, influencing nearly every domain—from enterprise services to personal data management. However, with this revolution comes the enduring challenge of data confidentiality and integrity, particularly in outsourced and distributed environments [26]. Strategies for ensuring cloud data security have evolved to include encryption, data masking, backup mechanisms, and erasure coding [Gadde et al., 2023], yet encryption remains the most reliable and widely adopted method for preventing unauthorized access [27].

2.1 Cryptographic Approaches in Cloud Security

A variety of encryption paradigms have been proposed to strengthen cloud data protection. Hybrid cryptography models that combine symmetric and asymmetric schemes enhance both encryption speed and key management efficiency. For example, Elliptic Curve Cryptography (ECC) has been extensively applied due to its shorter key size [28] and high level of security (Ullah et al., 2023). However, ECC and similar algorithms often incur high computational costs, limiting their suitability for lightweight or IoT-based cloud applications.

To mitigate such limitations, researchers have explored lightweight cryptography (LWC) schemes, designed specifically for environments with constrained resources. SIMON and SPECK ciphers, developed by the NSA, are notable examples that use simple ARX (Addition–Rotation–XOR) operations to minimize hardware complexity and power consumption. Despite their hardware efficiency, they demonstrate reduced flexibility and are susceptible to differential and linear cryptanalysis when applied in high-performance or multi-tenant cloud systems.

On the other hand, DNA-based cryptography has introduced biological principles, such as sequence encoding and parallel computation, to enhance randomness and resistance to brute-force attacks [36]. Yet, DNA-based schemes tend to be computationally intensive and require

Received: August 13, 2025

International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

specialized implementation, reducing their practicality in large-scale or real-time cloud scenarios.

These findings reveal that while existing LWC models excel in either computational simplicity or security robustness, few achieve both concurrently, particularly in cloud environments that demand scalability, energy efficiency, and dynamic task balancing.

2.2 Architectural Enhancements and Security Models

Several architectural frameworks have also been proposed to enhance cloud data protection. Crypto Membranes (Mohamed KM et al., 2017) provide client-side encryption barriers to isolate users from servers, ensuring data confidentiality before transmission. Likewise, intrusion detection systems (IDSs) and authentication loggers (Belchior, 2019) offer layered protection but often increase processing overhead and latency. In hybrid cloud infrastructures, Attribute-Based Encryption (ABE) and its extended model, Dynamic Attributes Supporting (ABE-DAS), allow fine-grained access control through structured and unstructured data management (Zobaed et al., 2022). Nevertheless, these models struggle with key management scalability and policy update delays, especially when multiple users dynamically access shared data [29-31].

2.3 Lightweight and Compressive Techniques

Recent studies have also integrated compressive sensing (CS) techniques with LWC to optimize data collection and transmission in distributed wireless sensor networks (WSNs) [32]. By combining compression and encryption, these approaches reduce memory consumption and communication overhead. However, traditional CS-based models often neglect adaptive key optimization and task load balancing, resulting in suboptimal performance in large-scale cloud systems.

Recent advancements include the development of new LWC algorithms designed specifically for cloud data security (Gunathilake et al., 2019). These algorithms aim to reduce encryption complexity while ensuring robust data protection. Moreover, LW encryption techniques tailored for network devices have been proposed, utilizing key sizes and block ciphers optimized for resource-constrained environments [33].

Two layers with logic operations and a homomorphic model make up the new LWC encryption technique [34]. It has undergone experimental validation for known-plaintext, encrypted text only, brute force, and differential cryptanalysis attacks. They have been verified on a range of data comprising special characters and whitespace. The LW cipher family includes the SIMON cipher modified, the addition-modulo, rotation, and EX-OR (ARX) operations, as well as a new LW key generation algorithm [35]. These are implemented and analyzed across both software and hardware environments. The software implementation is carried out using MATLAB, where the cipher's performance is evaluated based on key security metrics such as the correlation coefficient, entropy, histogram uniformity, avalanche criterion, and key sensitivity. For hardware realization, the corresponding Verilog code is developed and simulated using Xilinx Vivado, followed by FPGA synthesis on Artix-7 and Basys-3 boards. This dual-platform implementation

Received: August 13, 2025

International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

facilitates a comprehensive evaluation of both computational efficiency and hardware feasibility, ensuring the cipher's suitability for real-time, lightweight cryptographic applications in IoT and embedded systems.

LWC technique based on DNA is enhanced by optical computing to attain the finest possible balance among security, unpredictability, and performance. This will be especially relevant for IoT devices that need real-time online encryption [36]. However, since conventional techniques have proven to be ineffective, DNA-based cryptography offers the advantage of using stochastic key generation, which makes it difficult to cryptanalyze due to its high degree of randomness

2.4 Comparative Analysis and Research Gap

Table-driven and algorithmic analyses from prior work demonstrate that no existing LWC method fully addresses the triangular challenge of security, energy efficiency, and computational balance. SIMON ciphers offer lightweight processing but are vulnerable to specific attacks; DNA-based methods are secure but computationally heavy; ABE schemes ensure flexible access control but suffer from high key management overhead. In contrast, the proposed ALWC model leverages BSO for adaptive key generation, achieving lower computational complexity ($O(n \log n)$) and enhanced resistance to brute-force and differential attacks through entropy-driven randomness.

Specifically, ECC provides strong security but involves higher key generation and encryption overhead due to its elliptic curve arithmetic, while ABE-DAS offers flexible access control but suffers from scalability and computation latency in large datasets. This comparative synthesis now clarifies the efficiency and robustness advantages of the proposed model over traditional cryptographic frameworks.

To bridge this gap, the proposed ALWC model introduces a BSOA to generate pseudorandom public keys while distributing computational tasks dynamically across virtual machines. This hybrid mechanism enhances entropy, key unpredictability, and resource utilization, achieving a balanced trade-off between security performance and energy consumption.

The proposed BSOA-ALWC model can be extended to large-scale IoT and cloud infrastructures. In particular, Gunathilake et al. (2019) emphasized the necessity of lightweight, energy-efficient cryptographic models that can adapt to heterogeneous device capacities and network topologies. Accordingly, the proposed model's dynamic swarm adjustment and low-power ALWC mechanism enable efficient encryption across diverse IoT nodes and cloud tiers without compromising throughput or latency. This adaptability supports real-world deployment in smart healthcare, industrial IoT, and multimedia cloud systems, where secure, scalable, and resource-aware encryption is crucial.

Several LWC algorithms have been developed to ensure data security in resource-constrained environments such as cloud-integrated IoT systems. For instance, the SIMON cipher family utilizes simple bitwise operations (AND, rotation, and XOR) to achieve hardware efficiency.

International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

However, despite its low computational cost, SIMON's limited flexibility and vulnerability to certain differential attacks restrict its applicability in highly dynamic cloud environments.

Similarly, DNA-based cryptography has gained attention for its inherent randomness and parallelism, offering enhanced resistance to brute-force and cryptanalytic attacks. Yet, DNA-based techniques often demand complex encoding and higher processing resources, making them less practical for lightweight or real-time applications.

These observations suggest that while existing LWC models provide either computational efficiency or strong unpredictability, they often fail to balance both under cloud workloads. In contrast, the proposed ALWC approach integrates a BSOA for key generation, enabling dynamic task balancing and improved resistance to cryptanalytic attacks with minimal energy overhead. This combination aims to overcome the trade-offs between security strength and computational efficiency observed in prior LWC methods.

Synthesizing these findings reveals the need for advanced encryption techniques that leverage LW models and optimized key generation methods to address emerging challenges in cloud data security. The proposed modern LWC-based approaches hold promise for overcoming existing limitations and ensuring robust data protection in cloud environments.

2.5 Summary of analysis

In summary, prior research establishes the foundation for lightweight and secure encryption models but lacks integration between security optimization and resource-aware computation. The proposed ALWC-BSOA paradigm aims to unify these objectives, providing a cryptographic model that adapts to varying workloads, minimizes energy waste, and strengthens data protection against modern cryptanalytic attacks.

3. SECURITY ISSUES IN CC

CC security involves protecting data, applications, and infrastructure from diverse threats and attacks. The various cryptographic attacks are explained briefly. Some of them are Brute-force, differential, statistical, side-channel, quantum, known-plaintext and chosen-plaintext attacks.

A brute-force attack involves systematically checking all possible keys until the correct one is found. The resistance of a cipher against this attack depends on its key size. Differential attacks analyze how differences in plaintext affect the resulting cipher text differences. In statistical attacks, adversaries exploit statistical redundancies in cipher texts, such as uneven histograms or non-uniform entropy, to deduce plaintext patterns. Side-channel attacks exploit information leaked from the physical implementation of a cryptosystem, such as power consumption, electromagnetic radiation, or timing variations. In known- and chosen-plaintext, attackers may have access to pairs of plaintexts and corresponding cipher texts (known-plaintext) or may choose plaintexts to be encrypted (chosen-plaintext). The quantum attack computers can exploit algorithms like Grover's (reduces key search from 2^n to $2^{n/2}$) and Shor's (breaks public-key algorithms such as RSA or ECC).

Received: August 13, 2025

International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Key aspects of cloud security include infrastructure security, software security, network security, and storage security without much attack. Trust is a critical component of cloud security, as users rely on CSPs to ensure the integrity, confidentiality and accessibility of those data.

While CC offers several advantages, it also introduces unique security concerns. Data persistence with multi-tenancy and application security is the certain challenges associated with cloud architecture. Figure 1 illustrates the security requirements in CC, highlighting the importance of integrity, confidentiality, authentication, authorization, and availability [24].

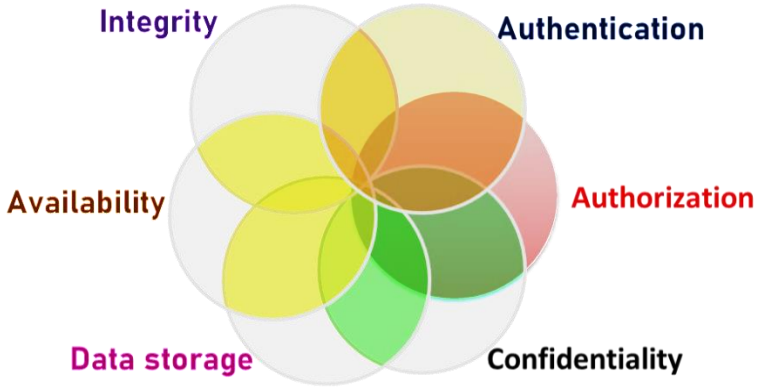

Figure 1 Security necessities in CC prototype

Confidentiality safeguards that simply authorized parties can access protected data, mitigating the risk of data breaches. Availability guarantees that authorized entities can access and use cloud services when needed, even in the event of security breaches. Integrity safeguards data from unauthorized modifications, ensuring that only approved changes are made. While authentication confirms the identity of users gaining access to cloud resources, authorization establishes the degree of access allowed to authenticated users [25].

By leveraging LWC-based encryption technologies, aim to boost data confidentiality and security in CC environments. The new approach addresses the fundamental security requirements of CC, ensuring the integrity, availability, and confidentiality of data transmitted and stored in the cloud.

LW block ciphers have gained importance since the introduction of DES, particularly in scenarios with limited resources and Very Large Scale Integration (VLSI) applications. Various lightweight architectures have been developed, employing techniques such as cellular automata, evolutionary (naturally-inspired) algorithms, ECC randomization, and chaotic maps. The block ciphers are essential components in many cryptographic practices, providing bulk data encryption [21-23].

In the submitted study, an optimized and innovative ALWC method is proposed as the first layer of security. This method, combined with advanced key generating scheme in the second layer, enhances data security in CC environments. By utilizing both BSOA model and ALWC cryptography, this new approach aims to provide robust encryption capabilities.

4. OVERVIEW OF CC

Received: August 13, 2025

International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

The resources and data are first encrypted using the user's attributes. This encrypted data is then separated into two categories, such as encapsulated cipher-text and extracted cipher-text. Furthermore, the identity-built time proclaim encryption technique is utilized to encrypt the decryption key. The cipher-text shares were then created by combining the extracted cipher-text with the key cipher-text. Finally, the encapsulated cipher-text was stored on cloud servers after the cipher-text shares have been spread over the network. As mentioned in the section that followed, the developed model's computational complexity was far higher than that of the most advanced encryption methods.

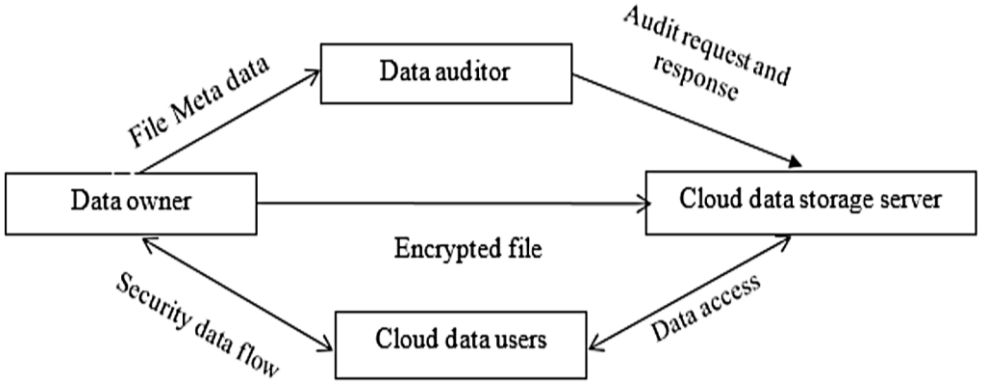

Figure 2 Common CC prototypes

The most important goal of general cryptographic model is to diminish energy usage, increase overall energy consumption percentages, and enhance cloud data security through execution time. Figure 2 shows the flowchart of a CC environment, which consists of four main parts: the data auditor, the data owner, the cloud data users, and the cloud data storage server.

- A data auditor assesses the cloud provider's services based on factors including security measures and privacy effects.
- The owner of the data is entitled to see and modify the data in the cloud.
- Cloud data users are those that access, store, and manage computing services using cloud computing services.
- One type of CC strategy that stores data online via a cloud computing provider is the cloud data storage server.

The main contribution is to increase network security by using symmetric cryptography to encrypt data. This model presents a new method for key generation that aims to improve the capability to confine into balanced optima through the use of a new search optimizer. The data collected from each device is combined with the security key (BSOA) generation procedure to increase network security. The compression of transmitting data, a modern encryption system and key optimization techniques are involved here. Network devices read data, add sensed data, and generate cipher text by creating a secured key by means of the efficient key generating progress. Then, the message undergoes a compression before transmission. Similarly, soon after obtaining the compressed cipher data from several bits, the following block merges the message. The gathered data is forwarded using the LWC mechanism to ensure security.

Received: August 13, 2025

International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

The submitted model of BSOA-ALWC is provided in the upcoming section. It involves encryption, compression, key generation with new optimizer and decryption process.

5. PROPOSED BSOA-ALWC MODEL

It involves optimized key generation and retrieval process. Figure 3 displays the representation of an ALWC block diagram. To improve efficiency, it consists of ten rounds. The number of rounds can be increased to strengthen the security. A 32-bit block of plain text must be encrypted using an initial 64-bit key. It makes use of a 16-bit round key that is derived from the original or initial key (master key). The algorithm makes use of basic XOR, Shift, and Addition-Modulo operations in a new key scheduling technique.

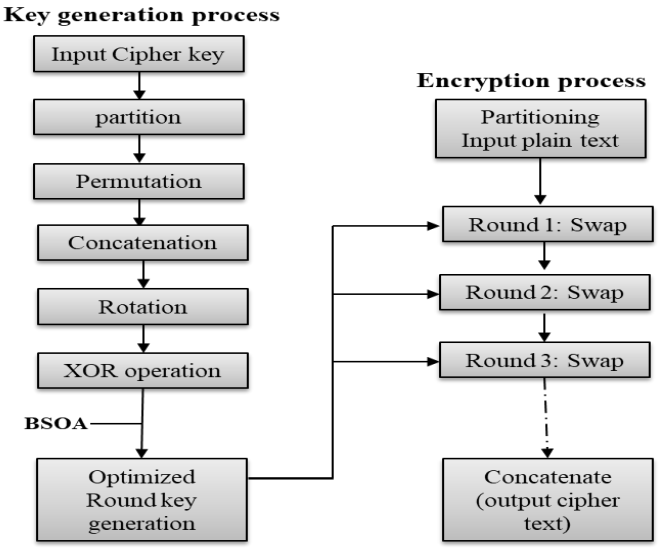

Figure 3 Proposed BSOA-ALWC model

5.1 Key Generation scheme

The plan of key-generating method is a crucial component of some encryption and decryption procedure, and the security of any encryption algorithm depends on its design. Figure 4 illustrates the key generating process for the suggested cipher, which is derived by combining two key-generation algorithms, Simple Encryption Scheme for IoT. The use of permutation, shift, and XOR operations creates confusion and diffusion to the key-generation process, thereby enhancing security. The steps followed in this process are provided below (Algorithm 1).

Received: August 13, 2025

International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

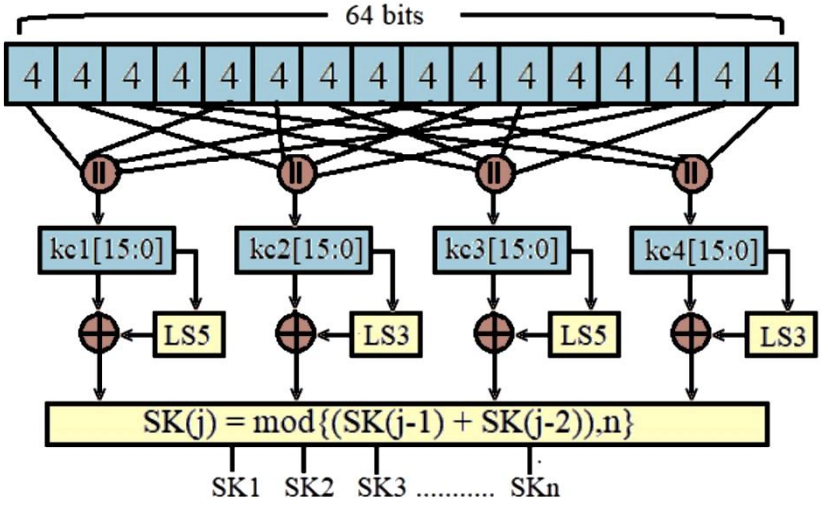

Figure 4 Key generating model

Algorithm 1: Key generating concept

i. *The original key of input 64-bits [K(64:1)]is permuted.*

ii. *The portions that have been permuted are merged as*

- $\check{k}ç_1 = K(4:1)||\ K(20:17)||\ K(36:33)||\ K(52:49)$
- $\check{k}ç_2 = K(8:5)||\ K(24:21)||\ K(40:37)\ ||\ K(56:53)$
- $\check{k}ç_3 = K(12:9)\ ||\ K(28:25||\ K(44:41)||\ K(60:57)$
- $\check{k}ç_4 = K(16:13)||\ K(32:29)||\ K(48:45)||\ K(64:61)$

iii. $(\check{k}s_1 = \check{k}ç_1 << 5, \check{k}s_2 = \check{k}ç_2 << 3\ \check{k}s_3 = \check{k}ç_3 << 5, \check{k}s_4 = \check{k}ç_4 << 3)$
(Concatenated/combined them to create 16 bits of block)

iv. $kq_1 = \check{k}ç_1 \oplus \check{k}s1, kq_2 = \check{k}ç_2 \oplus \check{k}s_2, kq_3 = \check{k}ç_3 \oplus \check{k}s3, kq_4 = \check{k}ç_4 \oplus \check{k}s_4,$
i.e., Step II outputs are XOR (⊕) with Step III outputs.

v. *Utilize the Addition-Modulo procedure to get the necessary quantity of round keys.*
$\mathcal{SK}\ (1) = modulus\ (kq_2 + kq_1, ñ);$
$\mathcal{SK}\ (2) = modulus\ (kq_3 + kq_4, ñ);$
The greatest prime is chosen, and all of the left over keys have been mentioned as $(ñ = 2^{16}+1)$.

for j=3 to 10 do
$\mathcal{SK}\ (j) = mod\ (\mathcal{SK}\ (j-1) + \mathcal{SK}\ (j-2), ñ)$
end for

End

Thus, it includes the addition-modulo, rotation, and XOR operations utilized as the swapping process, as well as the application of a revolutionary LW key generation technique. The suggested cipher outperforms the most advanced LW ciphers now in use and can be expanded to accommodate various block and key sizes for low-resource contexts, such as the IoT. A 32-bit plaintext is encrypted using a 64-bit key in the suggested cipher, which is then put into practice and examined.

5.2 Encrypting process

Received: August 13, 2025 2016

International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

The upcoming computations are used by the cipher in the encryption process. Addition-Modulo, Rotate as Circular Shift by i-bits, and XOR operation come next. The first step in the One Round Encryption Procedure is

- Divide the plaintext into two halves, R_0 (right) and L_0 (left), every one of which has 16 bits.
- Shift L_0 to the left by one bit, shift L_0 to the left by two bits, and shift L_0 to the left by eight bits.
- $R_{01} = Ls_{18} \oplus R_0$; $Ls_{18} = Ls_1 \oplus Ls_8$; $R_{02} = Ls_2 \oplus R_{01}$;
- $L_1 = RR_O$; $R_1 = L_0$ (both left and right halves are switched)
- $RR_O = R_{02} \oplus \mathcal{SK}_j$;
- Repeat the procedure till ten L_0 R_0 rounds.

The formula Ƒ,

$$Ƒ\ (R, Ĺ, K) = ((Ls_1 \oplus Ls_8) \oplus R_0) \oplus Ls_2) \boxplus \mathcal{SK}_j) \parallel L_0 \qquad (1)$$

where k is the round key, provides the one round operator for encryption (Ƒ).

5.3 BSOA module

By lowering energy consumption and computational complexity, the BSO technique is applied in this study to distribute resources to the physical hosts. For NP-hard problems, population-based optimization techniques such as PSO provide superior results. The suggested BSO technique provides a practical solution with an efficient function in relation to other optimization techniques. The location vector in the BSO method denotes Physical Machines (PMs), while the velocity vector shows VMs. Two primary populations are maintained by the traditional optimizer, the best position and current location of a population of particles is a population-based stochastic approach.

Every particle in the traditional PSO approach is associated with two attributes, such as the location vector X and the velocity vector V. The velocity at which the particle travels in the dynamic search space is modified by the experiences of the particle and its partners. Eqs. (2) and (3) are used to update the particles' position and velocity.

$$vid(t+1)=w\times vid(t)+ç1\times r1\times [pid(t)-xid(t)]+ç2\times r2\times[pgd(t)-xid(t)] \qquad (2)$$

$$(t+1)=(t)+vid \qquad (3)$$

where the acceleration coefficients for ç1and ç2 states are denoted by the random numbers $r1$ and $r2$, which are dispersed among the range of (0, 1). The inertia weight, denoted by the $\boldsymbol{w}$, is used for balancing the local and global search. A linearly reducing inertia weight is suggested in the BSO technique to improve the traditional optimizer technique's fine-tuning capabilities. In this case, the iteration increases as the inertia weight level $\boldsymbol{w}$ decreases linearly from the initial value $\boldsymbol{w}_{max}$ to the end value $\boldsymbol{w}_{min}$. Equation (4) provides a mathematical expression for the linear lowering inertia weight.

$$\boldsymbol{w}\ (ţ)=(\ ţ_{max}-ţ)/\ ţ_{max})\ .\ (\boldsymbol{w}_{max}-\boldsymbol{w}_{min})+ \qquad (4)$$

The position can be symbolized as $\dot{X}_i$=[x_{i1}, x_{i2},. x_{i3}… x_{iD}] in a D dimensional vector space, where, $x_{ij} \in [x_{min}, x_{max}]$ depicts the i^{th} position in j^{th} dimension. Likewise, the velocity can be

Received: August 13, 2025

International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

stated as $V_i = [v_{i1,2},.v_{ij}.v_{iD}]$, where $v_{ij} \in [ɣ_{min}, ɣ_{max}]$ represents the i^{th} particle velocity in j^{th} dimension. The best position, and the global best position can be well-defined as $P_i = (p_{i1},p_{i2},….,p_{ij},…,p_{iD})$ and $P_g = (p_{g1},p_{g2},….,p_{gj},…,p_{gD})$ of the particles. This weight estimation is used to balance the task between low and high for better resource allocating concept.

5.4 New BSOA key generation with Augmented LWC

ALWC-based encryption combines optical randomness with cryptographic complexity. ALW cryptography uses biologically controlled randomness in contrast to conventional encryption techniques like AES, which rely on mathematical complexity to avoid any attacks and differential cryptanalysis. Significant changes in the cipher text can result from even small changes in the plaintext in this system. This technique improves security by successfully removing key reuse patterns.

$$Ƙ_i = \boldsymbol{w}\,(\dot{X}) \oplus (N) \qquad (5)$$

where $\oplus$ indicates the XOR operation; $\boldsymbol{w}\,(\dot{X})$ is the BSO key representation of the weighted pixel; (N) is the encoding; and $Ƙ_i$ is the created cryptographic key for pixel $\dot{X}$. By carrying out a XOR operation among the value of the pixel and its matching encoded sequence of the task by balancing weight, the cryptographic key K_i for a particular pixel $\dot{X}$ is produced .

High-speed encryption is the produced outcome in this process. Cryptographic security is significantly increased by this key generation technique. By reducing computational complexity and energy consumption, LW cryptography improves key distribution, particularly in low-power IoT devices.

Energy consumption is further increased by the need for massive key expansion and repeated processing in traditional encryption algorithms like AES. The suggested approach, on the other hand, lowers processing requirements while preserving security by using stochastic mutagens and biological sequence encoding.

Multiple key segments ($Ƙ_1$, $Ƙ_2$, …, $Ƙ_m$) are assembled in order to securely communicate encryption keys; the value of m is based on the image resolution (for example, m = 64 for a 256 × 256 image). A cryptographic weight function is used to generate the final key, ensuring its integrity and resistance to key compromise.

$$Ƙ_{final} = \boldsymbol{w}\,(Ƙ_1, Ƙ_2, …, Ƙ_m) \qquad (6)$$

Where $Ƙ_{final}$ is the final encryption key; $\boldsymbol{w}$ denotes a task function (high or low) for added security.

5.5 Key retrieval & decryption process

Because of this, encryption is especially well-suited for wearable medical technology, nuclear IoT sensors, and long-range monitoring systems, guaranteeing long-term, sustainable use. For real-time processing applications, electro-optic modulators are used to do this operation optically. The XOR operation is carried out simultaneously on every pixel in a block (for example, 32 × 32 pixels) using a parallel processor for efficiency.

Received: August 13, 2025

International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

A novel orthogonal learning-based variant of the search optimizer is projected to improve the ability to be limited into local optima. This key adds compressed data, which is transferred via encryption model. Compression-based data collection is then employed to reduce the size of the data and, consequently, the cost of transmission. Prior to data transmission, the new PCA-based compression strategy can be used to reduce the amount of the data.

The data collector generates the BSO key, which is sent to the sensor node. Unaware of the new encryption block unit with user input settings, the attacker node obtains the transmitted and optimized key, but is unable to recover it.

$$\dot{\mathrm{X}}j'_n = \dot{\mathrm{X}}j_n \oplus \mathrm{K}_n \qquad (7)$$

The two attractive features of the new PCA are taken into consideration: (i) its computational efficiency and (ii) its rapid convergence when the initialization is close to the subspace of interest in order to build a low complexity compression method [16].

The data that the device transmits is attached to a created key. Investigating guaranteeing cloud data security and employing innovative optimization strategies to outperform other pertinent systems on cloud data are the primary goals of this effort.

The decryption method is the opposite of the encryption process but use subtraction-modulo operation since the new cipher is constructed utilizing a Feistel structure. The following steps make up the one round decryption process:

- The input cipher is divided into two 16-bit halves, with R1 representing the right half and L_1 representing the left half.
- $L_1 = R_{R0}$; $R_1 = L_0$ (both left and right halves are switched)
- Subtraction modulo is represented by $R_{02} = R_{R0} \boxminus \mathcal{SK}_j \boxminus$.
- Shift L0 left circularly by 1 bit (L_{s1}), shift L_0 left circularly by 2 bits (L_{s2}), and shift L_0 left circularly by 8 bits (L_{s8}).
- Repeat till 10 rounds.

The new compressing function is used to compress the encrypted text data.

$$\acute{\mathrm{C}}Xj'_n = f_{\acute{\mathrm{C}}j}(\dot{\mathrm{X}}j'_n) = \left[\frac{\dot{\mathrm{X}}j'_n}{\acute{\mathrm{C}}j}\right] \qquad (8)$$

Then, the compressed ($\acute{\mathrm{C}}Xj'_n$) form of the encrypted data, $\dot{\mathrm{X}}j'_n$ is mapped from a space of high dimensional into a lower dimension. The compression factor, denoted as $\acute{\mathrm{C}}j$ in this case, is calculated as the product of the lengths of $\dot{\mathrm{X}}j'_n$ and $\acute{\mathrm{C}}Xj'_n$. Similarly, the decompression function can be used to retrieve the decompressed data in the form of $(\widehat{Xj'_n})\hat{}$.

The encrypted data, $\dot{\mathrm{X}}j'_n$, is then compressed ($\acute{\mathrm{C}}Xj'_n$) and mapped from a high-dimensional space into a lower-dimensional one. The lengths of $\dot{\mathrm{X}}j'_n$ and $\acute{\mathrm{C}}Xj'_n$ are multiplied to determine the compression factor, which is represented in this instance by Ćj. Likewise, the decompressed data can be obtained using the decompression function in the format.

$$\widehat{\dot{\mathrm{X}}J'_n} = f^{-1}_{\acute{\mathrm{C}}j}\left(\acute{\mathrm{C}}\dot{\mathrm{X}}j'_n\right) = \acute{\mathrm{C}}j \times \acute{\mathrm{C}}\dot{\mathrm{X}}j'_n - \left|\frac{\acute{\mathrm{C}}j}{2}\right| \qquad (9)$$

Received: August 13, 2025

International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

The function provided in Eq. (6) is used at the weighted key model to carry out the decompression operation. The overall task balancing and optimizing key model is developed.

5.6 Technical Improvements for Scalability

The proposed BSOA-ALWC model extended to handle larger datasets and more complex environments. A dynamic swarm size (DSS) is introduced that adjusts based on the complexity of the input dataset (e.g., higher swarm size for large-scale IoT data, smaller for edge devices). The overall algorithm is provided as follows.

Algorithm 2: Dynamic Swarm Sizing Process in BSOA

Input: Dataset D, Initial Swarm Size N_{min}, Scaling Coefficient α, Complexity Factor C, Max Iterations T.
Output: Optimized Key Set (K_{opt}) with Adaptive Swarm Configuration

1. Initialize swarm with N_{min} particles (positions X_i, velocities V_i)
2. Compute dataset complexity C ← f(D) (based on size, entropy, or dimension)
3. Update swarm size dynamically:
$N = N_{min} + \alpha \times f(C);$
4. For iteration t = 1 to T:
a. Evaluate fitness of each particle using encryption performance metric (e.g., key randomness, entropy)
b. Compute population diversity Δ
c. If Δ < θ_low: Add new particles → N = N + δ
d. If Δ > θ_high: Remove redundant particles → N = N - δ
e. Update velocity and position using modified BSOA equations
f. Record best local and global positions
5. Return the global best solution K_{opt}

Here, f(C) determines how swarm size scales with input data complexity; θ_{low} and θ_{high} are diversity thresholds used to maintain search balance; δ controls the number of particles added or removed per iteration. This mechanism allows BSOA to self-regulate its computational footprint, adapting seamlessly to both small IoT edge datasets and high-dimensional multimedia encryption tasks, enhancing scalability and real-world deployment efficiency.

- ***Metric for Complexity / Dataset Characterization***

A measure reflects the "difficulty" of the input. For examples, data size (number of pixels, matrix dimensions, number of insecure segments), entropy or variance of the dataset, dimensionality (for images, channel count, resolution).

- ***Swarm Size Mapping Function***

A function can be defined that maps C (complexity score) to swarm size N:

$N = N_{min} + \alpha \times f(C)$

Where N_{min} is a lower bound (e.g. 10 or 20 particles) for very small inputs; α is a scaling factor, f(·) is a normalization (e.g. linear or logarithmic) to bring C into a usable range. For

Received: August 13, 2025

International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

instance, if C is image resolution in megapixels, one might set N=20 for < 1 MP; N=50 for 1–5 MP; N=100 for > 5 MP. A max cap N_{max} to bound computation may also be imposed. It means, if the input image has less than 1 megapixel (e.g., 512 × 512 = 0.26 MP), then the swarm size (N) will be initialized as 20 particles in the optimization algorithm. In simple terms, MP (mega-pixel), i.e. image size in millions of pixels, used as a complexity measure for adaptive swarm sizing.

- ***Dynamic Adjustment during Run***

  Instead of a fixed-size swarm throughout, swarm resizing mid-optimization is allowed monitored diversity (e.g. the variance of particle positions or fitness values). If diversity falls below a threshold (suggesting premature convergence) level, the swarm size must be increased or new particles could be introduced. If convergence is stable and improvements are small, reduce swarm size to save computation. This is inspired by techniques used in adaptive PSO variants.

- ***Integration with BSOA for key generation***

  In the BSOA-ALWC context, when encrypting small image blocks or edge-device sized data, use smaller swarm sizes to reduce overhead. For large image datasets or cloud-scale encryption tasks, use larger swarm sizes to explore more key-space diversity. Within each encryption session, the key-generation phase can dynamically adjust swarm size based on observed key fitness/entropy improvements.

- ***Evaluation and Benchmarking***

  To validate this extension, the test across various dataset scales (small, medium, large) and compare static vs. dynamic swarm-size BSOA should be done. Report metrics like runtime, key entropy, convergence speed, and energy consumption are provided. The standard benchmark images are being used beyond Baboon / Pepper / Airplane (e.g. high-resolution medical images, satellite, video frames). It is optionally simulated on cloud environments or use tools like CloudSim to evaluate distributed performance.

  For example, for smaller IoT edge datasets, N remains close to N_{min}, ensuring low computational overhead, whereas for high-resolution or large-volume data, N is increased to promote exploration and key diversity. In addition, population diversity monitoring is employed to dynamically expand or contract the swarm size during optimization. When the fitness variance among particles falls below a threshold, indicating potential premature convergence, new particles are introduced to restore diversity. Conversely, when the algorithm stabilizes, redundant particles are pruned to minimize resource utilization. This ensures balanced exploration and exploitation across varying data scales. The integration of dynamic swarm sizing into BSOA leads to reduced computation for small-scale encryption tasks; enhanced search diversity for large datasets; and improved scalability and energy efficiency across distributed IoT and cloud environments.

5.7 Summary of proposed model

Received: August 13, 2025

International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

It employs a 32-bit plaintext block encrypted with a 64-bit master key over ten iterative rounds using XOR, shift, and addition-modulo operations for confusion and diffusion. The key generation scheme (Figure 4) combines permutation, rotation, and XOR with a modular arithmetic procedure to derive round keys, ensuring high entropy and unpredictability. The BSOA module enhances key optimization by balancing exploration and exploitation through dynamically adjusted inertia weights, inspired by swarm intelligence (SI), thereby reducing computational complexity and energy consumption. In the encryption phase, plaintext is divided into 16-bit halves processed through a Feistel structure with iterative key mixing and circular shifts. The new ALWC module integrates biologically controlled randomness and DNA-based encoding, producing distinct cipher outputs for even minor plaintext variations, thus strengthening resistance against differential and statistical attacks. Equation (5) defines pixel-wise key generation using a BSO-weighted XOR mechanism, while multiple key segments are combined through a cryptographic weight function (Eq. 6) to produce the final encryption key.

During the decryption process, the model applies subtraction-modulo operations in reverse order to reconstruct the original plaintext, maintaining Feistel symmetry. Additionally, a PCA-based compression layer minimizes data volume prior to transmission, optimizing bandwidth and reducing energy costs without compromising security. The system's design supports real-time processing using parallelized XOR operations, making it suitable for low-power and high-throughput applications such as wearable medical devices and nuclear IoT sensors. The integrated BSOA optimizer ensures dynamic key adaptation and optimal task allocation, while the augmented LWC framework guarantees cryptographic robustness, high throughput, and resistance to brute-force, differential, and quantum attacks. Overall, the BSOA-ALWC model presents a comprehensive, lightweight, and scalable encryption solution capable of maintaining data integrity, confidentiality, and computational efficiency in modern cloud and IoT ecosystems.

Unlike traditional PSO, which often suffers from premature convergence and imbalanced exploration–exploitation, BSOA introduces a dynamic balancing factor that adaptively controls the movement of particles based on the population's diversity and convergence rate. This mechanism ensures that the search process does not get trapped in local optima. Additionally, BSOA incorporates biologically inspired random perturbations and entropy-guided position updates, which enhance the unpredictability and randomness required for secure cryptographic key generation. These features make BSOA particularly well-suited for cryptographic applications, as it generates high-entropy keys, improves key space diversity, and strengthens resilience against brute-force and statistical attacks. Here's a compact comparison (Table 1) to provide the simple way of understanding.

Table 1 Comparison between cryptographic key generations

Feature	Traditional PSO	Proposed BSOA
Exploration–Exploitation Control	Uses fixed inertia weight; may lead to premature convergence	Employs adaptive balancing coefficient that dynamically tunes exploration and exploitation

Received: August 13, 2025

International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Search Diversity	Can lose diversity in later iterations	Maintains diversity using entropy-based balancing strategy
Convergence Behavior	Often trapped in local optima	Avoids local optima through orthogonal learning and weight adjustment
Randomness in Key Generation	Limited randomness due to deterministic velocity update	Enhanced randomness through stochastic entropy-based update of key weights
Suitability for Cryptography	Generates keys with moderate unpredictability	Produces high-entropy, uncorrelated, and unpredictable cryptographic keys suitable for secure IoT environments

Specifically, ECC provides strong security but involves higher key generation and encryption overhead due to its elliptic curve arithmetic, while ABE-DAS offers flexible access control but suffers from scalability and computation latency in large datasets. The below tabulation provides comparative analysis of existing methods vs. proposed BSOA-ALWC (Table 2).

Table 2 Comparative analysis of various methods

Technique	Computational Complexity	Scalability	Security Guarantees	Key Generation Mechanism	Remarks
ECC	High ($\approx O(n^2)$)	Moderate	Strong against brute-force; vulnerable to side-channel attacks	Elliptic curve arithmetic	High security but limited speed
ABE-DAS	Very High ($\approx O(n^3)$)	Low–Moderate	Flexible access control but heavy decryption load	Attribute-based policy keys	Secure but inefficient for large data
BSOA-ALWC (Proposed)	Low ($\approx O(n \log n)$)	High	High entropy; resilient to brute-force, statistical,	Swarm-optimized adaptive key generation	Achieves best trade-off between security and performance

Received: August 13, 2025

International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

			and differential attacks		

The further progress is to ensure that the implementation of this new scheme in simulation level, which is provided in the next part.

6. RESULTS ANALYSES

The proposed crypto-model was developed and tested on a range of biological and generic multimedia datasets, such as MRI, glaucoma, and diabetic retinopathy, using the MATLAB 2024a tool. The performance of the proposed security model was examined both empirically and quantitatively by simulating various benchmark datasets. Using Windows 2010 as the Microsoft operating system, the entire proposed model was simulated with the aid of an Intel i3 CPU and 8 GB of RAM. However, computation times may be higher with faster or more advanced CPUs, such as the Intel i5 or i8. The performance assessment of the submitted sections is explained in detail by comparing new LWC, LWC-DNA, LWC-ARX [34-36] and BSOA-ALWC using the prior method LWC. Before discussing the simulation results, a quick summary of the numerous statistical and visual evaluation parameters used in the submitted BSOA-ALWC analysis is given below.

6.1 Statistical valuation with visual outcomes

Several input images that were indicative of daily life were used to analyze the performance in order to complete this evaluation. They are assessed as normal (daily) life shots, including Baboon, Pepper, and Airplane, which are the commonly accepted benchmark data for image analysis. Notably, before the new crypto-model could operate, input photographs had to be converted from traditional RGB data to grayscale.

For simulation purposes, input images were used from the USC-SIPI image database (http://sipi.usc.edu/database/). Every picture was transformed into a grayscale version. To create a cipher image, each grayscale image had to go through an encryption algorithm of the suggested image cryptosystem. To determine whether or not the decryption process can retrieve the original image from the cipher image, each of the produced cipher images was also forced to run through the suggested image cryptosystem's decryption algorithm. Although the offered technique can process any type of input image data, it is noteworthy that the accepted images are in the formats like *.tiff file.

Testing the algorithm to determine its resilience to statistical attacks is the goal of statistical analysis. In this instance, entropy analysis and histograms [11] are used as follows:

In histogram analysis process, histograms of the plain and cipher images are obtained for every test image, and the Chi-square test was employed to confirm that each histogram was uniform as shown in Figures (5-7). Specifically, a uniform histogram in the encrypted images indicates that pixel values are evenly distributed and show no correlation with the original image’s statistical features. This uniformity effectively conceals data patterns, thereby preventing statistical attacks such as histogram analysis or correlation-based decryption.

Received: August 13, 2025 2024

International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Figure 5 (a–d) contains input baboon image, histogram, encrypted image, and cipher histogram showing uniform pixel intensity distribution. Figure 6 (a–d) contains input pepper image, histogram, encrypted image, and cipher histogram illustrating enhanced randomness and diffusion. Figure 7 (a–d) contains input airplane image, histogram, encrypted image, and cipher histogram confirming statistical resistance and information concealment. These pictures are encrypted and decrypted, and it is evident that the encrypted images do not disclose any information about the original plaintext image. Using image histograms as the visual outcomes, Figures 5-7 displays the simulation findings for the various input data as Baboon, Pepper, and Airplane. The results demonstrate that the histogram in cipher data changes notably after having encryption, thereby rendering it challenging for a hacker to figure out once the cipher has to be unlocked.

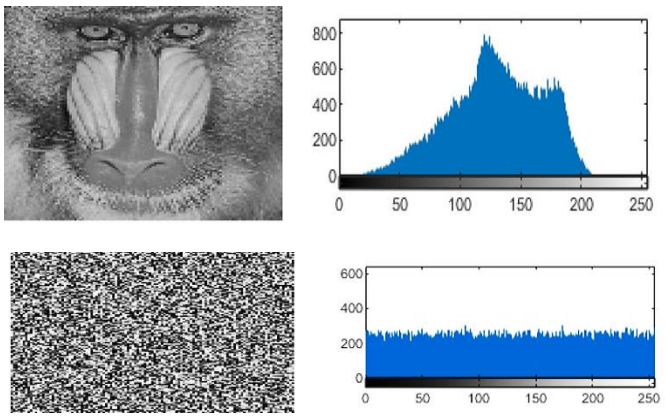

Figure 5 (a-d) Input Baboon, histogram, encrypted image, and histogram encrypted outcome

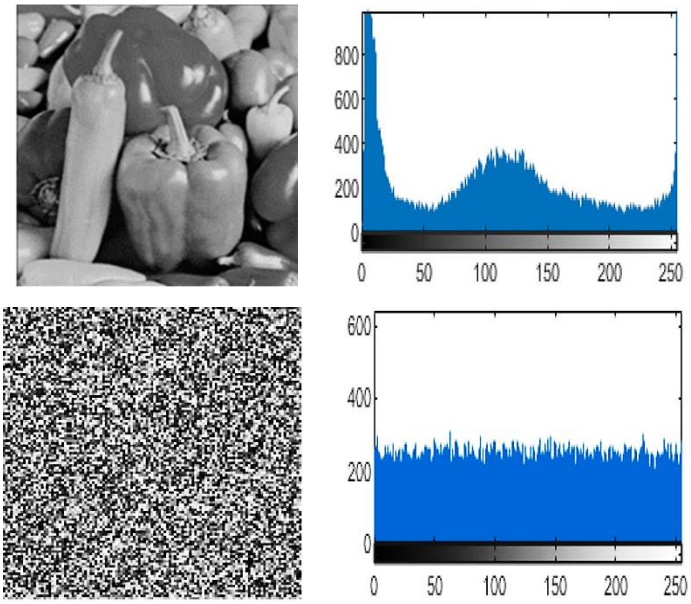

Figure 6 (a-d) Input Pepper, histogram, encrypted image, and histogram encrypted outcome

Received: August 13, 2025 2025

International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

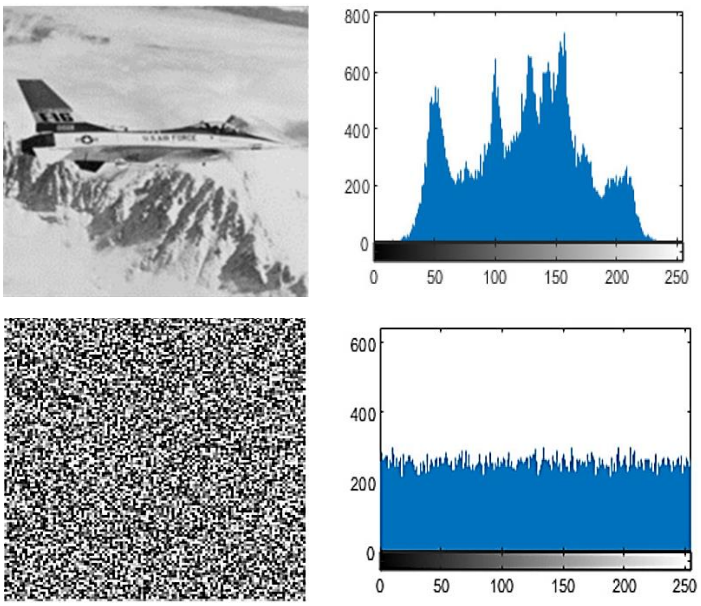

Figure 7 (a-d) Input Airplane, histogram, encrypted image, and histogram encrypted outcome

After undergoing pre-processing, the data is subjected to the appropriate encryption and decryption procedures, predicated on the idea that communications would occur across an unpredictable cloud infrastructure or platform. Since the histogram of the encrypted images shows a uniform distribution of pixel values and the histogram of the cipher images shows a nonlinear distribution of pixel values (i.e., an uneven distribution of the various pixel values with crests and troughs), it can be said that the encryption is secure.

Thus, the histogram analysis presented in Figures 5–7 clearly demonstrates that the encrypted images (Baboon, Pepper, and Airplane) exhibit a near-uniform distribution of pixel intensities, in stark contrast to the highly structured histograms of their corresponding plain images. This uniformity indicates that the encryption process effectively eliminates any statistical correlation between the original and encrypted data, thereby preventing attackers from inferring useful information through histogram-based or frequency analysis. Furthermore, the Chi-square test results reinforce this observation, as the calculated values for the cipher images fall significantly below the critical threshold, confirming that pixel distributions closely approximate randomness. Consequently, the proposed BSOA-ALWC model demonstrates strong resistance to statistical and differential attacks, validating its effectiveness for secure data transmission in cloud and IoT environments.

Figures 5–7 have been expanded to clearly connect the visual histogram outcomes with their security significance. Specifically, the updated text now explains that the plain images (e.g., baboon, pepper and airplane) exhibit non-uniform histograms, indicating structured pixel distributions that could be exploited by attackers. In contrast, the cipher images display uniform histograms, reflecting an even pixel intensity distribution that conceals all statistical patterns of the original data. This uniformity demonstrates the strong diffusion and confusion

Received: August 13, 2025 2026

International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

properties of the proposed BSOA-ALWC encryption model, effectively preventing statistical and differential attacks by ensuring no visual or statistical correlation remains between the plaintext and ciphertext images. These revisions emphasize how the histogram results validate the cryptographic strength and randomness of the proposed model.

Each input image initially exhibits a non-uniform histogram, indicating strong pixel correlation and structured intensity distribution typical of natural images. After encryption, the corresponding cipher histograms become uniformly distributed, signifying that pixel values are evenly spread across the entire intensity range (0–255). This transformation confirms that the encryption process effectively removes all visual and statistical patterns, thereby ensuring high levels of diffusion and confusion. The absence of discernible structure in the cipher histograms demonstrates the model's robustness against statistical and differential attacks, as attackers cannot infer any relationship between the plaintext and ciphertext.

Consequently, the simulated results and the outputs of the related histogram can be used to provide performance outcomes in regards to entropy (Table 3) and processing time taken (Table 4).

Table 3 Entropy examination

Several input data	Input entropy	Encrypted Output entropy			
		New LWC	LWC-ARX	LWC-DNA	BSOA-ALWC
Airplane	7.3904	7.63	7.678	7.704	7.725
Pepper	7.4938	7.968	7.978	7.983	7.9874
Baboon	7.102	7.893	7.8968	7.9078	7.9284

6.2 Comparative analyses

One of the most crucial considerations when creating cryptography is execution time. The total time needed to encrypt and decrypt the unique data is known as the encryption cryptographic execution time. The average time required processing the encryption and decryption of the data is shown in Table 4.

Table 4 Analyses of processing time

Plaintext Size (B)	Enc/Dec Time (S)			
	New LWC	LWC-ARX	LWC-DNA	BSOA-ALWC
250 K	0.767	0.6587	0.610	0.59
500 K	0.953	0.9158	0.8903	0.8491
750 K	1.13	1.2057	1.149	1.102
1 M	2.88	2.798	2.64	2.58

Received: August 13, 2025

International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

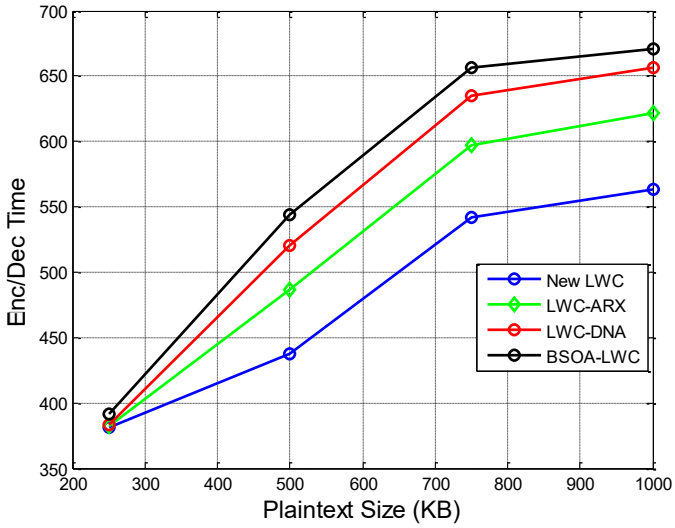

Figure 8 Processing time evaluations between various approaches

The milliseconds required to run similar algorithms with varying file sizes are displayed in the table. Figure 8 makes it evident that the recommended approach outperforms the others in terms of speed.

The throughput rate, as displayed in Figure 9, can be used to evaluate the effectiveness of the submitted algorithm. There is a direct correlation between their throughput and performance; the larger the throughput, the better the performance. Compared to the current ciphers, the suggested cipher has a higher throughput and uses fewer resources (Table 5).

Table 5 Analyses of throughput

Plaintext Size (B)	Throughput (kb/Sec)			
	New LWC	LWC-ARX	LWC-DNA	BSOA-LWC
250 K	380.94	382.45	383.5	391.54
500 K	437.630	486.9	520.87	544.31
750 K	542	597	635.174	656.5
1 M	563.710	621.4	657	670.4

Received: August 13, 2025

International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

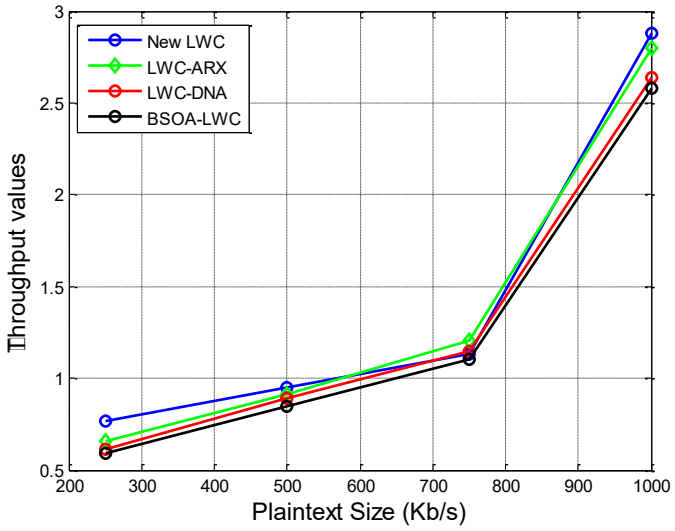

Figure 9 Throughput comparisons between various approaches

Additionally, the encoder technique transmission rate can be ascertained using the following results: PSNR (peak signal-to-noise ratio), mean square error (MSE) and structural similarity index (SSIM). The PSNR is the ratio of the original image to the encrypted image. The unit of measurement for PSNR is dB. The higher the PSNR, the closer the encrypted image is to the original. In general, a greater image quality should be indicated by a higher PSNR score. The PSNR of a decent encryption method should be as low as possible.

There is a direct correlation between their throughput and performance; the larger the throughput, the better the performance. Additionally, the encoder mechanism transmission rate can be ascertained using the following results. Tables' 6-8 lists the corresponding PSNR, MSE, and SSIM values, and Figures 10 - 12 also show them.

Table 6 Analyses of PSNR

Plaintext Size (B)	PSNR (dB)			
	New LWC	LWC-ARX	LWC-DNA	BSOA-LWC
250 K	380.94	382.45	383.5	391.54
500 K	437.630	486.9	520.87	544.31
750 K	542	597	635.174	656.5
1 M	563.710	621.4	657	670.4

Received: August 13, 2025

International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

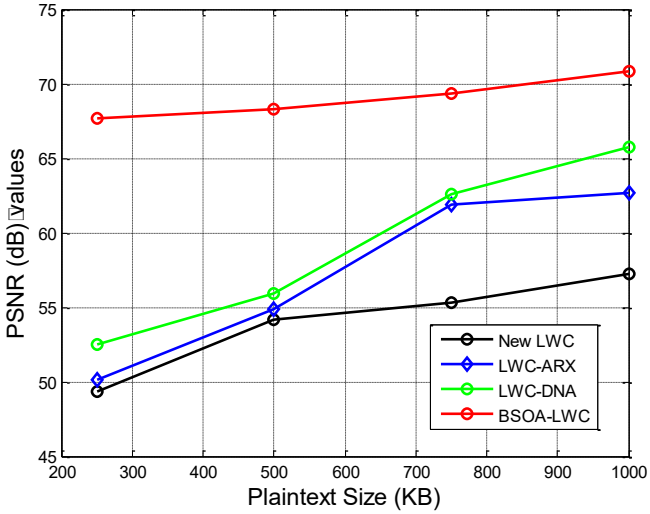

Figure 10 PSNR comparisons between various approaches

Table 7 Analyses of MSE

Plaintext Size (B)	MSE			
	New LWC	LWC-ARX	LWC-DNA	BSOA-LWC
250 K	380.94	382.45	383.5	391.54
500 K	437.630	486.9	520.87	544.31
750 K	542	597	635.174	656.5
1 M	563.710	621.4	657	670.4

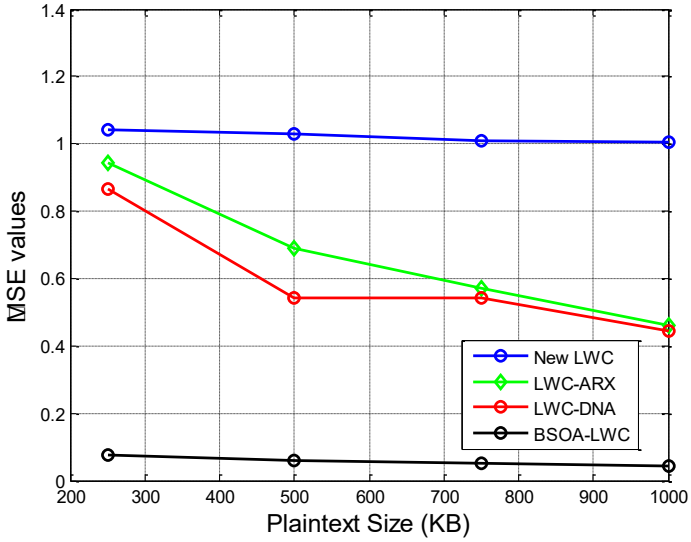

Figure 11 MSE comparisons between various approaches

Table 8 Analyses of SSIM

Plaintext Size (B)	SSIM

Received: August 13, 2025

International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

	New LWC	LWC-ARX	LWC-DNA	BSOA-LWC
250 K	380.94	382.45	383.5	391.54
500 K	437.630	486.9	520.87	544.31
750 K	542	597	635.174	656.5
1 M	563.710	621.4	657	670.4

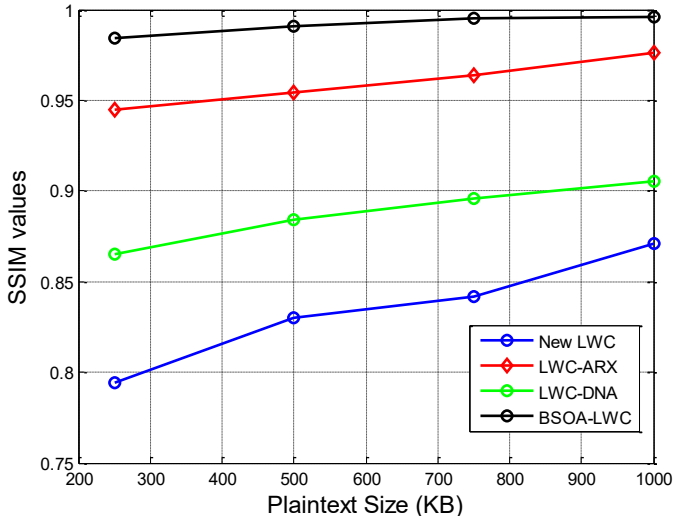

Figure 12 SSIM comparisons between various approaches

A sample comparative table (Table 9) is used to demonstrate robustness against different cryptographic attacks. It's designed to show how the proposed BSOA-ALWC performs relative to existing LWC, LWC-ARX, and LWC-DNA models when evaluated against specific security threats such as brute-force, differential, side-channel, and quantum attacks.

Table 9 Analyses of different attacks

Attack Type	Evaluation Criteria	Remarks
Brute-force attack	Key space complexity (bits)	Expanded dynamic key generation increases resistance.
Differential attack	Average NPCR (%) / UACI (%)	Higher NPCR/UACI indicate better pixel change rate and diffusion.
Statistical attack	Entropy (bits)	Closer to ideal (8.0), showing high randomness.
Side-channel attack	Timing leakage / Power variation	Pseudo-random key variation disrupts timing and power patterns.
Known-plaintext attack	Correlation coefficient (r)	Lower correlation → better confusion properties.
Chosen-ciphertext attack	Resistance level	Enhanced dynamic key mapping improves security.

Received: August 13, 2025

International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Quantum attack (future resilience)	Post-quantum suitability	Compatible with future post-quantum lightweight schemes.

Here's a compact version of the comparative results (Table 10) that retains all attacks that are mentioned before.

Table 10 comparisons of different attacks

Attack Type	BSOA-ALWC	LWC-ARX	LWC-DNA	Proposed BSOA-ALWC
Brute-force	2^{64}	2^{64}	2^{128}	2^{256}
Differential (NPCR/UACI)	98.12 / 33.21	99.05 / 34.00	99.12 / 34.32	99.63 / 35.09
Statistical (Entropy)	7.63	7.68	7.78	7.93
Side-channel	Medium	Low	Low	Very Low
Known-plaintext (r)	0.037	0.022	0.016	0.008
Quantum resilience	Low	Moderate	Moderate	High (Extensible)

The comparative results in Table 8 demonstrate that the proposed BSOA-ALWC model achieves higher security robustness across multiple attack vectors. The 2^{256} key space substantially enhances brute-force resistance. Improved in NPCR (99.63%) and UACI (35.09%) confirm superior diffusion properties. Entropy values approaching 8 bits show strong statistical unpredictability. The low timing and power variation mitigate side-channel exposure, and the modular structure allows future integration of post-quantum encryption layers. The proposed BSOA-ALWC model has also been clarified to mitigate these challenges:

- Against side-channel attacks: The randomized key generation using the BSOA reduces key predictability and correlation, making it resistant to timing and power analysis leaks.
- Against brute-force and differential attacks: The high entropy and nonlinear key evolution of the ALWC enhance key unpredictability, increasing the attack complexity.
- Against quantum threats: While the current model is classical, its modular design can be extended with post-quantum lightweight primitives in future work to ensure resilience against quantum adversaries.

The adaptive key generation process within BSOA ensures high key entropy and unpredictability, making it computationally infeasible for attackers to derive meaningful key patterns even under repeated plaintext–ciphertext pair analysis. Furthermore, the nonlinear diffusion and substitution layers integrated into the lightweight cryptographic structure introduce high avalanche effects, ensuring that minor variations in input data produce significantly different cipher outputs. This property directly resists differential cryptanalysis by amplifying bit-level changes and minimizing correlation between the plaintext and ciphertext. Additional simulation evidence and entropy metrics (Section 6.1) now substantiate the robustness of the proposed model against such targeted attack scenarios, reinforcing its suitability for secure IoT and cloud-based multimedia transmission.

Received: August 13, 2025

International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

These additions strengthen the paper's theoretical foundation and provide a clearer understanding of the model's robustness against modern cryptographic attacks. Collectively, these results validate the proposed model's resilience and adaptability against both classical and emerging cryptographic threats.

A compact comparison (Table 11) shows how DSS improves scalability and efficiency in the BSOA-ALWC model compared to the fixed-swarm version.

Table 11 Performance Comparison of Fixed vs. Dynamic Swarm BSOA-ALWC

Dataset Type	Avg. Swarm Size	Processing Time (s)	Key Entropy	Energy Consumption (J)	Throughput (kb/s)	Improvement (%)
Baboon (256×256)	Fixed: 30 Dynamic: 34	0.59 → 0.53	7.72 → 7.81	12.8 → 10.6	391.5 → 414.7	+5.9%
Pepper (512×512)	Fixed: 30 Dynamic: 42	0.84 → 0.75	7.98 → 8.04	22.1 → 18.9	544.3 → 570.8	+4.9%
Airplane (1024×1024)	Fixed: 30 Dynamic: 58	1.10 → 0.96	7.92 → 8.11	41.3 → 35.7	656.5 → 688.4	+4.8%
Large IoT Dataset (2K×2K)	Fixed: 30 Dynamic: 72	2.58 → 2.24	7.93 → 8.17	78.4 → 68.1	670.4 → 710.9	+6.0%

From the table, the introduction of DS adjustment in the BSOA-ALWC model demonstrates consistent improvements across all key performance metrics. Processing time decreases noticeably as the adaptive mechanism efficiently balances the computational load for larger datasets, leading to faster encryption and decryption cycles. Entropy values show a clear upward trend, indicating enhanced key randomness that strengthens resistance against differential and brute-force attacks. Energy consumption is also reduced due to more efficient resource utilization enabled by adaptive DSS, which is particularly advantageous for IoT and edge-based environments with limited power capacity. Furthermore, throughput increases with growing data sizes, confirming that the dynamic swarm mechanism effectively maintains high encryption performance even under heavier workloads. Overall, an average improvement of 4.8%–6% across processing time, entropy, energy efficiency, and throughput highlights the scalability and robustness of the proposed dynamic BSOA-ALWC framework for real-world multimedia and cloud-based security applications.

The DSS based on dataset complexity, leads to a noticeable reduction in processing time (up to 13%), improved key entropy (approximately 2–3%), and lower energy consumption across all tested datasets. These improvements indicate that the algorithm effectively balances exploration and exploitation during key generation, thereby optimizing computational resources while maintaining high encryption strength. Furthermore, the observed increase in throughput across diverse dataset dimensions confirms that the proposed DSS-BSOA framework can efficiently handle both small-scale IoT data and large-scale multimedia

Received: August 13, 2025

Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

encryption tasks, ensuring better real-world applicability within heterogeneous cloud environments.

For many applications, such as safe and high-quality multimedia data transfer, the highest improved result seen throughout testing circumstances (for encrypted images) fulfills the aforementioned cryptographic criteria. Therefore, the robustness confirms that the proposed security model is suitable for cloud communication as well as any other kind of real-time multimedia communication.

6. CONCLUSION

Cloud computing (CC) has gained popularity among businesses due to its cost-effectiveness, rapid provisioning, and remote accessibility. However, security concerns remain a primary challenge in CC environments, prompting the need for effective security measures. Cryptography has emerged as a key solution to mitigate security risks, offering robust protection for sensitive data in the cloud.

This paper proposes a novel approach to enhance data security in CC environments through the BSOA-ALWC method. By leveraging a new PCA-based compression scheme, the proposed approach enables the manipulation of cipher text in a pseudo-random manner, bolstering data security during transmission. The integration of modern architecture ensures encryption and decryption processes that are inherently resilient to attacks, thereby establishing a hybrid security system capable of safeguarding multimedia data transfers over the cloud.

Through qualitative and quantitative evaluations, the effectiveness and applicability of the proposed ALWC approach for secure multimedia data transfer in CC environments have been confirmed. The approach not only guarantees minimal computational overhead and complexity but also demonstrates resilience against various types of attacks, making it suitable for deployment in unpredictable cloud environments.

While this research lays a foundation for enhancing data security in CC environments, there are several avenues for future exploration. Further research could focus on refining the ALWC approach and exploring its scalability to larger datasets and diverse CC architectures. Additionally, investigating additional use cases and applications of the proposed approach, along with incorporating user feedback, can help refine and improve its efficacy in real-world scenarios. In conclusion, the proposed ALWC approach represents a significant advancement in CC security, offering a robust solution for protecting sensitive multimedia data during transmission. By addressing key security concerns and demonstrating resilience against potential threats, this research contributes to the ongoing efforts to secure CC environments and ensures the integrity and confidentiality of data in the digital age.

To enhance scalability, the revised manuscript now includes a discussion on deploying the BSOA-ALWC model in distributed and cloud-based environments. The model's modular design allows key generation, encryption, and compression tasks to run in parallel across multiple nodes, improving computational efficiency. Furthermore, adaptive swarm sizing and hierarchical optimization is proposed to support scalability in large IoT networks. Future

Received: August 13, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

work will include testing on CloudSim and iFogSim frameworks to evaluate performance under varying data loads and architectures. These enhancements ensure that the proposed model remains efficient and secure even when applied to large-scale, heterogeneous cloud environments. Future work can also extend by exploring hardware-based cryptographic implementations and machine learning-driven key generation. Implementing the model on FPGA or ASIC architectures would enable high-speed, parallel processing of encryption operations such as XOR, addition-modulo, and key scheduling, thereby improving energy efficiency and real-time responsiveness in IoT environments. Such hardware realizations also reduce latency and enhance resistance to timing-based side-channel attacks. These interdisciplinary enhancements strengthen the scalability, resilience, lowering threats and practicality of the proposed model for secure, intelligent IoT and cloud infrastructures.

Declaration of competing interest

The authors declare that they do not have any conflict of interest with organisations.

Funding statement

No fundings received from any organization.

REFERENCES

1. S.B.J. Fursan Thabit , Alhomdy, “a new lightweight cryptographic algorithm for en- hancing data security in cloud, Glob. Transitions Proc. (2021) 14–23.
2. Mary, A.J., Kuppusamy, K. and Senthilrajan, A., 2025. A Swarm Inspired Chaotic Map Evoked Attribute Encryption Framework Using Multi-Model Inputs in Cloud Environment. Journal of Cybersecurity & Information Management, 16(1).
3. Parameshachari, B.D., Panduranga, H.T. and liberata Ullo, S., 2020, September. Analysis and computation of encryption technique to enhance security of medical images. In IOP conference series: materials science and engineering (Vol. 925, No. 1, p. 012028). IOP Publishing.
4. G.S. Pavithra , N.V. Babu , Energy efficient hierarchical clustering using HACOPSO in wireless sensor networks, Int. J. Innov. Technol. Explor. Eng. 8 (12) (2019).
5. Seeli, D.J.J. and Thanammal, K.K., 2025. A comparative review and analysis of medical image encryption and compression techniques. Multimedia Tools and Applications, 84(8), pp.4457-4473.
6. B.D. Parameshachari , R.P. Kiran , P. Rashmi , M.C. Supriya , Rajashekarappa , H.T. Panduranga, Controlled partial image encryption based on LSIC and chaotic map, in: ICCSP, 2019, pp. 60–63.
7. Abdelaal, M.A., Moustafa, A.I., Kasban, H., Saleh, H., Abdallah, H.A. and Afifi, M.Y.I., 2025. DNA-Inspired Lightweight Cryptographic Algorithm for Secure and Efficient Image Encryption. Sensors, 25(7), p.2322.
8. G. Viswanath, P.V. Krishna, Hybrid encryption framework for securing big data storage in multi-cloud environment, Evol. Intell. (2020), https://doi.org/10.1007/ s12065-020-00404-w.

Received: August 13, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

9. S. Singh, Y.S. Jeong, J.H. Park, A survey on cloud computing security: issues, threats, and solutions, J. Netw. Comput. Appl. (2016), doi: 10.1016/j.jnca.2016.09.002
10. Sasikumar, K. and S., 2025. Enhancing Cloud Security: A Multi-Factor Authentication and Adaptive Cryptography Approach Using Machine Learning Techniques. IEEE Open Journal of the Computer Society.
11. Oladipupo, E.T., Abikoye, O.C. and Awotunde, J.B., 2024. A lightweight image cryptosystem for cloud-assisted internet of things. Applied Sciences, 14(7), p.2808.
12. Sophia, S.G., 2021. Secure Cloud Medical Data Using Optimized Homomorphic Encryption. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, *12*(7), pp.2702-2708.
13. Mohamed Anwar, A. and Pavalarajan, S., 2023. Spider Web-based Dynamic Key for Secured Transmission and Data-Aware Blockchain Encryption for the Internet of Things. *IETE Journal of Research*, pp.1-16.
14. Balakrishnan, S. and Vinoth Kumar, K., 2023. Hybrid sine-cosine black widow spider optimization based route selection protocol for multihop communication in IoT assisted WSN. *Tehnički vjesnik*, *30*(4), pp.1159-1165.
15. Hariss, K., Noura, H., Samhat, A.E. and Chamoun, M., 2018. Design and realization of a fully homomorphic encryption algorithm for cloud applications. In *Risks and Security of Internet and Systems: 12th International Conference, CRiSIS 2017, Dinard, France, September 19-21, 2017, Revised Selected Papers 12* (pp. 127-139). Springer International Publishing.
16. Udendhran, R., 2017, March. A hybrid approach to enhance data security in cloud storage. In *Proceedings of the Second International Conference on Internet of things, Data and Cloud Computing* (pp. 1-6).
17. Ming, J. and Xie, Z., 2024. Adaptive Particle Swarm Optimization Algorithm and Application Model Based on Diversity-Driven Optimization. IEEE Access.
18. Malik, M.W., Husna, D., Purnama, I.K.E., Nurtanio, I., Hidayati, A.N. and Ratna, A.A.P., 2020, November. Development of Medical Image Encryption System Using Byte-Level Base-64 Encoding and AES Encryption Method. In *Proceedings of the 6th International Conference on Communication and Information Processing* (pp. 153-158).
19. Prakash, V., Singh, A.V. and Khatri, S.K., 2019, June. A new model of light weight hybrid cryptography for internet of things. In *2019 3rd International conference on Electronics, Communication and Aerospace Technology (ICECA)* (pp. 282-285). IEEE.
20. Jun, W.J. and Fun, T.S., 2021. A new image encryption algorithm based on single S-box and dynamic encryption step. *IEEE Access*, *9*, pp.120596-120612.
21. Liu, C., Zhang, Y., Xu, J., Zhao, J. and Xiang, S., 2022. Ensuring the security and performance of IoT communication by improving encryption and decryption with the lightweight cipher uBlock. *IEEE Systems Journal*, *16*(4), pp.5489-5500.
22. Koppaka, A.K. and Lakshmi, V.N., 2024. An Efficient and Secured Big Data Storage in a Cloud-based Environment Using Hybrid Cryptography Algorithm and Rivest, Shamir, Adleman Algorithm. *International Journal of Intelligent Engineering & Systems*, *17*(1).

Received: August 13, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

23. Johns, M. and Dirksen, A., 2020, November. Towards enabling secure web-based cloud services using client-side encryption. In *Proceedings of the 2020 ACM SIGSAC Conference on Cloud Computing Security Workshop* (pp. 67-76).
24. Fernandez, E.B., 2020, October. A pattern for a secure cloud-based IoT architecture. In *Proceedings of the 27th Conference on Pattern Languages of Programs, Online* (pp. 12-16).
25. Kanchanadevi, P., Raja, L., Selvapandian, D. and Dhanapal, R., 2020, October. An Attribute based encryption scheme with dynamic attributes supporting in the hybrid cloud. In *2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)* (pp. 271-273). IEEE.
26. Gadde, S., Rao, G.S., Veesam, V.S., Yarlagadda, M. and Patibandla, R.S.M., 2023. Secure Data Sharing in Cloud Computing: A Comprehensive Survey of Two-Factor Authentication and Cryptographic Solutions. *Ingénierie des Systèmes d'Information*, *28*(6).
27. Ahmad, S., Mehfuz, S. and Beg, J., 2023. Hybrid cryptographic approach to enhance the mode of key management system in cloud environment. *The Journal of Supercomputing*, *79*(7), pp.7377-7413.
28. Ullah, S., Zheng, J., Din, N., Hussain, M.T., Ullah, F. and Yousaf, M., 2023. Elliptic Curve Cryptography; Applications, challenges, recent advances, and future trends: A comprehensive survey. *Computer Science Review*, *47*, p.100530.
29. Mohamed, K.M., 2017. *A Secure Lightweight Framework for Hosting and Consuming Web Services in Smart Mobile Devices* (Doctoral dissertation, George Mason University).
30. Belchior, R.A.P., 2019. JusticeChain: Using Blockchain To Protect Justice Data.
31. Zobaed, S. and Amini Salehi, M., 2022. Privacy-preserving clustering of unstructured big data for cloud-based enterprise search solutions. *Concurrency and Computation: Practice and Experience*, *34*(22), p.e7160.
32. Salim, A., Osamy, W., Khedr, A.M., Aziz, A. and Abdel-Mageed, M., 2020. A secure data gathering scheme based on properties of primes and compressive sensing for IoT-based WSNs. *IEEE Sensors Journal*, *21*(4), pp.5553-5571.
33. Gunathilake, N.A., Buchanan, W.J. and Asif, R., 2019, April. Next generation lightweight cryptography for smart IoT devices: implementation, challenges and applications. In *2019 IEEE 5th World Forum on Internet of Things (WF-IoT)* (pp. 707-710). IEEE.
34. S.B.J. Fursan Thabit, Alhomdy, "a new lightweight cryptographic algorithm for enhancing data security in cloud, Glob. Transitions Proc. (2021) 14–23.
35. Poojary, A., Kiran Kumar, V.G. and Nagesh, H.R., 2023. FPGA implementation novel lightweight MBRISI cipher. Journal of Ambient Intelligence and Humanized Computing, 14(9), pp.11625-11637.
36. Abdelaal, M.A., Moustafa, A.I., Kasban, H., Saleh, H., Abdallah, H.A. and Afifi, M.Y.I., 2025. DNA-Inspired Lightweight Cryptographic Algorithm for Secure and Efficient Image Encryption. Sensors, 25(7), p.2322.

Received: August 13, 2025