A Swarm Inspired Chaotic Map Evoked Attribute Encryption Framework Using Multi-Model Inputs in Cloud Environment

A. Jeneba Mary[1,*], K. Kuppusamy[2], A. Senthilrajan[3]

[1]Research Scholar, Department of Computational Logistics, Alagappa University, Karaikudi, Tamilnadu, India

[2]Formerly Professor& Head (i/c), Department of Computational Logistics, Alagappa University, Karaikudi, Tamilnadu, India

[3]Professor, Department of Computational Logistics, Alagappa University, Karaikudi, Tamilnadu, India

Emails: jenebamary@gmail.com; ksamyk@alagappauniversity.ac.in; senthilrajana@alagappauniversity.ac.in

Abstract

As an increasing number of people and corporations move their data to the cloud side, how to ensure efficient and secure access to data stored on the cloud side has become a key focus of current research. Attribute-Based Encryption (ABE) is largely recognized as the best access control method for safeguarding the cloud storage environment, and numerous solutions based on ABE have been developed successively. Attribute-based encryption (ABE), which provides fine-grained access control and ensures data confidentiality, is widely used in data sharing. Hence, the strong and lightweight encryption schemes need more limelight of implementation in ABE to overcome the tampering and leakage problem that may cause the severe consequences to the users. To solve this problem, this paper proposes the Swarm Inspired Chaotic Encryption principles for designing the CP-ABE Systems for effective data sharing process. This scheme utilizes the chaotic properties along with the swarm properties for every individual transmission that leads to the strong defence characteristics. The intensive experimentation is carried out using Multi-modal Inputs such as the biometric images and eye iris images. The extensive experimentation is carried out using the various standard tests such as NIST (National Institute of Standard and technology), communication cost (CC) and metrics such as NPCR, UACI, entropies has been evaluated and analysed. Furthermore, excellence of the proposed model is determined by comparing with the other existing schemes. The evaluation demonstrates the CC of proposed scheme is only 30% than other algorithms and passed all the 12 standard tests. The experimental results illustrate the proposed scheme has more advantage in exhibiting the more randomness and light weight characteristics for health care which can more defensive against the attacks

Keywords: Attribute based encryption; Chaotic Maps; Swarm Intelligence; Biometric Images; Multi-level Inputs

1. Introduction

Cloud computing, as a new and promising paradigm for information technology and services, provides consumers with simple, quick, and convenient options for data storage and sharing [1]. Due to its advantages such as unlimited storage resources and low maintenance cost, an increasing number of users and businesses are opting to migrate, their data to the cloud side. The rise in popularity of cloud computing can be attributed to its features such as cost reduction, pay per-usage, virtualization, on-demand access, multi-tenancy, and scalability. Users and data owner's store and share data with others. Consequently, cloud service providers have a responsibility to ensure trust and security for their users. As cloud users entrust sensitive and personal data to the cloud, the risk of data breaches by malicious intruders remains a significant concern. To guarantee the security of outsourcing data, the data owners usually encrypt their data before uploading them to the cloud side. However, with a vast amount of encrypted data stored in the cloud side, efficiently and securely accessing the desired data poses a challenge [2-4].

Attribute-Based Encryption (ABE), as a typical encryption method, offers a fine-grained access control for the cloud storage service. It ensures secure and efficient access to encrypted outsourced data. The earliest prototype of Attribute-Based Encryption (ABE) can be traced back to a vague notion of identity-based encryption in 2005 [5]. Then, the

DOI: https://doi.org/10.54216/JCIM.160111
Received: November 24, 2024 Revised: January 30, 2025 Accepted: February 27, 2025

concept of ABE was extended, and schemes for both small-scale and large-scale attribute sets were developed. For the first time, the Key-Policy Attribute-Based Encryption (KP-ABE) and Cipher text-Policy Attribute-Based Encryption (CP-ABE) methods were separated from ABE. [6].

The cipher text can be successfully decrypted to obtain the plaintext only when the attribute set meets the access policy in both KP-ABE [7] and CP-ABE [8], which implements fine-grained access control for encrypted data on the cloud server. However, in CP-ABE, the secret key is determined by the attribute set of the data user, and the cipher text is related to the access policy. On the contrary, the secret key is tied to the access structure and the cipher text is attached to the attribute set in KP-ABE. Since the data owner sets the access structure of CP-ABE, CP-ABE has become a widely adopted technique for securing data in cloud storage environments by users.

1.1 Problem Structure

Many methodologies such as Multi-authority CP-ABE systems [9], Hierarchical CP-ABE [10], Hybrid CP-ABE systems[11], Privacy–preserving CP-ABE [12]were proposed to strengthen the CP-ABE based encryption and decryption systems for the storing the enormous data in the cloud . However, these algorithms proved its vital role in providing the strong defense against the multiple attacks, data leakage problems and computational burden remains to be the bottleneck for leveraging the cognitive framework to ensure the privacy and secured cloud environment.

1.2 Motivation and Research Contribution

As discussed, existing methods that utilizes the different version of ABE to safeguard the confidentially of the data when it is stored on the cloud servers. However, considering the large volume of data, the refluxing problems and computational overhead prevents the secured cloud infrastructure for storing and retrieving the data. To solve the problem, this research article proposes the Multi-level Authenticated Chaotic Swarm Intelligence (MLA-CSI) based ABE systems to safeguard the data systems against the growing unknown attacks. In the proposed research, different combination of chaotic maps with the Tasmanian Devil Optimization Algorithm has been proposed to improve the CP-ABE systems with the reduced computational time and high-secured environment. The key contribution can be summarized as follows

The paper proposes a novel lightweight encryption and decryption scheme based on bio-inspired attribute encryption and decryption scheme with the high defensive characteristics provided by the combination Tasmanian Devil Optimization Algorithm and Chaotic Maps.

1. The paper introduces the Multi-Level Inputs such as Fingerprint, Iris Images to act as the strong catalyst for designing the strong encryption technique in the place of conventional systems. This improves the encryption performances over the other existing algorithms.
2. To test the proposed scheme's performance, communication cost is calculated for the cloud environments. Using this primitive parameter, the operational cost is determined and compared with recent techniques. The comparison shows that the proposed scheme is lightweight in design and requires lower operational cost overhead.
3. The result of the analysis and comparison with existing ABES schemes demonstrates that the proposed scheme is more dominant, productive, and secure against all active and passive attacks [13], and it achieves the goal of secure design.

The rest of the paper is organized as follows: Section-2 presents the different ABES protocol proposed by various authors. The preliminary overview of optimization, Henon maps and its properties are detailed in Section-3. The working mechanism of the proposed model, key generation process, encryption and decryption process are detailed in Section-4. The security analysis and experimental validation with comparative analysis is demonstrated in Section-5 Finally the paper is concluded with future enhancement in Section-6.

2. Related Work

Nair and Dharan (2024) [14] developed a multimodal biometric security system using separately extracted feature fusion-based CNN with bat optimization (SEFF-CNN-BO). The system combines iris, face, and fingerprint features with attribute-based encryption for secure key sharing. By incorporating bat optimization and user input string-based permutation with SHA-256 hashing, they achieved key revocability and enhanced security. Results demonstrated 99.56% accuracy and 99.64% recall, with proven resistance against known attacks and 100% key revocability. However, the computational complexity of processing multiple biometric modalities simultaneously may present challenges in real-time applications.

Tian et al. (2024) [15] introduced an attribute-based heterogeneous data privacy sharing (AB-HDPS) scheme for block chain-assisted Industrial IoT. Their approach enables PKI-based attribute-authorized users to search cipher text from

DOI: https://doi.org/10.54216/JCIM.160111
Received: November 24, 2024 Revised: January 30, 2025 Accepted: February 27, 2025

certificate less cryptosystem data owners. The system features multiple authorities for attribute key generation, white-box traceability, and subset-cover trees for attribute revocation. While demonstrating resistance to internal keyword guessing and chosen-plaintext attacks, the integration of block chain ensures traceability and audit capabilities. Nevertheless, the scheme's performance in high-throughput IoT environments requires further investigation.

Pointcheval and Schädlich (2024) [16] presented Multi-Client ABE (MC-ABE), extending multi-input ABE by separating encrypt or secret keys and introducing label-based joint decryption. Their construction supports various policy classes based on SXDH and overcomes previous limitations of standard assumption-based approaches. They also developed a compiler converting constant-parity MC-ABE into Multi-Client Predicate Encryption, with security proven under the LWE assumption. However, implementing large-scale distributed systems presents practical challenges.

Abdul Kader and Kumar (2023) [17] proposed a geometric octal zones distance estimation optimization algorithm with ABE (GOZDE-ABE) for securing real estate information using block chain. The system combines block chain's data integrity with ABE's access control, storing encrypted documents in IPFS with hash-based location tracking. The approach demonstrated improved security for business information and high-value transactions, though scalability concerns in handling large volumes of real estate transactions remain to be addressed.

Yang et al. (2023) [18] developed an ABE scheme for multi-cloud environments with data security classification. Their approach divides data into two security levels across different cloud providers, implementing CP-ABE for fine-grained access control with outsourced decryption. While proving effective against selective-attribute plaintext attacks and reducing computational overhead, the system's adaptation to dynamic multi-cloud environments requires further investigation to address potential scalability constraints.

Agrawal et al. (2022) [19] introduced pioneering work in multi-input predicate encryption (miPE) and multi-input attribute-based encryption (miABE). They developed the first two-input key-policy ABE for NC1 from LWE and pairings, and created a three-input ABE for NC1 by combining different construction approaches. Their compiler transforms multi-input ABE to multi-input PE using Lockable Obfuscation, providing the first improvement to witness encryption compression without relying on compact functional encryption. While groundbreaking, their theoretical frameworks are constrained by significant practical implementation complexities, which pose challenges to their large-scale adoption and real-world applicability.

Nagaraju and Boraiah (2022) [20] proposed a key-cipher-policy-based ABE (KCP) mechanism combining CP-ABE and KP-ABE approaches for cloud storage security. Their hybrid solution addresses key challenges in attribute revocation and key generation time while handling large attribute sets. The approach improves efficiency in key generation and provides enhanced access control for multimedia data in cloud environments. However, the system's performance under high concurrent access scenarios needs additional evaluation.

Zhang et al. (2021) [21] developed a hybrid encryption online/offline CP-ABE scheme for 5G networks, addressing computational limitations of mobile devices. Their approach uses symmetric encryption for data encapsulation and cloud user assistant (CUA) for offline calculations, incorporating verification mechanisms to prevent tampering. While demonstrating reduced computational overhead and fine-grained access control, the dependence on CUA availability could present operational challenges in certain network conditions.

Tarannum et al. (2020) [22] designed a multi-modal biometric authentication framework utilizing iris, facial, and fingerprint features for distributed applications. Their system implemented a novel integrity computational algorithm and encryption technique, achieving approximately 7% computational integrity bit change and 5% runtime improvement on large datasets. Though effective, the framework is constrained by its uncertain performance across varying environmental conditions and sensor qualities, necessitating deeper analysis.

Islam and Madria (2020) [23] presented ReVO-ABE, a directly revocable collusion-resistant ABE scheme, and built the Dynamic Multi-Group Secure Data Sharing (DMG-SDS) system. Their solution uniquely enables group operations like merging and splitting without affecting non-revoked users' keys, demonstrating superior performance compared to contemporary schemes. However, their approach faces scalability limitations in very large organizational settings, requiring further validation to ensure effectiveness.

3. Preliminaries Overview

The mathematical methodology for the Tasmanian Devil Optimization (TDO) algorithm is outlined in this segment. TDO is one of the most recent optimization techniques developed to mimic the natural behaviour of the Tasmanian devil, particularly during its foraging activities. The algorithm models the devil's strategies for finding food, which include either attacking and consuming live prey or scavenging from carcasses. TDO has been tested across 23 benchmark functions to assess its effectiveness and has been further applied to optimize four engineering design

DOI: https://doi.org/10.54216/JCIM.160111
Received: November 24, 2024 Revised: January 30, 2025 Accepted: February 27, 2025

problems. Its performance is validated through comparisons with eight established optimization techniques, with results affirming its strong competitive performance. The core phases of the TDO process are detailed below.

3.1 Initialization

Tasmanian Devil Optimization (TDO) is similar to other population-based methods that begin with an iterative process-involving search agents known as Tasmanian devils. In this process, a set of agents is randomly generated within the defined search space. Every agent represents a vector, with its elements corresponding to the number of variables in the problem. This initial step can be expressed as follows:

$$X_{ij} = x_j^{min} + rand.(x_j^{max} - x_j^{min}), i = 1,2,\dots,M, j = 1,2,\dots,n \quad (1)$$

In the Tasmanian Devil Optimization (TDO) algorithm, the value of "$rand$ " denotes a stochastic variable uniformly distributed within the interval [0, 1]. The parameters $x_j^{min} and\ x_j^{max}$ denote the minimum and maximum boundaries for the j-th dimension of the search space. Here, M refers to the population size of Tasmanian devils, and n corresponds to the number of variables. Once the initialization phase is complete, the fitness of each candidate solution is measured using the objective function (OF). The best-performing solution, based on the OF, is considered the optimal member of the population and is updated during each iteration through the feeding strategies of Tasmanian devils. Each devil has a 50% probability of either scavenging carrion or hunting for food. Thus, during this each iteration one of these two strategies is randomly selected to update the position of each Tasmanian devil.

3.2 Eating carrion: exploration stage

Tasmanian devils sometimes prefer scavenging for carrion rather than hunting live prey. In their habitat, other predators often hunt large prey but leave behind remains they cannot fully consume. Additionally, these predators may not be able to finish their meal before a Tasmanian devil arrives. As a result, the devil takes advantage of these leftovers. This scavenging behaviour mirrors the iterative approach in problem-solving algorithms, where Tasmanian devils' method of finding carrion mimics the TDO (Tasmanian Devil Optimization) algorithm's search for an initial optimal solution. Each Tasmanian devil's position is akin to a potential solution in the search space, and other individuals in the population represent different carrion sources. The Tasmanian devil then selects one of these carrion locations at random as its target.

$$C_i = X_k, i = 1,2,\dots,M, k \in \{1,2,\dots,M | k \neq i\} \quad (2)$$

where C_i signifies the chosen carrion for the i[th] Tasmanian devil and k is arbitrarily chosen from 1 to M.

In light of the selected information, the updated location of the Tasmanian devil is determined as follows.

$$x_{i,j}^{\text{new},S1} = \begin{cases} x_{ij} + r \cdot (c_{ij} - I \cdot x_{ij}), & F_{C_i} < F_i \\ x_{ij} + r \cdot (x_{ij} - c_{ij}), & \text{otherwise} \end{cases} \quad (3)$$

$$X_i = \begin{cases} X_i^{\text{new},S1}, & F_i^{\text{new},S1} < F_i \\ X_i, & \text{otherwise} \end{cases} \quad (4)$$

In this context, $X_i^{\text{new},S1}$, $x_{i,j}^{\text{new},S1}$ represents the updated location of the ith Tasmanian devil, calculated which relies on the first strategy. The variable, $X_i^{\text{new},S1}$,$x_{i,j}^{\text{new},S1}$, refers to the specific element in the jth dimension. Additionally, F_{C_i} corresponds to the objective function value of the selected carrion. The parameter r is a randomly generated number between 0 and 1, and I is a randomly chosen integer, either be 1 or 2.

3.3. Eating prey (exploitation phase)

At this stage, the Tasmanian devil engages in hunting and feeding on its prey, which occurs in two distinct phases. In the initial phase, it surveys the environment to identify potential prey that it can attack. Following this, in the second phase, once the Tasmanian devil approaches its target, it begins the chase, captures, and consumes the prey. The mathematical modeling of the first phase is described by Equations (5) to (7). In the second phase, the Tasmanian devil's position is updated by considering the locations of other members in the population, which serve as the prey's positions. A random member (k[th]) is selected to represent the prey's location during this process of prey selection. This procedure is outlined as follows.

$$P_i = X_k, i = 1,2,\dots,M, k \in \{1,2,\dots,M | k \neq i\} \quad (5)$$

Based on the chosen prey, the subsequent step involves determining the updated location of the Tasmanian devil, as outlined below.

DOI: https://doi.org/10.54216/JCIM.160111
Received: November 24, 2024 Revised: January 30, 2025 Accepted: February 27, 2025

$$x_{i,j}^{\text{new},S2} = \begin{cases} x_{ij} + r \cdot (p_{ij} - I \cdot x_{ij}), & F_{P_i} < F_i \\ x_{ij} + r \cdot (x_{ij} - p_{ij}), & \text{otherwise} \end{cases} \quad (6)$$

$$X_i = \begin{cases} X_i^{\text{new},S2}, & F_i^{\text{new},S2} < F_i \\ X_i, & \text{otherwise} \end{cases} \quad (7)$$

The updated location of the i[th] Tasmanian devil, denoted as $X_i^{\text{new},S2}$, represents its new location using the second strategy. The element corresponding to the jth dimension of this new position is referred to as $x_{i,j}^{\text{new},S2}$. The term Finew, S2 represents the objective function value for the updated position, while $F_{P_i}$is the objective function value of the selected prey.

In this process, the Tasmanian devil simulates chasing its prey within the targeted location. This behavior is captured through the mathematical formulations in Equations. (8) – (10), which model the pursuit stage. The devil's location is considered the center of a surrounding area where it tracks its prey. The radius of this neighborhood, determined by Eq. (8), defines the zone within which the pursuit occurs. A new location, reflecting the Tasmanian devil's movement during the chase, is then calculated using Eq. (9).

$$R = 0.01(1 - t/T), \quad (8)$$

$$x_{i,j}^{\text{new}} = x_{ij} + (2r - 1) \cdot R \cdot x_{ij} \quad (9)$$

$$X_i = \begin{cases} X_i^{\text{new}}, & F_i^{\text{new}} < F_i \\ X_i, & \text{otherwise} \end{cases} \quad (10)$$

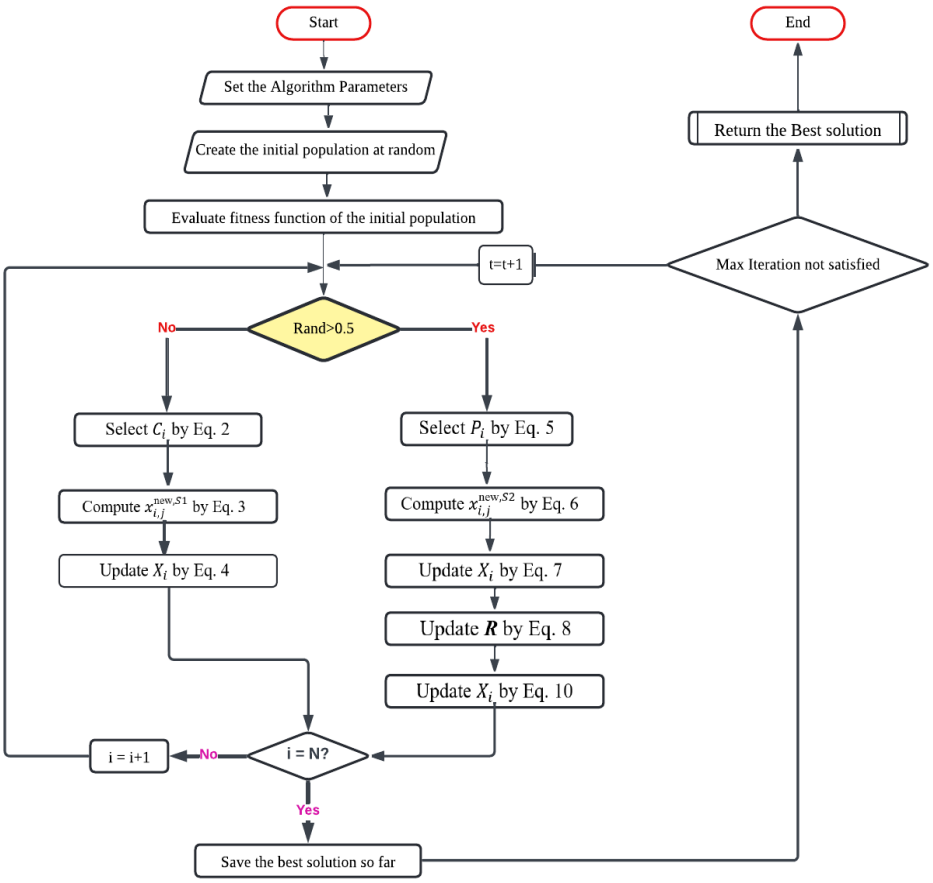


Figure 1. Overall Working Architecture of the Proposed Tasmanian devil Optimization Algorithm

In this context, R represents the neighborhood radius around the attack location, while t and T correspond to the current iteration and the maximum number of iterations, respectively. X_i^{new} Refers to the updated position of the iii[th] Tasmanian

DOI: https://doi.org/10.54216/JCIM.160111
Received: November 24, 2024 Revised: January 30, 2025 Accepted: February 27, 2025

devil in proximity to X_i, $x_{i,j}^{new}$denoting the jth component or variable of X_i^{new}. Additionally, ith-indicates the new value of the objective function for X_i^{new} . A visual representation of the Tasmanian Devil Optimization (TDO) algorithm can be found in Figure 1.

3.4 Scroll Maps – Overview and Properties

Dynamical systems with multi scroll attractors can present more complex dynamics than general chaotic systems with mono-scroll attractors. The State Space equation for automatic chaotic system is given by

$$\dot{x}_1 = -ax_1 + bx_2x_3 \quad (11)$$
$$\dot{x}_2 = -cx_2^3 + dx_1x_3 \quad (12)$$
$$\dot{x}_3 = ex_3 - fx_1x_2 \quad (13)$$

The above equations (11), (12), (13) can be modified by the adding the hyperbolic equation $p_1\, tanh(x_2 + g)$ which is given in equation

$$\dot{x}_1 = -ax_1 + bx_2x_3 \quad (14)$$
$$\dot{x}_2 = -cx_2^3 + dx_1x_3 \quad (15)$$
$$\dot{x}_3 = ex_3 - fx_1x_2 + p_1\, tanh(x_2 + g) \quad (16)$$

Chaotic attractor is obtained when$a = 2$, $b = 6$, $c = 6$, $d = 3$, $e = 3$, $f = 1$, $p_1 = 1$, $g = 2$and the chosen initial conditions are $[x_1(0), x_2(0), x_3(0)] = [0.1, 0.1, 0.6]$.

When the hyperbolic function is introduced in first state with the parameter $g = -3$ and for the initial conditions$[0.1, -0.1, -0.6]$ it shows double scroll attractor which is shown in Figure 2.

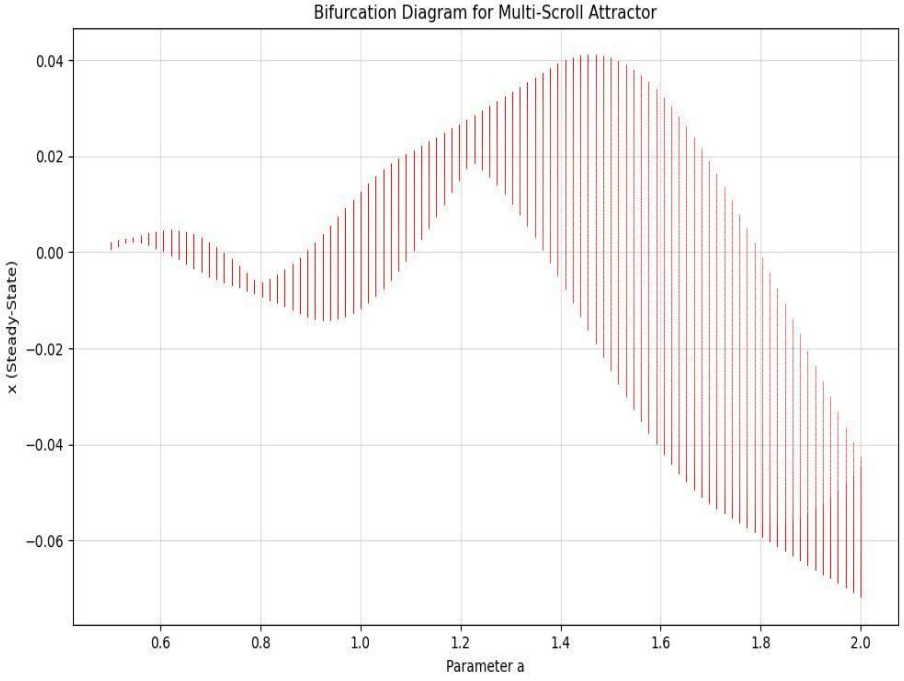


Figure 2. Non –Linear Behavior diagram of Multi-Scroll Attractors

3.5 Henon Maps- Principles of working

Henon Maps [24] are the disruptive quadratic and non-linear maps given by its characteristic equation

$$X_{n+1} = 1 - aX_n^2 + Y_n \quad (17)$$
$$Y_{n+1} = 1 - bX_n \quad (18)$$

DOI: https://doi.org/10.54216/JCIM.160111
Received: November 24, 2024 Revised: January 30, 2025 Accepted: February 27, 2025

The classical maps depends on the two parameters 'a' and 'b' which has the values of a=1.4 and b=1.3. For the classical values, Henon map is chaotic. For the other values of and b, henon maps may exhibit the chaotic behavior, which can be identified with the several times of iteration. Figure 3 represents the chaotic behavior of the henon maps using classical values.

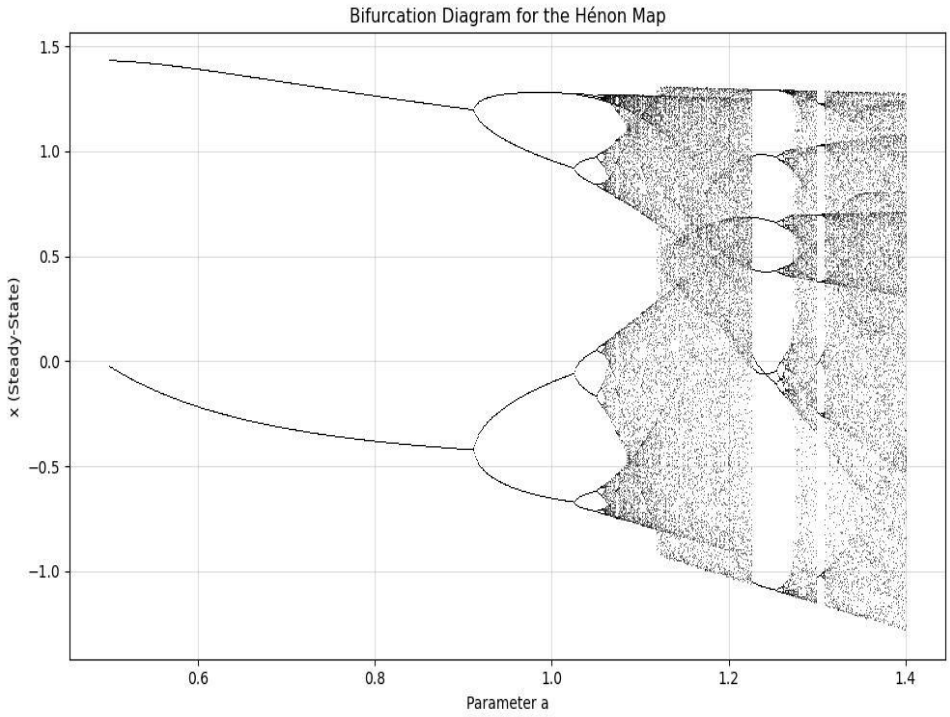


Figure 3. Non –Linear Behavior diagram of Henon Maps

4. System Overview

Architecture of the proposed system is shown in Figure 4. The system model consists of four entities: Central Authorization (CA), Data User (DU), Data Owner (DO), and Cloud Service Providers (CSPs).

4.1 Data Owner (DO): The DO is a party that possesses large amounts of data to be uploaded to the cloud side. It is in charge of defining the access structure and, then, generating the cipher text of the data. In addition, it is also responsible for dividing the entire data. The DO's entire data are divided into two parts based on their level of security, which are encrypted and then sent to CSPA and CSPB, respectively.

4.2 Cloud Service Providers (CSPs): An MCSP is a party that offers a range of services, such as data storage.

4.3 Data User (DU): The DU is a party that desires to access the ciphertext stored in the CSP. If the attribute set of the DU meets the access structure, it can use the secret key to decrypt the cipher text and obtain the data. Note that only by decrypting the encrypted data in cloud service can the entire data be obtained

4.4 Central Authority (CA): The CA is a fully trusted entity that performs any assigned tasks according to the protocol specifications and generates the correct output. It is in charge of generating the secret key for the DU and CSPA, as well as generating the new secret key for the DU based on the attribute set.

In the proposed model, cloud service providers are used to store data and divide the ABE-DSC security level of the cloud service providers into two levels. It should be emphasized that, depending on the needs of the DO, the suggested model can be extended to several security levels by utilizing secured cloud service providers.

DOI: https://doi.org/10.54216/JCIM.160111
Received: November 24, 2024 Revised: January 30, 2025 Accepted: February 27, 2025

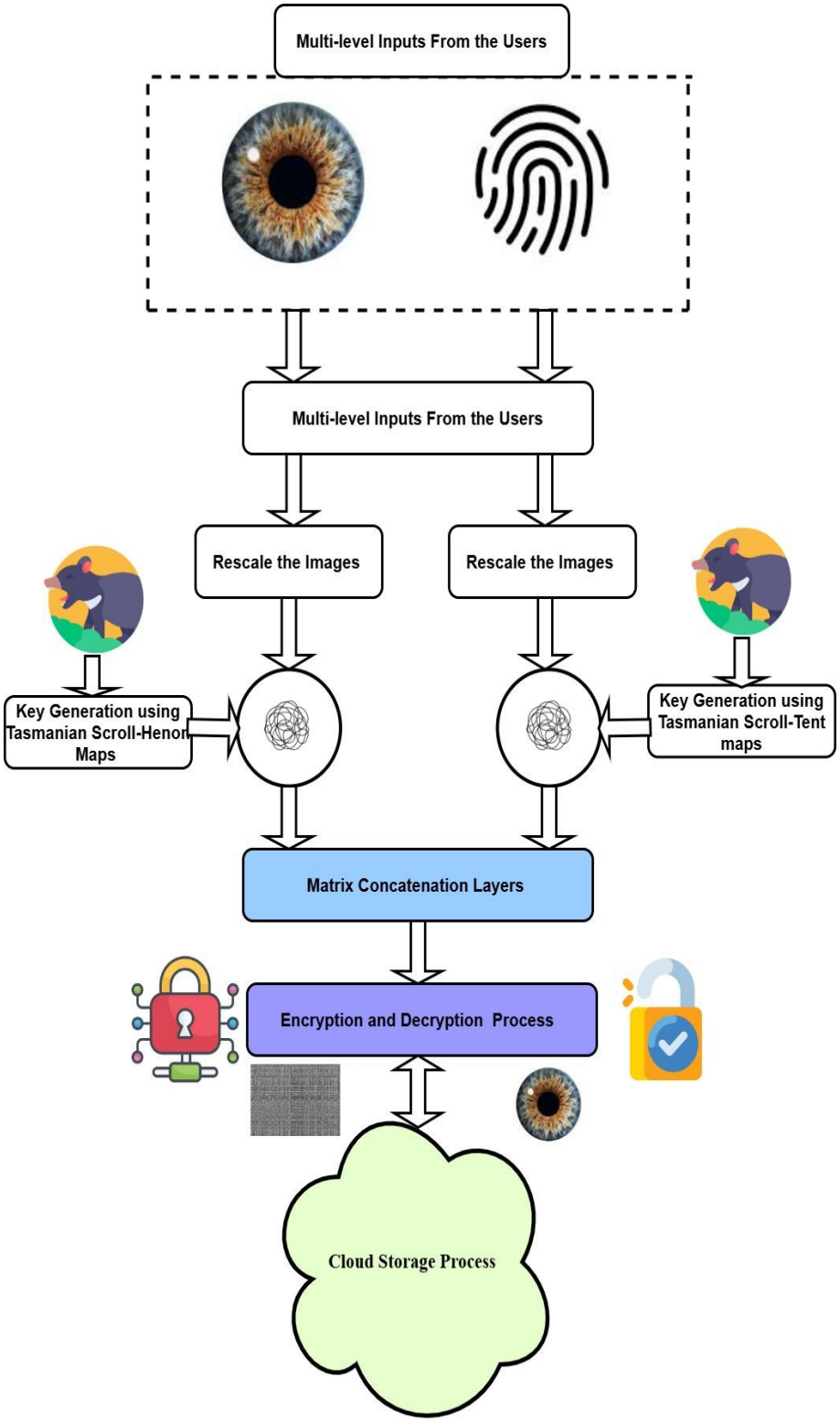


Figure 4. Overall System Architecture for the Proposed Encryption Schemes Adopted in CP-ABE Systems.

4.5 Key Generation Process

In this component, high dynamic keys are formulated by using the hybrid combination of Henon maps and Tasmanian devil optimized scroll maps. The detailed systematic process of key generation is presented below in Algorithm-1.

DOI: https://doi.org/10.54216/JCIM.160111
Received: November 24, 2024 Revised: January 30, 2025 Accepted: February 27, 2025

Algorithm-1 Key Generation Process

Step 1: As the first step, initial conditions for the henon maps have been generated. In this case, output from the henon maps(X) are used as the initial conditions of generate the output maps from the Scroll Inspired devil (SID) model

Step 2: The SID are used to generate the different and high random keys which are highly susceptible against the any malfunctions

Step 3: The Biometric Images (I) and (I) are permutated (P) to form the high randomness key (E_k). The formed key is deployed for further process

$$E_b = Permutate\big(I, SID(X)\big)$$

$$where\ I = \ Bio - metric\ data$$

Step 4: The Iris images and novel SID are diffused to form any High randomness keys, which are mathematically expressed as

$$E_i = Diff\big(\mathrm{E}, SID(X)\big)$$

$$where\ I = Iris\ Image\ data$$

Step 5: The two keys E_k and E_c are concatenated to generate the new keys used for the encryption process that is mathematically expressed as

$$E(T) = E_k\ Concate\ Ei$$

4.6 Encryption Process

Encryption with hybrid maps adds the security and privacy levels in the input parameters. (Algorithm- 2). In case of the encryption with SID maps, diffusion operation is applied between each element of the input data (both biometric and IRIS image) and chaotic value generated by hybrid keys. Diffusing the i^{th} element of the image data with the random key values produces the strong encrypted data. Before encryption , all the keys and data are rescaled to common factor as 256(for reducing the complexity in the process).In the similar fashion, reversible operation (Algorithm 3), as performing diffusion operation between the encrypted data and the same encryption key (or parameter) will yield the original plain data . The distinct characteristics exhibited by chaotic systems, including determinism, periodicity, and sensitivity to initial conditions, make them a compelling option for constructing cryptographic systems. One of the major advantages of Chaos-based encryption techniques is their computational efficiency [25].

Step	Algorithm-2// Proposed Encryption Schemes
1	Input : Data Parameters (B),(I)
2	Output : Encrypted Data (E)
3	Key generation Process using Algorthm-1 //E(T) is total key structure generated
4	Rescale the B,I, E(T)

DOI: https://doi.org/10.54216/JCIM.160111
Received: November 24, 2024 Revised: January 30, 2025 Accepted: February 27, 2025

5	For i= 1 to n iteration
6	E1(i) = B(i) * E(Ti) E2(i) = I(i) * E(Ti)
7	End
8	E =Concat (E1 ,E2)
9	The output from the encryption process

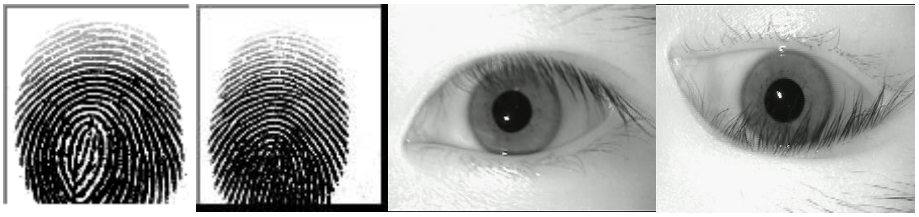
Step	**Algorithm-3// Proposed Decryption Schemes**
1	Input : Encrypted Data E
2	Output : Original Data parameters (B),(I)
3	Key generation Process using Algorthm-1 //E(T) is total key structure generated
4	Rescale the B,I, E(T)
5	For i= 1 to n_iteration
6	B(i) = E1(i) / E(Ti) I(i) = E2(i) / E(Ti)
7	End
8	Retrieving the Original Data B, I
9	The output from the decryption process

As mentioned in Algorithm-2 & Algorithm-3, encryption and decryption process involves the following phases: 1) Key generation process: The keys are generated by iterating the different initial conditions of SID maps. 2) Diffusion process is involved between the data and scroll keys to form the encrypted data. The main objective of this operation is to make the non-linear relationship between the original and encrypted data. Also in the encryption process, multiple iterations are employed to update the different random keys. In each iteration, the key may undergo the changes to introduce additional randomness and strengthen the security of the encryption.4) Final encrypted output is more random and statistically independent with the original data. 5) The reversible process of decryption is involved with same chaotic map iteratively to the cipher data using identical initial conditions, parameters and key as in the encryption phase to retrieve the original plain data.

5.1 Result Analysis

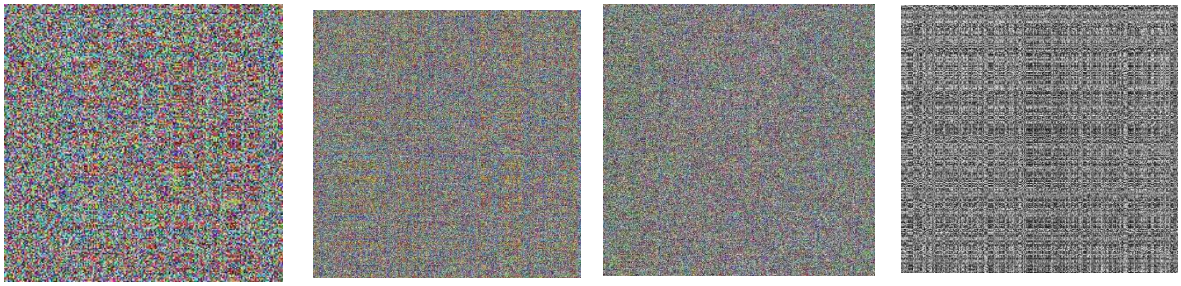
This section deals with the security analysis for the proposed S-DAC Systems for encrypting the different set of images. Thegeneral fingerprint and iris images are used for testing the proposed schemes. Figure 5 shows the input Images and Figure6 shows the encrypted images. From this, it is clear that the encrypted images are truly scrambled which is undefined for identification.

DOI: https://doi.org/10.54216/JCIM.160111
Received: November 24, 2024 Revised: January 30, 2025 Accepted: February 27, 2025



(a) (b) (c) (d)

Figure 5. Sample Input Images from the two different Datasets



(a) (b) (c) (d)

Figure 6. Encrypted Images from the Sample Datasets

5.2 Differential Attack Analysis:

The property of cipher key should be very sensitivity to slight change for resisting side channel attacks. In order to test the key sensitivity, NPCR and UACI were calculated to measure the performance of encryption algorithm with the respect to the secret key. The changes ares introduced in the cipher keys formed by the proposed S-boxes keeping the other bits as unchanged. The NPCR and UACI for the different encrypted images are calculated using following mathematical expression and depicted in the table II and I. It is clear that proposed s-box exhibits more sensitivity to the changes.

$$NPCR = \frac{\sum_{i,j} E(i,j)}{L} * 100 \quad (19)$$

$$UACI = \frac{1}{L}\sum_{i,j} \frac{|f(i,j) \neq f(i,j)|}{256} * 100 \quad (20)$$

where

$$E(i,j) = \begin{cases} 1, f(i,j) \neq f(i,j) \\ 0, f(i,j) = f(i,j) \end{cases} \quad (21)$$

Table 1: Illustration of NPCR and UACI for Biometric Cipher Images

SL.NO	No of Bits Change	NPCR (%)	UACI
01	10%	99.895%	33.97%
02	20%	99.89%	33.96%
03	30%	99.83%	33.92%
04	40%	99.81%	33.90%

DOI: https://doi.org/10.54216/JCIM.160111
Received: November 24, 2024 Revised: January 30, 2025 Accepted: February 27, 2025

05	50%	99.82%	34.92%
06	60%	99.79%	33.89%
07	70%	99.82%	33.90%
08	80%	99.85%	33.95%
09	90%	99.82%	33.93%
10	100%	99.83%	33.95%

Table 2: Illustration of NPCR and UACI for IRIS Cipher Images

SL.NO	No of Bits Change	NPCR (%)	UACI
01	10%	99.89%	34.59%
02	20%	99.90%	33.97%
03	30%	99.81%	34.89%
04	40%	99.9%	33.87%
05	50%	99.87%	34.70%
06	60%	99.85%	34.89%
07	70%	99.89%	34.89%
08	80%	99.83%	33.50%
09	90%	99.85%	34.9%
10	100%	99.89%	33.84%

5.3 Adjacent Pixel Correlation Analysis:

The normal images usually have high correlations among the pixels. The encrypted images will have low correlations between the pixels. To evaluate the correlations to prove the strength of the encryption, we have selected nearly above test images and adjacent pixel point correlation of an image has been calculated by the following mathematical expressions.

$$R_{xy} = \frac{cov(a,b)}{\sqrt{E(x)E(y)}} \quad (22)$$

$$cov(a,b) = D\{[a - D(a)][b - D(b)]\} \quad (23)$$

$$e(a) = \frac{1}{n}\sum_{i=1}^{n} a_i \quad (24)$$

$$L(x) = \frac{1}{n}\sum_{i=1}^{n}[a_i - a(x)]^2 \quad (25)$$

Where e(a) and L(x) represents the expectations and variance of the plain text images and cipher image datasets. Table III presents the correlation coefficient analysis between the plain image and its corresponding cipher images.

DOI: https://doi.org/10.54216/JCIM.160111
Received: November 24, 2024 Revised: January 30, 2025 Accepted: February 27, 2025

Table 3: Representation of the Correlation Coefficient Analysis between the Plain Image and Cipher Images

Details	Plain Images			Cipher Images		
	Horizontal	**Vertical**	**Diagonal**	**Horizontal**	**Vertical**	**Diagonal**
Sample Biometric-1	99.909	99.989	99.950	0.00000333	0.00411	0.00000490
Sample Biometric-2	98.6575	98.566	98.900	-0.0001234	0.000223	0.000094
Iris Image-1	235.890	228.900	228.08	0.0000678	0.000012	0.0000303
Iris Image-2	432.900	444.890	442.900	0.00000562	0.000007	000.02323

5.4 Information Entropy Analysis:

Information entropy is the measure of randomness that reflects the highest degree of uncertainty of image information. The higher the entropy values can prove higher randomness of cipher images. The mathematical expression for the entropy calculation is given by

$$g(m) = \sum_{l}^{l-1} q(m) \log_2 \frac{1}{q(m_i)} \quad (26)$$

Where l represents the gray level. The q (m) is the probability of gray value is appearing in the image matrix. For8-bitgrayimage, length of the bits is taken as 256. For good encrypted images, entropy value should be 8. The entropy values obtained for the different images sets are tabulated in table IV.

Table 4: Entropy values for the different image datasets

Images tested	**Entropy Values**
Sample Biometric-1	7.999992
Sample Biometric-2	7.999993
Iris Image-1	7.999994
Iris Image-2	7.999995

5.5 Computational Time Analysis:

Besides checking the encryption process, any encryption schemes should have faster response to encrypt the data. Since our proposed algorithm involves the both prediction and encryption, we have taken only the encryption time for the image once the attack is injected. We have taken 256 X 256 input images for this analysis and calculated time for the different image sets are given in table V.

Table 5: Computational Time Complexity Analysis

Sl.no	Image Datasets	Encryption time(s)
01	Sample Biometric-1	0.456
02	Sample Biometric-2	0.432
03	Iris Image-1	0.401
04	Iris Image-2	0.438

DOI: https://doi.org/10.54216/JCIM.160111
Received: November 24, 2024 Revised: January 30, 2025 Accepted: February 27, 2025

5.6 Randomness Test Analysis

The security aspects of any encryption system relate highly to the key used in encrypting/decrypting the communicated messages. As the encryption scheme that will be used is symmetric, once the adversary possesses the key, w device becomes vulnerable to all different attacks. Therefore, we must ensure that the key generator is truly random and it cannot tic approaches.

In addition, pseudorandom numbers generated for cryptographic applications must be unpredictable: if the initial conditions are unknown, the adversary cannot foresee the next output bit in the sequence generated even if he/she possesses any knowledge about the previous random numbers in the sequence. The National Institute of Standards and Technology (NIST) to ensure that the given random or Pseudo-Random generator can be used for cryptographic purposes describe a set of statistical tests for the randomness of number sequences. The described procedures aim to detect any deviation of a given binary sequence from being random. A poorly designed generator mostly explains the deviation. The research work uses nearly various statistical tests described by the NIST to prove the high randomness is achieved in the keys. In this test, key generated every iteration are converted into binary values using the python libraries.

From Table VI, it is clear that the proposed algorithm successfully passes all NIST test specifications, demonstrating its robustness and reliability in various statistical evaluations.

Table 6: NIST Test Performance of the Proposed Algorithm

Sl. No	NIST Test Specification	Status of test
1	DFT Test	PASS
2	Run Test	PASS
3	Long Run Test	PASS
4	Frequency Test	PASS
5	Block Frequency Test	PASS
6	Frequency Mono Test	PASS
7	Overlapping Template of all One’s test	PASS
8	Linear Complexity Test	PASS
9	Matrix Rank Test	PASS
10	Lempel-ZIV Compression Test	PASS
11	Random Excursion Test	PASS
12	Universal Statistical Test	PASS

5.7 Comparative Analysis

To prove the excellence of the proposed model, encryption time and decryption time are measured for the each existing model to encrypt and decrypt the user data

DOI: https://doi.org/10.54216/JCIM.160111
Received: November 24, 2024 Revised: January 30, 2025 Accepted: February 27, 2025

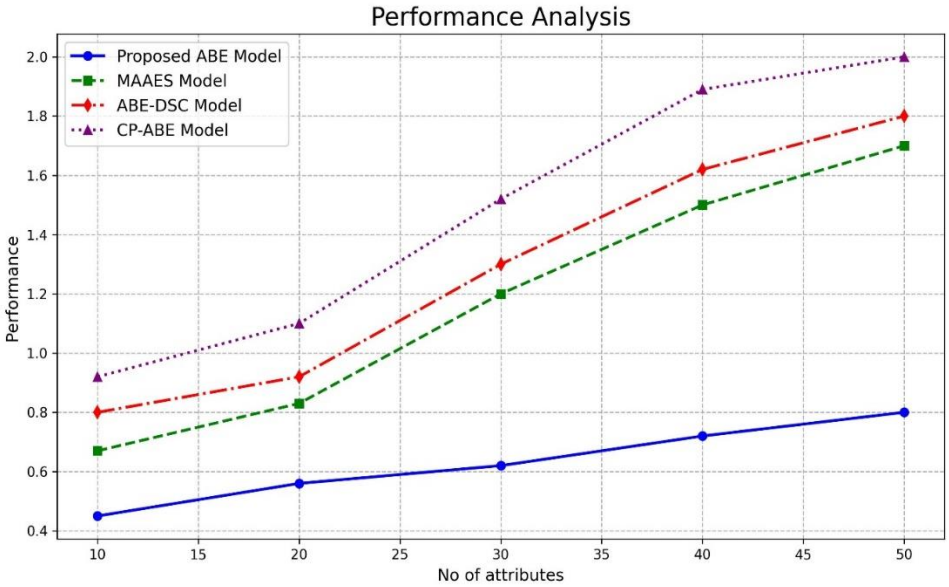


Figure 7. Encryption Time for the Different Model in encrypting the multi-level inputs

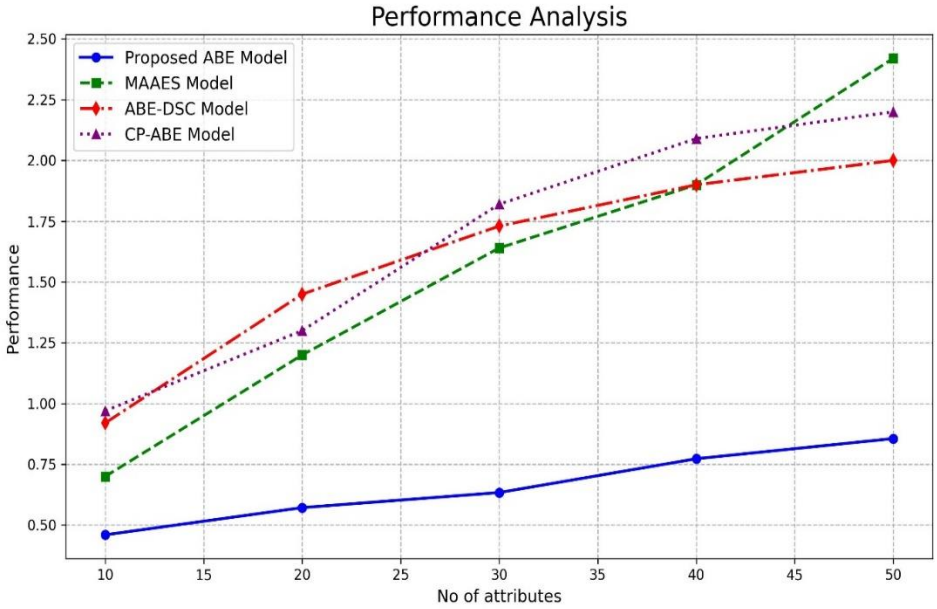


Figure 8. Decryption Time for the Different Model in decrypting the multi-level inputs

The proposed model has been designed and implemented for assessing information security, integrity, non-tampering and confidentiality in IoT data communication. The proposed model that has been built on novel ABE cryptographic technique has improved the internet security that has been illustrated in Figures (7-8). The keys generated using adaptive theory will be embedded as private keys in the proposed system. The client uses the private key to decrypt data from the cloud server. However, if encryption takes too little time, there is a higher risk of intruders hacking the data. Hence, the experimentation is carried out for measuring the encryption time of the proposed model. To establish the supremacy of the proposed model, existing algorithms such as CP-ABE, MAASE-ABE, and ABE-DS are considered. Figures7-8 shows the comparative analysis of different algorithms in generating the encrypted data. From experimentation, CP-ABE has produced the longer time for the small size data, which may increase the probability for intruder to tamper the medical data. Hence, it is worthy to prove the integration of chaos has considerable effect on the performance of encryption time.

DOI: https://doi.org/10.54216/JCIM.160111
Received: November 24, 2024 Revised: January 30, 2025 Accepted: February 27, 2025

However, since the generated keys depend on the inputs, the encryption time may be slightly longer for deployment in the proposed system. MAASE-ABE and ABE-DS has produced considerable amount of time. Moreover, they have added more randomness and computational unpredictability as par with the proposed model. However, the CP-ABE AND ABE-DS consumes more time, makes its unsuitable for deploying for the strong defensive characteristics. Hence, the results demonstrates the proposed model has provided more randomness and exhibits light weight behavior (integration of hybrid chaotic systems) that can ensure the high security and integrity in Cloud services

6. Conclusion and Future Enhancement

In this research work, a lightweight, swarm chaotic based ABE scheme has been proposed for Cloud data storage and access. The novel Tasmanian devil evoked hybrid chaotic encryption and decryption schemes for designing an efficient ABE schemes. The intensive experimentation has been carried out and NIST tests are calculated. The performance of designed encryption process has been compared with the other existing methods deployable for the Cloud applications. The results show that the proposed model is faster than the other existing models without pricing the data security and integrity. Besides, the proposed schemes pass the NIST statistical tests that prove its high randomness behavior that can defend against any attack. Hence, the proposed scheme has a higher level of security with fewer computations and makes its applicable to cloud services.

As the future scope, the proposed schemes can further be enhanced by the reducing the computations so that it can be deployable in any IoT devices used for smart health care applications.

Acknowledgement:

This work has been financially supported by the RUSA – Phase 2.0 grant, as sanctioned in Letter No. F. 24-51/2014-U, Policy (TN Multi-Gen), Department of Education, Government of India, dated October 9, 2018

References

[1] A. Adeel, M. Ali, A. N. Khan, T. Khalid, F. Rehman, Y. Jararweh, and J. Shuja, "A multi-attack resilient lightweight IoT authentication scheme," *Trans. Emerg. Telecommun. Technol.*, vol. 33, no. 3, p. e3676, 2022, doi: 10.1002/ett.3676.

[2] N. Alassaf, B. Alkazemi, and A. Gutub, "Applicable light-weight cryptography to secure medical data in IoT systems," *J. Res. Eng. Appl. Sci.*, vol. 2, no. 2, pp. 50–58, 2017, doi: 10.46565/jreas.2017.v02i02.002.

[3] N. Alassaf and A. Gutub, "Simulating light-weight-cryptography implementation for IoT healthcare data security applications," *Int. J. E-Health Med. Commun.*, vol. 10, no. 4, pp. 1–15, 2019, doi: 10.4018/IJEHMC.2019100101.

[4] S. Xu, J. Yuan, G. Xu, Y. Li, and X. Liu, "Efficient ciphertext-policy attribute-based encryption with blackbox traceability," *Inf. Sci.*, vol. 540, pp. 389–404, Oct. 2020.

[5] C. Ge et al., "Revocable attribute-based encryption with data integrity in clouds," *IEEE Trans. Dependable Secure Comput.*, vol. 9, no. 5, pp. 2864–2872, 2022, doi: 10.1109/TDSC.2021.30659992446.

[6] L. Guo, X. Yang, and W. C. Yau, "TABE-DAC: Efficient traceable attribute-based encryption scheme with dynamic access control based on blockchain," *IEEE Access*, vol. 9, pp. 8479–8490, 2021, doi: 10.1109/ACCESS.2021.3049549.

[7] R. Guo, G. Yang, H. Shi, Y. Zhang, and D. Zheng, "O3-R-CP-ABE: An efficient and revocable attribute-based encryption scheme in the cloud-assisted IoMT system," *IEEE Internet Things J.*, vol. 8, no. 11, pp. 8949–8963, 2021, doi: 10.1109/JIOT.2021.305554.

[8] S. Hu, X. Wang, H. He, and T. Zhong, "Complex and flexible data access policy in attribute-based encryption," *J. Supercomput.*, vol. 78, no. 1, pp. 1010–1029, 2022, doi: 10.1007/s11227-021-03867-5.

[9] M. Jammula, V. M. Vakamulla, and S. K. Kondoju, "Performance evaluation of lightweight cryptographic algorithms for heterogeneous IoT environment," 2022.

[10] X. Fu et al., "A survey of lattice-based expressive attribute-based encryption," *Comput. Sci. Rev.*, vol. 43, p. 100438, 2022, doi: 10.1016/j.cosrev.2021.100438.

[11] M. M. AbdulKader and S. G. Kumar, "An efficient geometric octal zones distance estimation and attribute-based encryption for secure transfer of sensitive data," *Telecommun. Syst.*, vol. 84, no. 2, pp. 251–270, Feb. 2023, doi: 10.1007/s11235-023-01030-4.

DOI: https://doi.org/10.54216/JCIM.160111
Received: November 24, 2024 Revised: January 30, 2025 Accepted: February 27, 2025

[12] Y. Ming, B. He, and C. Wang, "Efficient revocable multi-authority attribute-based encryption for cloud storage," *IEEE Access*, vol. 9, pp. 42593–42603, 2021.

[13] Z. Lu et al., "Novel searchable attribute-based encryption for the Internet of Things," *Wireless Commun. Mobile Comput.*, vol. 2022, p. 8350006, 2022, doi: 10.1155/2022/8350006.

[14] M. S. Nair and S. Dharan, "Design of a multimodal biometric-based protection system by generation of a revocable cryptographic key using separately extracted feature fusion-based convolutional neural network with bat optimization (Version 1, Preprint)," *Res. Square*, 2024, doi: 10.21203/rs.3.rs-4853162/v1.

[15] T. Tian et al., "Attribute-based heterogeneous data privacy sharing in blockchain-assisted industrial IoT," *IEEE Internet Things J.*, 2024, doi: 10.1109/JIOT.2024.3510872.

[16] D. Pointcheval and R. Schädlich, "Multi-client attribute-based and predicate encryption from standard assumptions," *Cryptol. ePrint Arch.*, Paper 2024/1945, 2024, doi: 10.1007/978-3-031-78020-2_2.

[17] M. M. AbdulKader and S. G. Kumar, "An efficient geometric octal zones distance estimation and attribute-based encryption for secure transfer of sensitive data," *Telecommun. Syst.*, vol. 84, pp. 251–270, 2023, doi: 10.1007/s11235-023-01030-4.

[18] G. Yang et al., "An efficient attribute-based encryption scheme with data security classification in the multi-cloud environment," *Electronics*, vol. 12, no. 20, p. 4237, 2023, doi: 10.3390/electronics12204237.

[19] S. Agrawal, A. Yadav, and S. Yamada, "Multi-input attribute-based encryption and predicate encryption," *Lecture Notes in Computer Science*, vol. 10, pp. 1007–978, 2022, doi: 10.1007/978-3-031-15802-5_21.

[20] K. M. Nagaraju and R. Boraiah, "Key-cipher policy attribute-based encryption mechanism for access control of multimedia data in cloud storages," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 28, no. 1, pp. 545–550, 2022, doi: 10.11591/ijeecs.v28.i1.pp545-550.

[21] Z. Zhang, S. Cao, and X. Yang, "An efficient outsourcing attribute-based encryption scheme in 5G mobile network environments," *Peer-to-Peer Netw. Appl.*, vol. 14, pp. 3488–3501, 2021, doi: 10.1007/s12083-021-01195-2.

[22] A. Tarannum et al., "An efficient multi-modal biometric sensing and authentication framework for distributed applications," *IEEE Sens. J.*, vol. 20, no. 24, pp. 15014–15025, 2020, doi: 10.1109/JSEN.2020.3012536.

[23] A. Islam and S. Madria, "Attribute-based encryption scheme for secure multi-group data sharing in cloud," *IEEE Trans. Serv. Comput.*, 2020, doi: 10.1109/TSC.2020.3038836.

[24] M. Jammula, V. M. Vakamulla, and S. K. Kondoju, "Performance evaluation of lightweight cryptographic algorithms for heterogeneous IoT environment," 2022.

[25] S. Hu, X. Wang, H. He, and T. Zhong, "Complex and flexible data access policy in attribute-based encryption," *J. Supercomput.*, vol. 78, no. 1, pp. 1010–1029, 2022, doi: 10.1007/s11227-021-03867-5.

DOI: https://doi.org/10.54216/JCIM.160111
Received: November 24, 2024 Revised: January 30, 2025 Accepted: February 27, 2025