Journal of Intelligent Systems and Internet of Things
Vol. 12, No. 02, PP. 138-149, 2024
DOI: https://doi.org/10.54216/JISIoT.120210

A Hybrid Logistic Scroll Chaotic Encryption Algorithm for Ensuring the Cloud Security to Counerfeiting the Attacks

Madireddy Swetha[1,*], Kalaivani Kathirvelu[1]

[1]Department of Computer Science and Engineering, Vels Institute of Science, Technology and Advanced Studies (VISTAS), Chennai, India

Emails: swetha.mudupu@gmail.com, kalai.se@velsuniv.ac.in

Abstract

Cloud computing is meant for storing the huge data using third party that ensures that confidential data cannot be accessed by the other users. But with rapid growth of technologies, data in the cloud normally increases which questions its security in storing in the cloud. Hence the protecting the cloud data seeks the strong security levels to counterfeit the different cloud attack. In order to achieve the highest level of security for cloud data, this study suggests a powerful encryption technique that combines chaotic scrolls and logistic maps. The proposed model exhibits the following advantages over the other algorithms: 1) High dynamic key generation 2) ability to counterfeit the multiple attacks 3) High randomness encrypted data which can provide more confusion of hacking from the intruder's insight. To prove the strength of the proposed model, NIST National Institute of Science and Technology (NIST) is used for significant experiments. in which different statistical tests were carried out to prove the strength of the proposed model. The level of security of the suggested model is also evaluated and investigated using formal analysis using Burrows-Abadi-Needham Logic (BAN). The given model is thoroughly verified using both the Profverif tool and AVISPA. In terms of communication costs and unpredictability, the suggested model's randomness has also been contrasted with that of another existing algorithm. Results demonstrates that the proposed model shows its ability to provide more potent protection to the cloud data than the other existing encryption algorithms.

Received: August 22, 2023 Revised: November 17, 2023 Accepted: April: 14, 2024

Keywords: Cloud Computing, Security; Chaotic Encryption; Scroll and Logistic maps, NIST; Burroes-Abadi-Needham; AVISPA

1. Introduction

Data from Internet of Things (IoT) devices is stored on the cloud, which is a public and open environment. It offers a customer a one-stop solution for accessing the data through the Internet at any time, from anywhere. The rapid rise of hackers targeting information compromises the safety of the information kept in the cloud. Therefore, from the standpoint of protecting user data, maintaining the security of cloud data has become the top research goal.

Numerous approaches now in use concentrate on subjects including evidence of possession using ciphertext, ciphertext-based data retrieval, and data privacy protection. While current methods [5-8] show robust protective methods towards attacks, however, security vulnerabilities such as misconduct, spying, and counterfeiting provided by malicious insiders or persistent attackers could jeopardise the protection of cloud-based services and gadgets [1-4].

Because of this, the encryption techniques used in a cloud context must be tailored in order to work in the aforementioned situation. In order to address the need for data security, the present framework aims to implement robust encryption algorithms relies on chaos theory and symmetric key cryptography. However, under the aforementioned situation, the methods provided by the present encryption algorithms result in high running costs. However, the approaches outlined by the existing encryption algorithms needs more space, non-susceptible to attacks and high chance of the data in protection. This study suggests using strong chaotic encryption in combination with a hybrid scroll and logistic map system to address this weakness and offer the highest level of security for patient information. The suggested design also the main contribution of this research study is summed up as follows:

1. Proposes the Hybrid Chaotic Encryption Scheme to counterfeit the multiple attacks and to provide high secured protection to the data.

2. To confirm the validity of the informal security analysis, deploy the code for the developed system in the well-known "Automated Validation of Internet Security Protocol and Application (AVISPA)" tool [10] and the Pro Verif software [11].

3. Evaluate the suggested system using the NIST criteria, showing that it is preferable to the current one with respect to of supremacy, security towards all forms of passive and active attacks, and achievement of high secrecy.

The rest of the essay is organized as follows: Section II discusses the many encryption methods that have been proposed by various researchers. Along with the multi-scroll and logistic maps, Section IV also includes a detailed explanation of the key creation and encryption processes. A comparative study and an experimental validation of the security analysis are presented in Section VI. Finally, Section-V wraps up the article with future developments.

2. Related Work

Utilizing "Covariance Matrix Adaptation Evolution Strategies (CMA-ES)", the "Efficient Probabilistic Public Key Encryption (EPPKE)" method that M.G. Aruna et al. developed in 2020 is improved. This improves security for data that has been transferred to the cloud. Finally, the system's exceptional security and speed were demonstrated by its encryption and decryption speeds of 0.61 and 0.5 seconds, respectively. The primary drawback of this system, however, is that it uses more energy when there is a lot of network traffic [13].

P. Kanchanadevi et al. presented a method to hybrid cloud security called "Attribute-Based Encryption with Support for Dynamic Attributes (ABE-DAS)" in 2020. Significantly reducing data leakage and protecting data privacy are the goals of this architecture. Dealing with dynamic and mobile location transformation may also be handled using this method. However, this framework's higher communication cost has been noted as its main disadvantage [14].

A forward-secure public key searching encryption technique was proposed by M. Zeng et al. (2022) in which a server located in the cloud is unable to determine any concerning a password-protected data file that has been uploaded later and contains the earlier disputed keyword. Additionally, to aid users in understanding the architecture concept, a structure for developing attribute-based searchable cryptography based forward-secure public key encryption schemes was provided. This system's primary flaw, which prevents it from properly providing security, is its increased temporal complexity [15].

In order to provide a safe password management solution, K. Loganathan et al., 2021 suggested an effective "Double-Layer Password Encryption (DLPE)" technique. Password security focuses on creating strong passwords and preventing password theft by other parties. Password security focuses on creating strong passwords and preventing password theft by other parties. Double encryption

reduces the likelihood of finding data defects, hostile assaults, and application hackers while still allowing for secured data access thanks to its strong password capabilities. Password management was made possible by the integrity and secrecy of the data. This approach, however, is extremely costly to implement in real time [16].

The data safety offered by cloud computing was improved by a method that was introduced by A. Kumar et al. in 2020. The suggested workaround encrypts user data using the RSA and AES algorithms. Better data protection may be achieved prior to cloud storage thanks to the hybridization of these two techniques. To create the "Hash Message Authentication Code (HMAC)", the secure hash algorithm 512 is employed. Third-Party Auditors (TPAs) can now utilise a reliable audit package. In the case of heavy network traffic, this architecture also offers great data security. This framework's longer authentication time, however, is a drawback [17].

Efficient Dynamic Searchable Symmetric Encryption (SEDSSE), which was introduced by H. Li et al. in 2020, is a method for protecting cloud-based medical data. Using the secure "K-Nearest Neighbour (KNN)" and "Attribute-Based Encryption (ABE)" approaches, this technique resulted in a dynamically searchable symmetric encryption system that can concurrently guarantee forward and backward privacy. In addition to improving storage, search, and update difficulty, it overcomes the key sharing issue. Storage overhead, index creation, trapdoor generation, and query speed are all efficiently handled by this architecture. However, this framework's key drawback is that it uses more resources to keep performing at the same level even with high network traffic [18].

Y. Shin et al. (2020) suggested server-aided encryption approaches to achieve maximal secrecy while incurring the expense of operating a key server. The major objective of this strategy is to provide an inter-key server deduplication method that will allow cloud storage service providers to do deduplication across ciphertexts from multiple key servers inside or across tenants. It was possible for Key servers to coordinate or pre-share secrets because to the decentralized design of this approach, which was independent of any centralized entity. It allows cloud storage services to maintain tight data privacy standards while providing high levels of deduplication efficiency and scalability. The fundamental flaw with this system, though, is that it takes longer to complete handoff operations in real-time scenarios [19].

A successful Fuzzy Semantic Searchable Encryption Strategy (FSSE) was introduced by G. Liu et al. in 2020. With the use of this technique, encrypted data in cloud computing may be searched using several keywords. This framework allows fuzzy search since it is based on the technique for creating fingerprints and Hamming distance. This framework expanded the query keywords and determined how semantically comparable the enlarged word of the query keywords was to the original query keywords in order to accomplish semantic search. This plan is more effective, improves system usability, and provides the security promise of searchable encryption. However, this architecture has a drawback due to its high energy usage [20].

A secure connectivity for communication in the cloud computing ecosystem was proven by M. U. Sana et al. (2021) by allowing third-party to gain access to the data in an encrypted form for processing without revealing the supplier party's data to safeguard private data. This approach encrypts data needed to train neural networks using the "Matrix Operation-Based Randomization and Encipherment (MORE)" methodology, which is based on entirely homomorphic encryption. This technique enables neural network calculations to be done directly on floating-point data with a barely perceptible increase in computing complexity. This framework's high resource need, however, has been noted as a limitation [21].

An effective encrypted traffic detection system was proposed by D. Chen et al. in 2022, while also protecting user privacy. To accomplish both privacy and security inside one inspection cycle, hash functions, symmetric encryption and pseudorandom functions are the only lightweight cryptographic procedures used in the system. Potential conflicts between the client and server may potentially be resolved using a dispute resolution system. The robust security, privacy protection, and performance of this technique are achieved. Nevertheless, the computational burden is not reduced [22].

Table 1: Quick overview of related works

Authors	**Techniques used**	**Merits**	**Demerits**

M. G. Aruna et al., (2020) [1]	EPPKE	High speed encryption	Require more energy
P. Kanchanadevi et al., (2020) [2]	ABE-DAS	Suited for handling dynamic and movable location transformation	High communication overhead
M. Zeng et al., (2022) [3]	Forward-secure, public-key encryption technique	High efficiency	High time complexity
K. Loganathan et al., (2021) [4]	DLPE	Data integrity, confidentiality enabled password management	Highly expensive framework for real time scenarios
A. Kumar et al., (2020) [5]	RSA algorithm and the AES algorithm	High data protection under dense network traffic	Require more time for authentication
H. Li et al., (2020) [6]	KNN and ABE technique	Efficiency with regard to storage overhead, index development, trapdoor generation, and query.	More resource consumption
Y. Shin et al., (2020) [7]	Server-aided encryption schemes	High scalability while preserving strong data confidentiality	Requires more time for handoff operations in real time scenarios
G. Liu et al., (2020) [8]	FSSE	Enhances system usability and more efficient	High energy consumption
M. U. Sana et al., (2021) [9]	ANN, MORE and FHE	Minor computational overhead	More resource consumption
D. Chen et al., (2022) [10]	a method for detecting encrypted communication that protects privacy	Less authentication time	High computational overhead

3. Logistic maps, scroll maps and proposed encryption schemes

3.1 Logistic Maps – An Overview:

A comparison of 3D logistic chaotic maps with 1D chaotic maps shows that the latter have greater chaotic properties, as mentioned in [22–25]. Given by are the mathematical formulae for 3D logistic maps.

$$X = \mu x\big(1 - x(i)\big) + \beta y' X + \alpha Z \quad (1)$$

$$Y = \mu y\big(1 - y(i)\big) + \beta x' Z + \alpha Y \quad (2)$$

$$Z = \mu z\big(1 - z(i)\big) + \beta z' y + \alpha X \quad (3)$$

When the $0.35 < \mu < 0.381$, $\beta < 0.0022$ and $\alpha = 0.0015$, The 3D Logistic maps are shown in the aforementioned equations. Figure depicts the 3D chaotic systems' suggested Chaos phenomenon for the aforementioned values.

3.2 3D Multi Scroll Chaotic Systems:

More complicated dynamics can be seen in dynamical systems with many scroll attractors than in ordinary chaotic systems with a single scroll attractor. AN automated chaotic system's State Space equation is provided by

$\dot{x}_1 = -ax_1 + bx_2x_3$ (3)

$\dot{x}_2 = -cx_2^3 + dx_1x_3$ (4)

$\dot{x}_3 = ex_3 - fx_1x_2$ (5)

The hyperbolic equation $p_1\, tanh(\, x_2 + g)$ from eqn can be added to the aforementioned equations (1), (2), and (3) to change them.

$\dot{x}_1 = -ax_1 + bx_2x_3$ (6)

$\dot{x}_2 = -cx_2^3 + dx_1x_3$ (7)

$\dot{x}_3 = ex_3 - fx_1x_2 + p_1\, tanh(\, x_2 + g)$ (8)

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

With the beginning circumstances of [0.1, -0.1, -0.6] and A double scroll attractor is generated by function called hyperbolic introduced in the 1st state with the value $g = -3$, as illustrated in Figure 1. With starting circumstances [0.1, -0.1, -0.6] and parameters$p_1 = -1$, $g = 3$, and introduced in the second state, it exhibits four scrolls as shown in Figure 2. Figure 3 illustrates a single scroll in the third stage, which has the parameters $p_1 = 1$, $g = 3$, and beginning conditions [0.1,0.1,0.6]. We may thus affirm that The feature of multiscroll is present in the system.

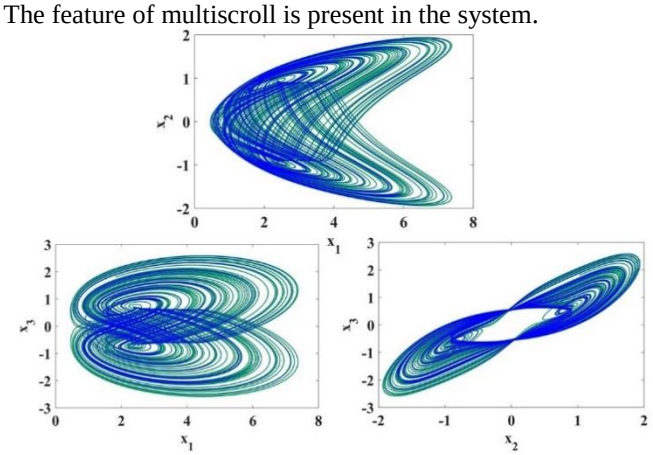


Figure 1: A cubic nonlinear system's phase images with $p_1\, tanh(\, x_2 + g)$ function in 1st state

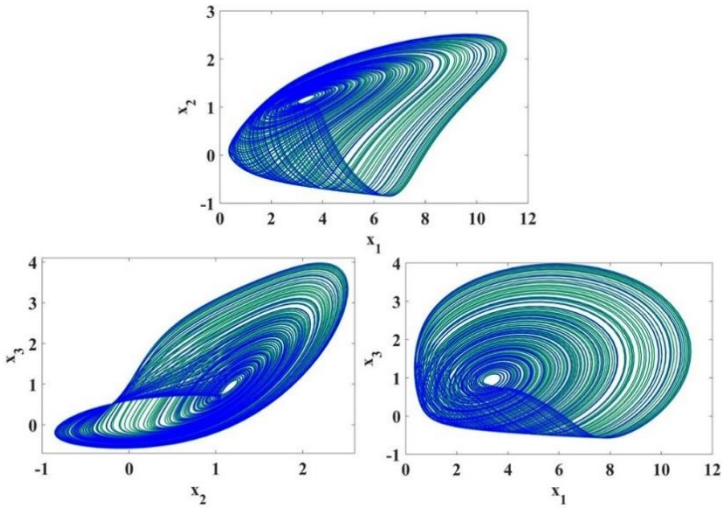


Figure 2: A cubic nonlinear system's phase images with $p_1\, tanh(\, x_2 + g)$ function in 3rd state

The derivative features indicated in [21] are adjusted in the aforementioned eqn(6-9) to produce multi-scroll 3D fractional/integer order chaotic systems. The ultimate chaotic system that may display the many scroll features is described as

$$\frac{d^q x_1}{dt^q} = -ax_1 + bx_2x_3 \quad (10)$$

$$\frac{d^q x_2}{dt^q} = -cx_2^3 + dx_1x_3 \quad (11)$$

$$\frac{d^q x_3}{dt^q} = ex_3 - fx_1x_2 + p_1\, tanh(x_2 + g) \quad (12)$$

The suggested multi-scroll integer order chaotic systems' bifurcation diagram is depicted in the accompanying figure.

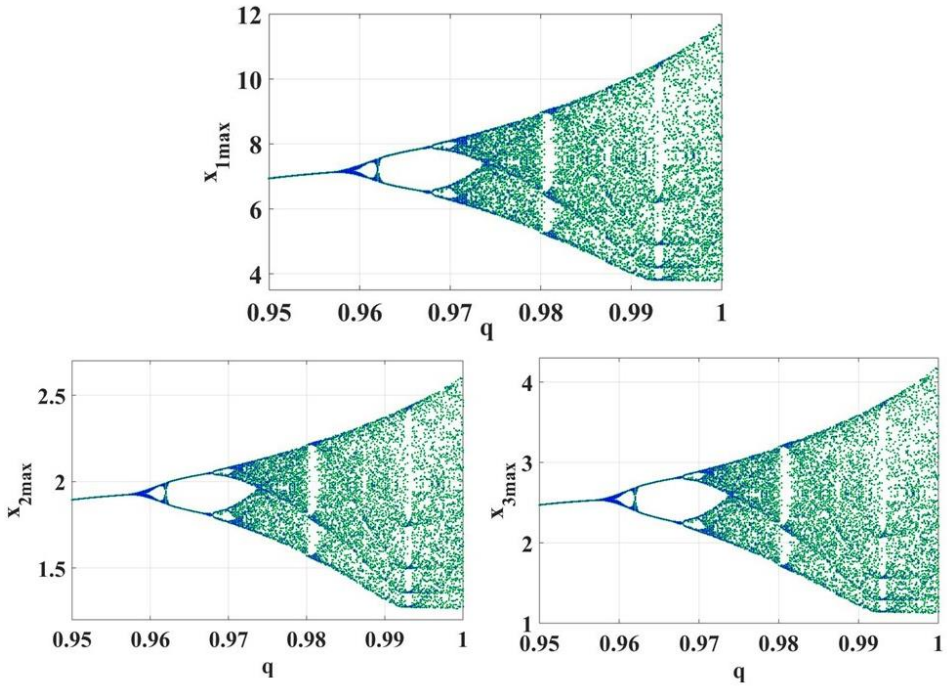


Figure 3: The Suggested Multi Scroll Chaotic System's Fractional Bifurcation Diagrams

3.3 Key Generation Process:

To generate the high complexity keys, high randomness initial condition is used for the formation of the chaotic equations. High complex keys are created at the first level as a result of computing the starting parameters, and these keys serve as the inputs for the logistic maps. The recommended output develops a new key that can serve as high-randomness keys using the diffusion process. The outputs from the logistic maps acts as the initial conditions to the scroll attractors. Figure 5 shows the flowchart for the complete key generation. The mathematical working mechanism of the proposed key generation is explained in brief steps.

Figure 4 Flow Chart for Detailed Encryption Process using Proposed Protocol

Step 1: As the first step, the chaotic outputs are computed and defined as the beginning conditions for the logistic maps.

Step 2: Logistic Maps are created based on the initial conditions formed. These are considered as the inputs to the multi-scroll maps.

Step 3: Scroll Chaotic maps are formed by the logistic output maps as described in Step 2.

Step 4: To create the high randomness key (Ek), new hybrid logistic scroll maps and the device's sensor data are diffused (D).

$$E_k = D\big(I, LSM(X, Y, Z)\big)$$

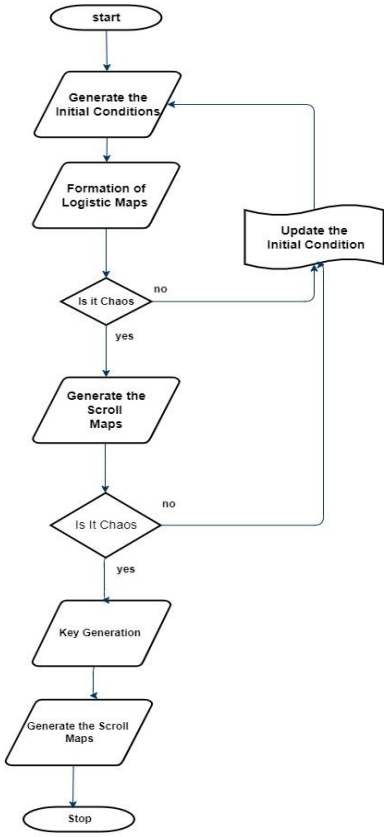
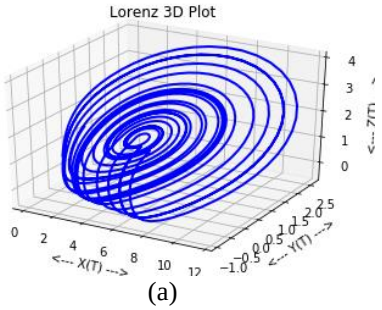
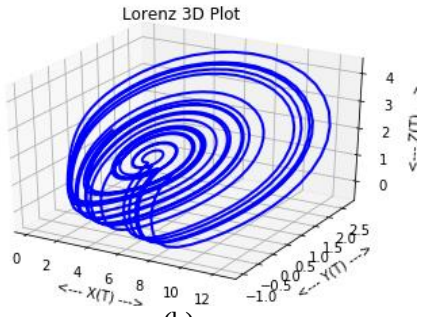


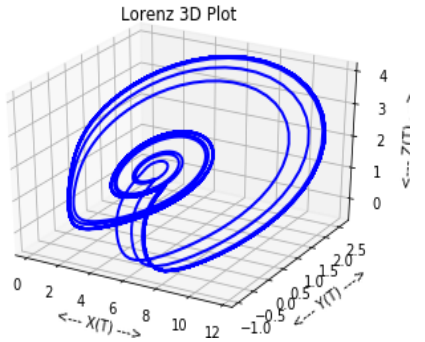
Figure 4: Flow Chart for Detailed Encryption Process using Proposed Protocol



(a)



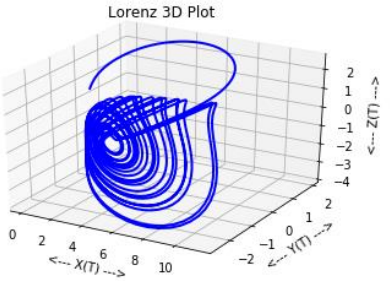
(b)



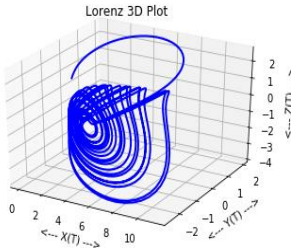
(c)

Figure 5: displays the various choatic behavior for 3D multi-scroll systems under the initial conditions.

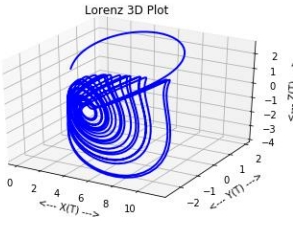
From Figure 5 displays the various choatic behavior for 3D multi-scroll systems under the initial conditions.After analysing the different choatic behavior of the Multi scroll systems , characteristics of hybrid model are illustrated in Figure 6



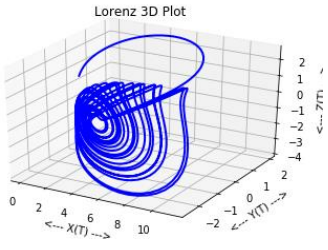
(a)



(b)



(c)



(d)

Figure 6: Choatic Behavoiur of the Proposed 3 D Hybrid Model with the Different Initial Conditions

4. Results and Analysis of Proposed Work

4.1 Implementation Details :

Python 3.10 was used to build the whole algorithm, which was then put into use on a PC workstation equipped with an I7 CPU, a 2TB hard drive, 16GB of RAM, and a 3.2 GhZ operating frequency.

4.2 Results and Discussion:

4.2.1 Statistical Randomness Analysis:

Because the technique of symmetric encryption is being used, once an intruder gets hold of the key, the gadget is open to all types of assaults. The security features of any cryptography technique are closely related to the key utilised to decode and encrypt the communications that pass through since it is so crucial. To prevent tic tactics, we need to make absolutely certain that the most important generator is truly random.

Even when an intruder knows the previous pair of random numbers within the sequence, they are unable to forecast the subsequent output bit in the sequence if the initial conditions are secret. This is another need for pseudorandom numbers generated for cryptographic reasons. A collection of statistical tests for the randomness of number sequences is provided by the National Institute of Standards and Technology (NIST) [24]. These evaluations are required to guarantee that the provided randomised or pseudo-random generator is able to be utilised for cryptographic applications. The mathematical models supporting the presentation aim to detect any change from randomness in a certain binary pattern. A generator with inadequate design is mostly responsible for the divergence. To demonstrate that the keys achieve a high level of unpredictability, practically every statistical test recommended by the NIST is used in the study report. The micro-Python modules that come with the embedded boards are used by the testing process to convert the keys that are created at every loop through binary information.

4.2.2 Test for Frequency Monobit:

Examining the ones to zeros proportion throughout every step of the pattern is the main emphasis. This experiment compares the pattern to the amount of zeros and ones that one would anticipate from a pattern that is genuinely unpredictable. The examination determines if the proportion of ones is near to 12, which is necessary for there to be approximately equal amounts of zeroes and ones in a pattern. It must pass in order for the remaining exams to proceed. When zeros and ones are mixed in this test, the values of -1 and +1 are assigned to each, respectively, producing cumulative numbers whose total mathematical representation is displayed as

$$S = ||S(n)||/n^{0.5} \quad (13)$$

S(n) represents the sum of the results, where n is the sample size. The P-value, which is used to assess randomness after calculating the Sum of the Values, has the following mathematical expression.

$$P= \text{erfc}(S/ (2)\text{^}0.5 \quad (14)$$

The frequency monobit testing yielded the following parameters, which are given in table 1

Table 1: the available quantities of the raw materials, and the profit returned from one unit of both products in the Classical Context

Iteration count	**Nature of test**	**Rule for Decision**	**Randomness Measurement (P)**	**Key Test Result**
1	Frequency Monobit	P>0.01	0.07583	PASS
2			0.045383	
3			0.05342	
4			0.04359	
5			0.06702	
6			0.090223	
7			0.06435	
8			0.08945	

9			0.89334	
10			0.089345	

The keys for the CHILS maps have shown complete unpredictability in all 10 rounds, making them appropriate for powerful encryption that can provide effective defense against network attacks.

4.2.2 Test for Frequency Monobit:

How many ones there are in k-bit blocks is the major focus of the exam. This experiment determines if the randomness premise predicts that the average number of ones in a k-bit block is about k/2. This test deteriorates into test 1, the Frequency (Monobit) test, for block sizes k=1. For each round of this test, K-bit encryption is divided into K/2, and the mathematical approach utilized to figure out their randomness is utilized as shown Table 2.

$$P = igamc(\frac{N}{2}, \frac{¥^{0.5}(obs)}{2}) \quad (15)$$

The gamma function used to calculate randomization is called $igamc$ in this case.

$$¥ = statistical\ randomess\ value\ which\ is\ given\ by\ the\ mathematical\ expression \quad (16)$$

Table 2: Randomness measurement with key test result

Iteration count	**Nature of test**	**Rule for Decision**	**Randomness Measurement (P)**	**Key Test Result**
1	Frequency Block bit	P>0.01	0.0345	PASS
2			0.33222	
3			0.23450	
4			0.02345	
5			0.2893	
6			0.19024	
7			0.8934	
8			0.02345	
9			0.08323	
10			0.0566	

Every key generated and examined twice during the course of every iteration has a randomness value greater than 0.01 in every instance. The table displays the typical test score for the major blocks.

4.3.2 Run Test:

A run is an uninterrupted string of the same bits, and the number of runs in the pattern is the main emphasis of the examination. With a bit with a different result prior to and following it, a run of length k is restricted to contain precisely k identical bits. If the number of zeros and one's in the test for runs is equal to what one may anticipate from a random pattern, then the answer is yes. Finding out if the oscillation among such numbers as ones and zeros is too fast or too sluggish is the aim of this investigation as shown in table 3.

The frequency test is made a prerequisite for this test, which is run in accordance with the precedent cases. The continuation of the key is checked for randomness using the mathematical equation provided by

$$P = erfc(|V(n)(obs) - 2n\pi(1-\pi)|)/2.828n\pi(1-\pi) \quad (17)$$

Where V(n)(obs)= has to be done

Table 3: Variation in Run Test with respect to Randomess

Iteration count	**Nature of test**	**Rule for Decision**	**Randomness Measurement (P)**	**Key Test Result**
1			0.2290	
2			0.3222	
3			0.2894	
4			0.3780	

5	Run_t	P>0.0	0.28920	PAS
6	est	1	0.22022	S
7			0.10456	
8			0.22303	
9			0.3450	
10			0.29034	

The faster oscillations were recognized by V(n)(Obs) in this test, which are regarded to be the changeover from ones to zeros, and which appear when there are several changes to the bit streams. Therefore, the bit generated using the suggested CH chaotic maps is performed with strong pseudo randomness.

4.3.3 Test of the longest run:

Mainly, the lengthiest one-run inside an M-bit block is of relevance to the examination. The goal of the experiment is to see if the longest run of ones in the pattern being evaluated matches the longest run of ones that a random sequence would reasonably anticipate. As you may recall, if the longest run of ones has an unusual length, then the longest run of zeros must likewise have an unusual length. The NIST standard is used to determine the M-values, which are listed in table 4.

Table 4: Test Result of Longest Run

Minimum n sequence	**Maximum M values**
128	8
6272	128
750,000	10^4

4.3.4 DFT Test:

It is generally the case that the longest one-run within an M-bit block matters for the analysis. The goal of this study is to determine if the longest run of ones in the structure under consideration and the longest run of ones that an arbitrary pattern might logically predict are similar. This is because, as one may remember, the longest run of zeros needs to have an odd length if the longest run of one does.

5. Conclusion

In this research work, the hybrid scroll logistic maps has been proposed for Cloud data. The proposed work also introduces the permutations and diffusion process which makes the data more random and security. The inclusion of scroll maps and logistic maps are shown the huge change in designing the traditional encryption. Furthermore, strong encryption algorithm system has been designed to evaluate the proposed model whether it is secure from vulnerabilities. Extensive testing has been done, and the results have been compared to various encryption methods presently in use for Cloud applications. The results show that the recommended model performs better in terms of speed while preserving the integrity and security of the data than other existing models. The proposed model also passes the NIST statistical tests, proving its high degree of unpredictability and resistance to attack. Because of this, the suggested model offers a greater degree of security with less processing, which makes it appropriate to embed in Internet of Things devices. As the future scope, the proposed S-BoX 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.

Funding: "This research received no external funding"

Conflicts of Interest: "The authors declare no conflict of interest."

References

[1] Ion, M.; Zhang, J.; Schooler, E.M. Toward content-centric privacy in ICN: Attribute-based encryption and routing. In Proceedings of the 3rd ACM SIGCOMM workshop on Information-Centric Networking, Hong Kong, China, 12 August 2013; pp. 39–40.

[2] Rahman, Z.; Yi, X.; Khalil, I.; Sumi, M. Chaos and Logistic Map Based Key Generation Technique for AES-Driven IoT Security. In Proceedings of the International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness, Online, 29–30 November 2021; pp. 177–193

[3] Rahaman, Z.; Corraya, A.D.; Sumi, M.A.; Bahar, A.N. A novel structure of advance encryption standard with 3-dimensional dynamic S-Box and key generation matrix. arXiv 2020, arXiv:2005.00157. 7. Ziv, J.; Lempel, A. A universal algorithm for sequential data compression. IEEE Trans. Inf. Theory 1977, 23, 337–343.
[4] Vashi, S.; Ram, J.; Modi, J.; Verma, S.; Prakash, C. Internet of Things (IoT): A vision, architectural elements, and security issues. In Proceedings of the 2017 international conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), Tamil Nadu, India, 10–11 February 2017; pp. 492–496.
[5] Farooq, U.; Aslam, M.F. Comparative analysis of different AES implementation techniques for efficient resource usage and better performance of an FPGA. J. King Saud Univ. Comput. Inf. Sci. 2017, 29, 295–302.
[6] Kocarev, L. Chaos-based cryptography: A brief overview. IEEE Circuits Syst. Mag. 2001, 1, 6–21.
[7] Mukhopadhyay, S.C.; Suryadevara, N.K. Internet of things: Challenges and opportunities. In Internet of Things; Springer: Berlin/Heidelberg, Germany, 2014; pp. 1–17.
[8] Tausif, M.; Ferzund, J.; Jabbar, S.; Shahzadi, R. Towards designing efficient lightweight ciphers for internet of things. KSII Trans. Internet Inf. Syst. 2017, 11, 4006–4024.
[9] Usman, M.; Ahmed, I.; Aslam, M.I.; Khan, S.; Shah, U.A. SIT: A lightweight encryption algorithm for secure internet of things. arXiv 2017, arXiv:1704.08688.
[10] Indrayani, R.; Nugroho, H.A.; Hidayat, R.; Pratama, I. Increasing the security of mp3 steganography using AES Encryption and MD5 hash function. In Proceedings of the 2016 2nd International Conference on Science and Technology-Computer (ICST), Yogyakarta, Indonesia, 27–28 October 2016; pp. 129–132.
[11] Aljawarneh, S.; Yassein, M.B.; Talafha, W.A. A resource-efficient encryption algorithm for multimedia big data. Multimed. Tools Appl. 2017, 76, 22703–22724
[12] Schneier, B. Applied Cryptography: Protocols, Algorithms, and Source Code in C; John Wiley & Sons: Hoboken, NJ, USA, 2007.
[13] M. G. Aruna and K. G. Mohan, "Secured cloud data migration technique by competent probabilistic public key encryption," in China Communications, vol. 17, no. 5, pp. 168-190, May 2020, doi: 10.23919/JCC.2020.05.014.
[14] P. Kanchanadevi, L. Raja, D. Selvapandian and R. Dhanapal, "An Attribute Based Encryption Scheme with Dynamic Attributes Supporting in the Hybrid Cloud," 2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2020, pp. 271-273, doi: 10.1109/I-SMAC49090.2020.9243370.
[15] M. Zeng, H. Qian, J. Chen and K. Zhang, "Forward Secure Public Key Encryption with Keyword Search for Outsourced Cloud Storage," in IEEE Transactions on Cloud Computing, vol. 10, no. 1, pp. 426-438, 1 Jan.-March 2022, doi: 10.1109/TCC.2019.2944367.
[16] K. Loganathan and D. Saranya, "An Extensive Web Security Through Cloud Based Double Layer Password Encryption (DLPE) Algorithm for Secured Management Systems," 2021 International Conference on System, Computation, Automation and Networking (ICSCAN), 2021, pp. 1-6, doi: 10.1109/ICSCAN53069.2021.9526381.
[17] A. Kumar, "A Novel Privacy Preserving HMAC Algorithm Based on Homomorphic Encryption and Auditing for Cloud," 2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2020, pp. 198-202, doi: 10.1109/I-SMAC49090.2020.9243340.
[18] H. Li, Y. Yang, Y. Dai, S. Yu and Y. Xiang, "Achieving Secure and Efficient Dynamic Searchable Symmetric Encryption over Medical Cloud Data," in IEEE Transactions on Cloud Computing, vol. 8, no. 2, pp. 484-494, 1 April-June 2020, doi: 10.1109/TCC.2017.2769645.
[19] Y. Shin, D. Koo, J. Yun and J. Hur, "Decentralized Server-Aided Encryption for Secure Deduplication in Cloud Storage," in IEEE Transactions on Services Computing, vol. 13, no. 6, pp. 1021-1033, 1 Nov.-Dec. 2020, doi: 10.1109/TSC.2017.2748594.
[20] Mahmoud Ismail, Naif El-Rashidy, Nabil M. Abdel-aziz, Mobile Cloud Database Security: Problems and Solutions, Journal of Fusion: Practice and Applications, Vol. 7 , No. 1 , (2022) : 15-29 (Doi : https://doi.org/10.54216/FPA.070102)
[21] Faya Safar, Raddad Al King, Data Security in Cloud Computing, Journal of International Journal of Wireless and Ad Hoc Communication, Vol. 7 , No. 1 , (2023) : 50-61 (Doi : https://doi.org/10.54216/IJWAC.070105)
[22] D. Chen et al., "Privacy-Preserving Encrypted Traffic Inspection With Symmetric Cryptographic Techniques in IoT," in IEEE Internet of Things Journal, vol. 9, no. 18, pp. 17265-17279, 15 Sept.15, 2022, doi: 10.1109/JIOT.2022.3155355