Turkish Journal of Computer and Mathematics Education Vol.12 No.10 (2021), 2531-2540

Research Article

New Lightweight Hybrid Encryption Algorithm for Cloud Computing (LMGHA-128bit) by using new 5-D hyperchaos system

Muhned Hussam[1] , Ghassan H. Abdul-majeed[2] ,Haider K. Hooomod[3]

[1]Computer Science Department, College of Education, Mustanisiryah University, Baghdad, Iraq
[2]University of Baghdad-Baghdad, Iraq
[3]Computer Science Department, College of Education, Mustanisiryah University, Baghdad, Iraq
[1]muhned_hussam@yahoo.com , [2]ghassan@uob.edu.iq, [3]drhjnew@gmail.com

Article History: Received: 10 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 28 April 2021

Abstract: The "cloud" is considered as a collection of hardware, storage data, multiple applications, interfaces, services, and networks, that provide the way through which users and companies can access the infrastructures remotely via the Internet on-demand from anywhere, at any time, which are independent of locations. Also can be increasing capacity or dynamically incorporating without investment in new facilities, training or licensing new programs to new workers. It extends the IT capabilities currently. Cloud computing is a common option for users and businesses for several benefits including increased productivity, high execution speed, low computer costs, efficiency, improved performance, and data reliability. Because of these benefits, each business holder and organization wish to store their data in the cloud [1]. But as more data and files are being placed in the cloud by people and organizations, worries are beginning about how safe the environment is starting to rise. The ideal safety mechanism for user's data in rest is to encrypt the data and store only the encrypted files into cloud storage, where providers of cloud or any unauthorized party unable to access the encryption key. So we need to use one or more cryptographic algorithms and protocols to encrypt the user's data before transfer to the clouds [2]. The main aim of this particular research is to protect the transmitted data with the help of encryption and decryption techniques. This research paper presents a new model for encrypting the data transmitted through cloud. The algorithms used in this model are: new lightweight hybrid encryption algorithm. We proposed to apply a hybrid of one part from PRESENT algorithm (PA) and another from TWINE algorithm (TA) by using different chaos keys in both encryption and decryption. For making the cloud more secure and to Confidence the data. The algorithm Chaos Keys Generation was used to produce random numbers by using a new chaos system with different initials and parameter values in order to generate 5-D chaos keys.

Keywords: Cloud Security, Cloud computing, new hybrid encryption algorithm, new 5-D hyperchaos system.

1. Introduction

Cloud computing is a forum for multi-lodger resource sharing, enabling various service providers to economically deliver applications as services. In terms of the use and management of IT resources and services, cloud computing is the latest technical innovation powered primarily by marketing and service offerings from major IT suppliers, including IBM, Google, Microsoft, and HP, together with Amazon [3]. The cloud computing architecture is generally made up of services, applications, servers, storage databases, and the computer network, as shown in Figure 1 [4].

Cloud computing is an Internet based technique where A large number of resources (e.g., networks, storage, applications and services) are shared to the customer. Data transmitted through internet in cloud is getting larger every day Because of the multiple benefits of Cloud that helps the user to keep his data with the least effort, reasonable cost and rapidly provisioned.

Security problems in cloud computing played a major role in slowing their acceptance. The ideal safety mechanism for user's data in rest is to encrypt the data and store only the encrypted files into cloud storage, where providers of cloud or any unauthorized party unable to access the encryption key. So we need to use one or more cryptographic algorithms and protocols to encrypt the user's data before transfer to the clouds such as Symmetric encryption algorithm, also referred to single-key encryption, they are algorithms that can use either stream ciphers that encrypt the message digits in a one at a time. Like (RC4 Cipher, salsa20 cipher...) or Block ciphers that taking a variety of bits and encrypting them as a single unit. An example (The Advanced Encryption Standard (AES), TWINE algorithm, PRESENT algorithm ...). The other type of encryption algorithm is the asymmetric algorithm or Public-key cryptography, which uses pair of keys an example: Rivest-Shamir-Adelman (RSA) used for digital signatures and key transport [5].

The efficiency of hybrid cryptography requires a large memory space and a big files register, especially when the number of rounds and episode size is large, also, when merging more than one algorithm, the time of implementation the algorithms will increase, and this is one of the drawbacks that we must avoid to obtain acceptance to the proposed hybrid cryptography. So we use lightweight cryptography algorithms (TWINE, and

PRESENT algorithms), which can remove most of the unimportant cycles and needs far less memory space, and then resulting in growth efficiency [6].

2. Cloud computing Characteristics

Cloud computing service providers presented multiple models based on their requirements. These standards improve cloud availability and performance. Cloud features are typically divided into four general parts. (Resource, service, structure, and economy). Each of these parts has several characteristics, which are called cloud computing characteristics, it is as follows [7]:

2.1 Resource

- Resource Sharing: cloud service providers are assigned and reassigned resources not shared according to the quarantine that exists through virtualization.
- Data Centers multi-located: Using data centers at different locations to increase network capacity, maximize service benefits and effective localization is one of the key advantages of cloud-based services.
- Resource Provisioning: resource provisioning and resource disassociation capability based on current demand is defined as key specification services of cloud computing. This method greatly reduces the pay of operations for users [8].

2.2 Service

- Service Level Agreement (SLA): management of Cloud service is an essential function of most cloud architectures to offer an operating model focused on services.
- Quick Respond: Cloud providers can respond quickly when they encounter fast service demand changes based on their automatic resource management feature. For instance, the user might need a large number of server resources for the duration of a certain task. Users can then release these resources when the job is done. [9].

2.2 Structure

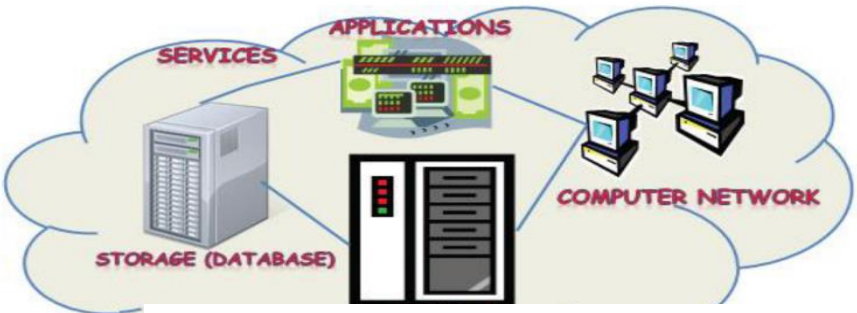


Fig.1: cloud computing architecture [5]

2.3 Layer Based Responsibilities: The cloud-based layer framework defines unique roles and goals for each layer's owner.

- Network Access: The tools and services of cloud computing are generally available online. This means that the efficiency of the access process depends largely on the Internet service provider's performance (ISP).
- Operating System: one of the most important differences between cloud computing and associated technologies (such as network and cluster systems) is the ability to operate a range of operating systems in cloud-based environments, using Hypervisor software (virtual machines). [10].
- Security and Privacy: Cloud-based data isolation increases security relative to similar technologies. However, security remains one of the toughest problem cloud computing issues. The consistency of the cloud protection approach is difficult to evaluate since many cloud service providers would not disclose their customer infrastructure.

2.4 Economic

- Lower Service Costs: Cloud storage services are often lower because of the infrastructure offered because the charge is made only for the space renewed by the customer.

- Power Consumption: Combined activities and pooled resources greatly minimize energy usage and put service providers and consumers closer to the definition of Information Technology (IT).
- Maintenance and Upgrade Costs: While overheads (such as hardware and software backup and removal) are reduced during maintenance and update operations under conventional models, due to a lack of IT interference, the price of these operations is decreased and Also, some services are free in cloud computing models.
- Pay-Per-Use Pricing Model: The calculation of the usage of IT services in the cloud is adapted to the pay-per-use idea. Service operating prices are decreased by utility- Relies on pricing as consumers pay for the service accordingly.

3. RELATED WORKS

Fu et al (2018), A color image encryption based on the chaos-efficient approach of random key generation was introduced. Three key existing elements can be extracted from the current condition of the iterative logistic map. It decreases the total number of repetitions by 3 times. The current state of the logistic map is disrupted during each iteration and the value of the disturbance is determined by the usual pixel values to ensure the efficiency of the suggested pattern against any type of attack [11].

Li, Chengqing (2018), introduced chaotic image encryption Depending on the Algorithm of Image Encryption deboned on Information Entropy (IEAIE). The digital chaotic system is based on the information entropy of the normal image. Worse, every security measure is questionable, undermining IEAIE's security credibility [12].

Jia, Nan (2016), proposed encryption method is by incorporating the chaos encryption algorithm and The Elliptic Curve Cryptography (ECC), which processes the data using one-dimensional logistical sequencing before it is encrypted to provide the first level of security, and then the next step encrypts it with an ECC encryption algorithm to provide the second level of security [13].

Liu, Hongjun, Xingyuan Wang, and Abdurahman Kadir (2014), they suggested Color image Encryption Using one-time keys and Choquet Fuzzy Integral (CFI) based on the hyperchaotic Qi scheme, To generate the 256-bit key, the hash method is designed and repeated until the initial parameter sequences for the CFI are generated. The CFI's performance works to confuse and disperse the image's red, green, and blue components, respectively [14].

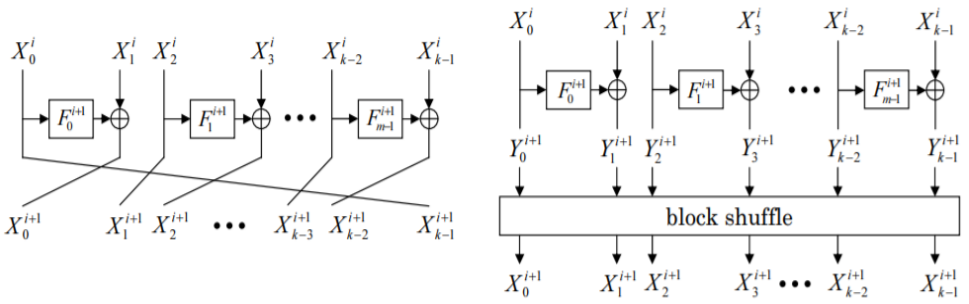
S. Hakim, M. Fouad (2017), a new secure hash algorithm is proposed for the MD5 and SHA-256 algorithms (with the final hash code length of 256) that can be used to sign applications or any message integrity since the hash code length is 512 bits [15].

Gope, Prosanta, (2019), proposed a lightweight and privacy-preserving Anonymous mutual user authentication protocol in which only the user with a trusted device has the right to access the Industrial Wireless Sensor Networks (IWSN). They considered the security of the physical layer to hold the sensor to guarantees safety even if the sensor node is captured by the opponent. The proposed protocol uses lightweight encoding alternatives, such as one-way cryptographic hash function, Physically Unclonable Function (PUF) and bitwise exclusive (XOR) operations [16].

Garima and Naveen (2014), According to this paper, the Triple Protection of Data stored In The cloud provides a method to protect cloud data using a combination of various cryptographic and steganographic technique. This paper suggests that two cryptographic viz.a.viz algorithms be merged. Advanced Standard Encryption (DSA and AES) and Steganography. DSA is used for authentication and data protection, AES is used, and for further encryption, Steganography is used [17].

Jolan Rokan Naif et al (2019), a new authorization technique has been proposed based on a lightweight Bcrypt with 4D chaos system. The proposed method includes three stages (128bit-SHA1, bit-256 HMAC, modified bit-128 with Blowfish-chaos) as these three stages have been modified to be suitable with IOT devices at high speed [18].

Dilli Ravilla et al ,(2015) , a hybrid MANET protocol is being applied in Network Simulator 2 (NS2) and hashing algorithm It. it focuses on using the HMAC-SHA 256 algorithm for message authentication and data integrity. This algorithm is a trust-based system to make the network more secure by preventing Denial-of-Services (DoS) and brute force attacks [19].



Chowdhury and DasBit (2015), proposed a lightweight hash based symmetric key message authentication code. to achieving secured communication and high-speed authentication. Detailed security analysis shows that lightweight message authentication code (LMAC) also thwarts passive attack as well as active attack [20].

L. Archana et al (2018), suggested a hybrid encryption algorithm by integrating AES and Fully Holomorphic algorithm to encrypt the data in the cloud, thereby file size get is compressed thereby increasing Data security and stack pile [21].

Fenghua Zhang et al (2019), discussed design a hybrid algorithm to solve the data security problem in the hospital cloud database. First, the AES algorithm is improved. The improved algorithm is called P-AES algorithm. The P-AES algorithm is then combined with the RSA algorithm, called a hybrid algorithm. The experimental results show that the hybrid encryption algorithm has the advantages of fast encryption and decryption speed, high security, good processing ability for longer data, and can solve the data security problem in cloud database to a certain extent [22].

4. 4. TWINE Algorithm (TA)

TWINE is one of the block cipher family, deals with 64-bit of symmetric lightweight cryptography that supporting 80 and 128-bit keys, writes TWINE-80 or -128 to indicate the key secret length. It applies block shuffle, another form of an original cyclic shift by using Type-2 generalized Feistel structure (GFS), with 16*4-bit sub-data blocks, to provide high diffusion and also be resistant against impossible differential attack or saturation attack. This round function is repeated 36 times used a 32-bit round key generated from the lengths of the secret key (80 or 128-bit keys) where the last round's diffusion layer is missed, TWINE steps are [23]:

1. Round: Encryption process in (TA) when implement 24-round in TWINE 80 or-128 bit keys it was broken by impossible differential attack thus, we apply 36-round in (TA) has good security against impossible differential attack.
2. S-box: The 4-bit S-box is selected in (TA) to achieve (1)distributions the highest differential and linear proposed are 2^(-2), (2) the Boolean level is 3, and (3) the polynomial includes more than one rules and has degree 14. The 4-bit S-box Similar to the AES S-box algorithm, we use the obverse of the Galois field.
3. Block Shuffle [24]: The block shuffle (π) Substitution of the block shuffle with the generalized Feistel structure (GFS) of Type-2 distinct from the ordinal cyclic shift, diffusion has been improved. Here, diffusion efficiency is determined by the lowest number of cycles for any input data difference to achieve maximum diffusion (that is, any input block distinct diffuses to all output blocks). Block shuffle works by transforming plaint text in (TA) into 4 separate shuffles running cyclically on 8 blocks (nibbles) rather than 16 blocks. "RK nibble index" denotes the RK round key index given to F0, F1, . , F7, F7. In each round, the difference in RK indices can be swallowed in the key generation and not in the encryption/decryption effect. Half shuffle" denotes an 8 nibble shuffle." Using the cyclic shift on the left as π, i.e., π(X0, X1,..., Xk-1)= (X1, X2,..., Xk-1, X0) For clarification purposes, we describe the following notes:

- Input data for I ≥ 0 is written as $\boldsymbol{x^i}$= ($\boldsymbol{x^i}$0, $\boldsymbol{x^i}$1, ⋯, $\boldsymbol{x^i_{k-1}}$).
- Intermediate data is $\boldsymbol{y^{i+1}}$= ($\boldsymbol{y^{i+1}_0}$, $\boldsymbol{y^{i+1}_1}$, ⋯, $\boldsymbol{y^{i+1}_{k-1}}$).
- Where $\boldsymbol{y^{i+1}_j}$= $\boldsymbol{x^i_j}$ if "j" is even and $\boldsymbol{y^{i+1}_j}$= $\boldsymbol{x^i_j}$ $\oplus \boldsymbol{f^i_{(j-1)/2}}$ if "j" is odd. (From left to right). As shown in figure (2).

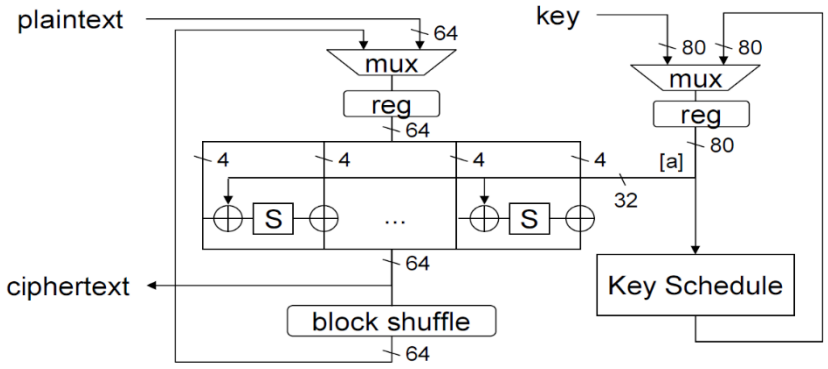
Fig.2: Type-II GFS (Left) and generalization (Right) [24]

4. Key Schedule. The (TA) The key parents allowed processes on the fly and make every round key through a sequential update of the key state. There is no intermediate key or bit permutation in particular. Since the standard of hardware is not our ultimate objective. We want to have sufficient resistance to slide attacks, meet-in-the-middle attacks, and related key protection attacks in our main schedule. [25]. Figure (3) shows the overall processes of the TWINE encryption.

Fig.3: Data path of TWINE-80 encryption.

5. PRESENT Algorithm (PA)

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$P(i)$	0	16	32	48	1	17	33	49	2	18	34	50	3	19	35	51
i	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
$P(i)$	4	20	36	52	5	21	37	53	6	22	38	54	7	23	39	55
i	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
$P(i)$	8	24	40	56	9	25	41	57	10	26	42	58	11	27	43	59
i	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
$P(i)$	12	28	44	60	13	29	45	61	14	30	46	62	15	31	47	63



The main concept of (PA) design is to enable implementations that are lightweight and fast. The length of the block in (PA) deals with 64-bits of block data and the length of the secret key is 80 or 128 bits. Using SP-network, the replacement layer consists of 16 4 x 4 S-boxes that execute in parallel. A standard bit-permutation is the permutation layer implemented in PRESENT, which helps to produce a simple security analysis and offers excellent performance in hardware and software environments, providing flexibility for different applications]. Figure (4) shows the overall processes of the PRESENT encryption. The 31 rounds comprise three steps:

1- Add Round key: a simple round intermediate-state XOR bitwise.
2- Sub Column: Parallel implementation of S-boxes in the same column to 4 bits. The following table introduces the work of this S-box in (PA) is hexadecimal notation.
3- P-Layer: In the following table, the current bit permutation is given; Bit I of the state is shifted to bit position P(i), As shown in table (1) [26].

table.1: the action of P layer in PRESENT

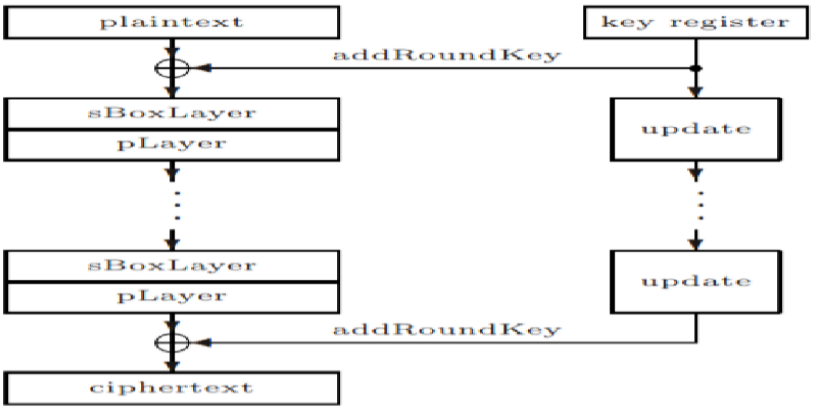


Fig.4: Data path of PRESENT -80 encryption [26]

6. THE PROPOSED SYSTEM DESIGN

The proposed system includes a number of advanced lightweight encryption and using a new chaos system with different initials and parameter values in order to generate 5-D chaos keys.. These systems are:

- 5- Chaos Keys Generation (using new 5-D hyperchaos system)
- New Lightweight Hybrid Encryption Algorithm (LMGHA).

Data blocks were encrypted using hybrid encryption consisting of more than one encryption algorithm, by using different chaos keys in both encryption and decryption. For making the cloud more secure and to Confidence the data.

The algorithm Chaos Keys Generation was used to produce random numbers by using a new chaos system with different initials and parameter values in order to generate 5-D chaos keys. Generated Chaos keys will be used in the encryption/ decryption, Figure (5) shows the structure and relationship between the proposed system parts.

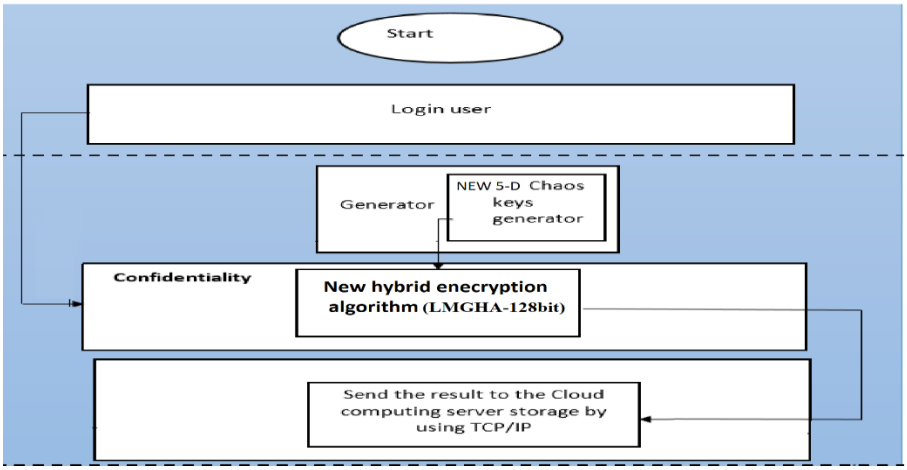


Fig.5: Block Diagram of the Proposed System Structure.

7. The 5-D Chaos Keys Generation Stage

The chaotic systems are formed by random states of their outputs running by-laws sensitive to initial conditions. So, there are many researchers in this part who employ a chaotic system in their work to add more security and power depending on the principle of chaos that slight change in one case of a non-linear system can lead to significant differences in later cases.

Looking at the random system generally, there are several types of chaotic systems, Lorenz, Hanon, Chen, Cat, etc. Lyapunov has positive chaos in the logistics scheme, while Lorenz has Lyapunov (2.16, 0, -32,4), meaning it has only one exponential dimension. Most studies try to enhance the Lorenz equation to boost its exponent, Lyapunov.

The proposed system were used for the security Mechanism of 5-D chaos keys (K1, K2…...K5). It contains a hybrid chaotic system in the chaos key generator stage. A set of the proposed new 5-D hyperchaotic system with different initials and parameter values were used to produce 5-D chaos keys values to the proposed system. The hyperchaotic system can be described in Equation (1) that shows the equations and parameters.

$$\begin{aligned} x[i+1] &= d*(y[i]-x[i])+y[i]*z[i]-f*p[i] \\ y[i+1] &= f*x[i]+(-1)^{(|p[i]+x[i]|}*g*p[i]-x[i]*z[i]+0.1*w[i] \\ z[i+1] &= x[i]*y[i]-e*z[i]-g*w[i] \\ w[i+1] &= -p[i]*z[i]+g*w[i]-0.1*x[i] \\ p[i+1] &= g*x[i]-0.1*z[i]-p[i] \end{aligned} \quad (1)$$

Where x, y, z, w and p are state variables and d, e, f and g are system parameters Where its values [d = 35, e = 83, f = 55 and g=1.25, we obtain the maximum Lyapunov exponents: [1.04164, 0.5318, 0.05961324, 0.05146074 and 1.05051608].The map outcomes of the new proposed 5-D chaotic system are shown in Figure (6).

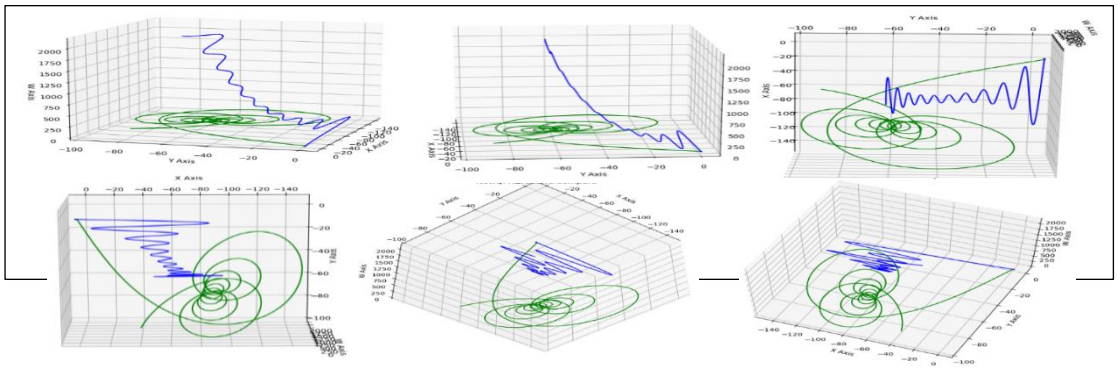


Fig.6: the map outputs of the proposed first chaotic 5-D system.

The generated chaos keys (K1, K2….. K5) are used in all proposed system and will be stored in the file to facilitate their use and reference in other operations.

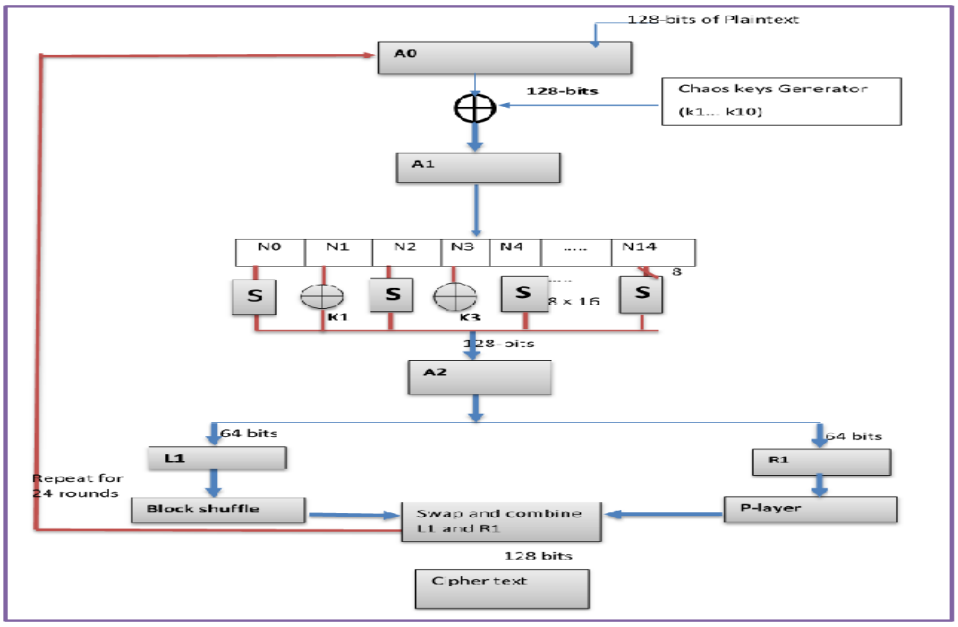
8. The New Proposed Lightweight Encryption Algorithm (LMGHA-128bit).

The new fast proposed algorithm be inspired by a combination of some functions from PRESENT and TWINE algorithms. We proposed to apply a hybrid of one part from these algorithms (P layer from PRESENT (PA) and block shuffle from TWINE (TA) algorithm) and added other features in the proposed new structure of hybrid Fiestle type with chaos keys to improve the working of the new proposed algorithm. We called it (LMGHA-128bit), This algorithm was designed to obtain high efficiency in encryption, resistance to various types of attacks with a suitable execution time, and to save memory as well as to reduce the complexity of the algorithm. Many researchers like in [26], proposed a modification to the TA by employ Type-2 generalized Feistel structure (GFS) to improve the diffusion property. In this proposed system we also use this block shuffle.

We will only consider 24 rounds of (LMGHA). This encryption algorithm is designed to deal with 128-bits of data to be compatible with the rest of the proposed and designed algorithms. The data entered into the (LMGHA) will be divided into two equal parts size 64-bits. The first section will be processed using the block shuffle of TA, and the second section will be encrypted by the P-layer of the PA. And then they will be collected together to generate 128-bits of encrypted data.

The LMGHA structure was adopted by the combinations of the 5-D keys generated by the proposed chaos. These chaos keys were used to increase the randomness of the output ciphertext and give more efficiency to the LMGHA.

The series of operations started from the input 128-bit blocks. the input data will XORed with 128-bits of chaos keys generations (K1, K2, ...K5) to produce 128-bits will be stored in (A1).



step, Next the data (N1) arranged as an 8 × 16-bit blocks array and implement the substitution encryption process by set eight S-boxes (8-bit inputs every one) on (N0) and then the next 8-bit of data input (N1) is xor with (K1) that generated from chaos key (8-bit inputs each one and the output of them is 8-bit too), and repeat S-BOX operation with 8-bits (N2) and xor next one (L3) with (K3) and so on to produce us (S0, S1, S2 … S14). The eight S-box that was modified to operated well done at the same time (parallel). The output of the S-box operation was collected one more time to produce 64-bits and the result was stored in (A2).

128-bits (N2) will be divided into two equal parts size 64-bits (L1, R1). The first section will be processed using the TA (block shuffle), and the second section will be encrypted by PA (P-layer), Bit i of the state is shifted to bit position P (i). Then the 64-bits output of (block shuffle) with 64-bits output of (P-layer) will be swapped and the operations repeated until 24 rounds to produce the final result 128-bits cipher block. The general block diagram of the LMGHA-128bit is illustrated in Figure (7).

Fig.7: The Diagram of the Proposed Lightweight LMGHA Algorithm

9. Experimental results

A. Chaos Keys Generator

The chaotic system was proposed to generate 5-D chaos keys (K1, K2....K5). The excessive change is done by making the 5-D key a chaotic structure with five positive values for Lyapunov. Table (2) indicates some Lyapunov experiment values.

The new chaotic system uses parameters d = 35, e = 83, f = 55 and g=1.25 for Lyapunov values with five dimensions that show positive values in $\lambda 1$=1.04164, $\lambda 2$=0.5318, $\lambda 3$=0.05961324, $\lambda 4$=0.05146074 and $\lambda 5$=1.05051608.

Table (4.2) Samples of the Lyapun

Time	Lyapunov (X)	Lyapunov (Y)	Lyapunov (Z)	Lyapunov (w)	Lyapunov (P)
1	1. 00894	0.44451	0.05001	0.04080	1.04111
2	1.01006	0.46881	0.05109	0.04118	1.04570
3	1.01408	0.47560	0.05187	0.04287	1.04899
4	1.02217	0.48951	0.05238	0.04309	1.05051
5	1.02689	0.49982	0.05319	0.04401	1.04995
6	1.03598	0.51029	0.05423	0.04560	1.04710
7	1.04164	0.53180	0.05557	0.04633	1.04523
8	1.03991	0.47894	0.05650	0.04756	1.04109
9	1.03781	0.45660	0.05789	0.04800	1.03885
10	1.03509	0.44430	0.05812	0.04914	1.03467

B. The Proposed New Lightweight Encryption Algorithm (LMGHA)

Many researches in hashing algorithms were designed and implemented to prove the confidentiality of data (cloud computing) integrity transfer through the networks. The proposed (LMGHA) algorithm was implemented

in the manner of cloud data confidentiality and integrity using new 5-D chaotic keys generating system to randomly increase of the primitive modified stages of the (LMGHA). The proposed system have been tested by using several tests. The time processing comprising for different data size are shown in Table (3). The statistical tests of NIST comprising for (LHKHA-MSA) in different rounds (12 and 24 rounds) are shown in Table (4).

Table 3. Benchmarking Performance of the LMGHA (32 rounds) average time (in msec) using the Random

NIST statistical tests Results Name	**LMGHA-128bit**		**LMGHA-64bit**	
	Rounds		**Rounds**	
	24	**20**	**24**	**20**
Frequency (Monobit) test	0.979	0.971	0.894	0.890
Runs test	0.999	0.997	0.958	0.950
Discrete Fourier transform	0.897	0.889	0.854	0.851
Block frequency	1.0793	1.0790	0.974	0.968
Longest runs test	1.0911	1.0902	0.988	0.980
Cumulative sums test	0.888	0.880	0.823	0.820
Serial test	1.0101	1.0999	1.0056	0.9995
Matrix rank test	0.7709	0.7700	0.6881	0.6867
Overlapping template test	0.8111	0.8101	0.8002	0.7997
Linear complexity test	1.111	1.100	0.873	0.868
Nonoverlapping template test	0.6682	0.6676	0.6231	0.6222
Random excursions variant test	1.011	1.0091	0.9541	0.9533
Random excursions test	0.9961	0.9954	0.9109	0.9096

Input Data

File Size	**(LMGHA)(32 round) (m-sec) 64-bit**	**(LMGHA)(32 round) (m-sec) 128-bit**
1KB	0.1010	0.0999
10KB	3.0312	2.1129
100KB	127.2567	80.8871
1MB	1175.5400	961.1201
10MB	12777.5542	11014.7665

As shown in Table 3, The LMGHA has a small encryption/decryption time in all files size comparing with LMGHA in 64-bit. The average LMGHA-128 bit encryption (0.0999 msec to 11012.0912 msec).

Table 4, shows NIST test results when applying (LHKHA-MSA) with different rounds (20, 24, 28 and 32) to various text sizes. The (LHKHA-MSA) passed all NIST tests and indicates the (LHKHA-MSA) has security features and can avoids many attacks types in both (12 and 24) rounds cases.

Table 3: NIST experiments Results of the LMGHA-128bit, and LMGHA-64bit with Different cycles.

10. Conclusion

1- The tests obtained shows, that the proposed system security has reached to the good results and all the objectives that have been set previously were achieved, through the availability of a high degree of security and reliability to the personal privacy. The confidentiality and data integrity operation be focus fields in many applications and systems used the sensors/ devices, cloud computing and networking in data collection.

2- The proposed system improved the security of the personal data stored on the cloud, through the modifications of the proposed more than one encryption algorithms and the proposed new hyperchaotic system (10-D).

REFERENCES

1. Arora, Rachna, Anshu Parashar, and Cloud Computing Is Transforming. "Secure user data in cloud computing using encryption algorithms." *International journal of engineering research and applications* 3.4 (2013): 1922-1926.
2. Omotunde, Ayokunle & Oludele, Awodele & Kuyoro, Shade & Chigozirim, Ajaegbu. (2013). Survey of Cloud Computing Issues at Implementation Level. Journal of Emerging Trends in Computing and Information Sciences.

3. Srinivasamurthy, S., Liu, D. Q., Vasilakos, A. V., & Xiong, N. (2013). Security and privacy in cloud computing: a survey. *Parallel & Cloud Computing*, *2*(4).
4. Al-Ramini, Lubna Mutasem. *Implementation of proposed lightweight cryptosystem for use in Cloud Computing Security*. Diss. Middle East University, 2018.
5. S. William, "Cryptography and Network Security" Principles and Practice, 7th edition, Pearson, Inc., 2017.
6. Hwu, Wen-Mei W. GPU computing gems emerald edition. Elsevier, 2011.
7. Buyya, Rajkumar, et al. "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility." *Future Generation computer systems* 25.6 (2009): 599-616.
8. Dikaiakos, Marios D., et al. "Cloud computing: Distributed internet computing for IT and scientific research." *IEEE Internet computing* 13.5 (2009): 10-13.
9. Malathi, M. "Cloud computing concepts." *2011 3rd International Conference on Electronics Computer Technology*. Vol. 6. IEEE, 2011.
10. Moghaddam, Faraz Fatemi, et al. "Cloud computing: Vision, architecture and Characteristics." *2015 IEEE 6th Control and System Graduate Research Colloquium (ICSGRC)*. IEEE, 2015.
11. Fu, Chong, et al. "A new chaos-based color image encryption scheme with an efficient substitution keystream generation strategy." *Security and Communication Networks* 2018 (2018).
12. Li, Chengqing, et al. "Cryptanalysis of a chaotic image encryption algorithm based on information entropy." *Ieee Access* 6 (2018): 75834-75842.
13. Jia, Nan, et al. "A New Method of Encryption Algorithm Based on Chaos and ECC." *Journal of Information Hiding and Multimedia Signal Processing* 7.3 (2016): 637-643.
14. Liu, Hongjun, Xingyuan Wang, and Abdurahman Kadir. "Chaos-based color image encryption using one-time keys and Choquet fuzzy integral." *International Journal of Nonlinear Sciences and Numerical Simulation* 15.1 (2014): 1-10.
15. Zhang, Fenghua, et al. "Hybrid encryption algorithms for medical data storage security in cloud database." *International Journal of Database Management Systems (IJDMS) Vol* 11 (2019).
16. Kaur, Jasleen, and Dr Sushil Garg. "Security in Cloud Computing using Hybrid of Algorithms." *International Journal of Engineering Research and General Science* 3.5 (2015):
17. Singla, Jasmeet Singh. "Cloud data security using authentication and encryption technique." *Global Journal of Computer Science and Technology* 13.3 (2013).
18. Saini, Garima, and Naveen Sharma. "Triple Security of Data in Cloud Computing." *International Journal of Computer Science & Information Technologies* 5.4 (2014).
19. *Challagidad, Praveen & Tuppad, Priyanka. (2016). Data Security in Cloud using Hybrid algorithm with Quantum Key Distribution*
20. Batra, Mahul, et al. "Secure file storage in cloud computing using hybrid encryption algorithm." *International Journal of Computer Engineering and Application* (2018).
21. Hakim, S., and M. Fouad. "Improving data integrity in communication systems by designing a new security hash algorithm." *Journal of Information Sciences and Computing Technologies (JISCT)* 6.2 (2017):
22. Gope, Prosanta, et al. "Lightweight and physically secure anonymous mutual authentication protocol for real-time data access in industrial wireless sensor networks." *IEEE transactions on industrial informatics* 15.9 (2019):
23. Tomoyasu, Suzaki. "Twine: a lightweight block cipher for multiple platforms." *Selected Areas in Cryptography*. Vol. 7707. Springer Berlin Heidelberg, 2012.
24. Suzaki, Tomoyasu, and Kazuhiko Minematsu. "Improving the generalized Feistel." *International Workshop on Fast Software Encryption*. Springer, Berlin, Heidelberg, 2010.
25. Poschmann, Axel, San Ling, and Huaxiong Wang. "256 bit standardized crypto for 650 GE–GOST revisited." *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer, Berlin, Heidelberg, 2010.
26. Bogdanov, Andrey, et al. "PRESENT: An ultra-lightweight block cipher." *International workshop on cryptographic hardware and embedded systems*. Springer, Berlin, Heidelberg, 2007.