International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 8 Aug 2021, pp: 1770-1776 www.ijaem.net ISSN: 2395-5252

A Novel Chaotic System for IoT Security Mechanism

Haider K. Hoomod, Jolan Rokan Naif
Mustansiriyah University Education College - Computer Science Baghdad-Iraq
Informatic Institute for Postgraduate Studies / Iraqi Commission for Computers and Informatic Baghdad-Iraq

Submitted: 10-08-2021 Revised: 25-08-2021 Accepted: 28-08-2021

ABSTRACT.
Internet of Things (IoT) devices deal with continuous numerical data, these data need to be secured by using advanced security mechanism, each part of IoT devices system need to be secured with the appropriate security system to avoid many attacks.
In this paper, a novel eight-dimensional Chaotic system was proposed (with 3 positive Lyapunov extensions values) to be used in the multi-stage data encryption algorithms as a part of IoT security mechanism to protect the sensing data transfer through network. The proposed security mechanism was designed by using the Hummingbird encryption algorithm and 8-D chaos keys (generate by novel 8-D chaotic system). This mechanism designed to increase security strong and speed of the IoT security mechanisms operation. The proposed novel Chaotic system was utilized for generating the encryption-authentication keys because of its sensitivity for the changing of initial conditions that making a big change in the output.
Keywords: Chaotic System, IoT Integrity , Hummingbird, IoT security.

I. INTRODUCTION

Chaotic Cryptography is the combination of mathematical Chaos theory and cryptography. Chaos theory is based on nonlinear behaviors (which are highly sensitive to their initial parameters), It has enabled structures sensitive equations of this theory from generate unpredictable random values that correspond with diffusion and confusion principles in order to construct cryptographic systems that have the maximum type of entropy and robust against any type of attacks [1,2].

The Chaos systems produce random values that are impossible to predict because they are sensitive to the initial values and if a slight change in those values will produce paths completely different from the paths produced by the original values. These important features make from Chaotic systems as a powerful choice in building many Encryption Systems especially systems that run on open networks [2,3].

Ekhlas et al. [3] proposed a textual content-encryption approach based on block cipher and chaotic maps. Their algorithm encrypted/decrypted an 8 × 8 bytes block primarily based on permutation and substitution the byte in S-box. Although their method employs large key space, it demonstrated low entropy and low security. A symmetric text cipher set of rules based totally on chaos was proposed by Murillo et al. [4]. Their scheme combined a mystery key of 128-bit length, optimized logistic maps with pseudo-random sequences, plain text characteristics, and optimal permutation diffusion spherical. The method demonstrated fast encryption speed; however, it has a small parameter space. Volos et al. [5] devised a textual content encryption process that is realized with a chaotic pseudorandom bit generator. The latter is based on two logistic maps with specific preliminary conditions and system parameters, running facet-by way of-side. The main advantage of the method in [5] is its simple realization using the X-OR function in the bit sequences

One major issue in digital chaotic cryptography is the numerical implementation. Since computers can represent real numbers up to certain precision only, the orbits computed differ, in general, from the theoretical ones. (As a matter of fact, numerical precision does not deteriorate along the orbit if its calculation involves multiplications only by integers, as in the case of affine transformations on the n-torus.) More fundamentally, any orbit in a finite-state phase space is necessarily periodic or, put in other words, there is no chaos in finite-state systems [6,7]

There are two important characteristics are uniformity distribution and cycle length. The Chaos systems have one or more different nonlinear equations such as Lorenz, Lu ,3D baker, Logistic is has three equations that produce three sets of random

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 8 Aug 2021, pp: 1770-1776 www.ijaem.net ISSN: 2395-5252

values Which is used to encrypt the contents of the message whether it is a color image or a text, to build strong cryptographic systems against threats security [2,8].

Chaos theory includes the study of dynamical systems that are extremely sensitive to initial conditions. It stands to reason that this sensitive could be helpful in cryptographic algorithms, like encryption and pseudorandom number generation. Researchers have made attempts to use Chaos-based functions on everything from encryption to hash functions to pseudo-random number generators. In the recent years, there has been in increase in the amount of papers published on the subject, and it seems to be gaining popularity. This increase of popularity does not mean that these cryptosystems and other cryptographic primitive developed are safe.

According to [9,10], there are two general methods to apply a Chaos map in a cipher system:

- one used Chaotic system to generate pseudo-random key stream which corresponds to stream ciphers.
- and the other used the plaintext or the secret key(s) as the preliminary conditions and control parameters then apply some iterations on Chaotic systems to gain cipher-text corresponding to the block ciphers.

This behavior is known as deterministic Chaos, or principally Chaos. Irregular like behavior, non-anticipating and affectability to initial value are three features that make it a suitable option to relate it with cryptography. The major difference is that encryption operations are characterized on limited sets of numbers whereas Chaos maps are characterized on true numbers. Chaotic behaviors are displays by Chaotic maps. These maps are grouped by non-stop maps and discrete maps. Discrete maps usually take the manifestation of iterated functions. Iterates are like rounds in cryptosystems, so discrete Chaotic dynamic systems are utilized as a part of cryptography. Every map consists of parameters which are correspondent to the encryption key in cryptography.

As per [10.11.12], there are two general approaches to apply a Chaos map in a cipher system:

- Chaotic systems utilization for production of pseudo-arbitrary key stream which compares to stream ciphers.
- Utilization of the plaintext or the mystery key(s) as the initial conditions and control parameters then apply a few cycles on Chaotic systems to obtain cipher content relating to the block ciphers.

$$\begin{aligned} \bar{X} &= \sigma(y - x) \\ \bar{Y} &= x(\rho - z) - y \\ \bar{Z} &= xy - \beta z \end{aligned} \qquad \text{.....(1)}$$

II. LOGISTIC MAP

Logistic map defines as one-dimensional map that used to model simple nonlinear discrete systems. The function that used to explain Logistic map was a recursive function as follows:

$$x_{n+1} = L(r, x_n) = r \cdot x_n \cdot (1 - x_n) \qquad \text{.....(2)}$$

where xn is a number between zero and one that represents the ratio of existing population to the maximum possible population. The values of interest for the parameter r are in the interval [0,4]. Consider Logistic map L: [0,1]→[0,1], given by Equation (2.8), the return map of Logistic function is given in Figure 2.12 for r = 4.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 8 Aug 2021, pp: 1770-1776 www.ijaem.net ISSN: 2395-5252

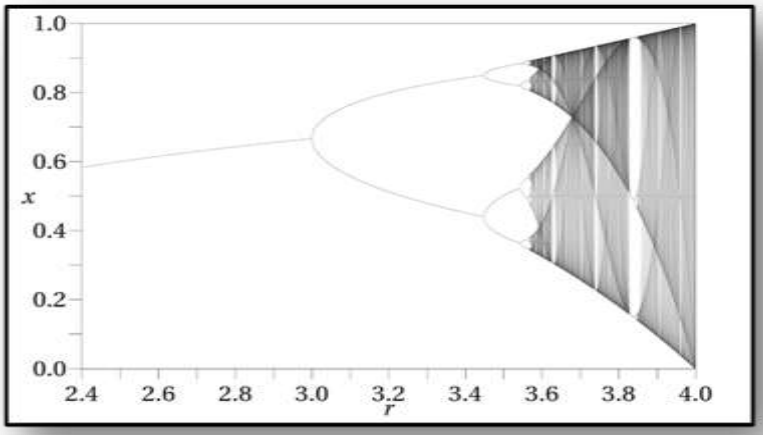

Figure (1) Logistic Bifurcation map [8]

Sensitivity of Logistic map to initial condition could be observed by plotting orbit diagrams with respect to two initial conditions with small difference. The corresponding orbit diagrams with respect to two initial conditions 0.350 and 0.351 for fixed values of r = 4 is drawn in Figure 2. There is suitable sensitivity to initial condition. In order to view Chaotic properties of Logistic map, bifurcation diagram and Lyapunov exponent of it should be calculated and plotted. Bifurcation diagram of Logistic map with respect to "r" are calculated and plotted in Figure (1) [13,14,15].

III. LORENZ CHAOTIC

The Lorenz Chaotic also uses three nonlinear equations to generate random values. The Lorenz system behavior is shown in Figure (2), mathematical formulas is as following:

In equation (1) above contains on are $\bar{X}, \bar{Y}, \bar{Z}$ variables represent the initial values of the system and σ, ρ and β are represent control values. The equations of Chaos mapping possess nonlinear equations. These equations differ in their characteristics than linear equations [10,11,12].

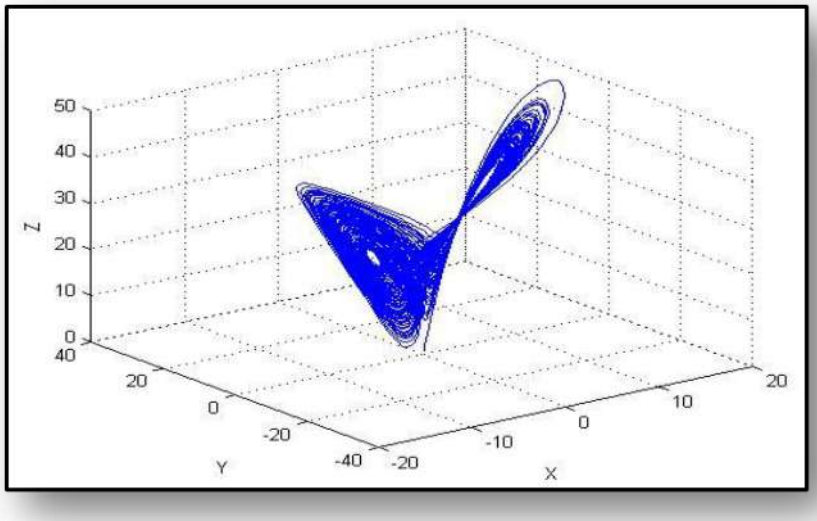

Figure (2): Lorenz Chaotic [17]

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 8 Aug 2021, pp: 1770-1776 www.ijaem.net ISSN: 2395-5252

IV. CHAOTIC MOTION FEATURES

The equations of Chaos mapping possess nonlinear equations. These equations differ in their characteristics than linear equations. The points below illustrate this [16,17,18]:

1. It is bounded: The activity of Chaotic system is always limited by predefined regions that that is called domain of Chaotic.
2. Aperiodic: The Chaos mapping behavior is a periodic in domain of Chaotic attractor or finite time for Chaotic, each orbit produces points representing the state. These points change constantly as the orbit changes.
3. Randomness: The Chaos mapping produces random values that represent paths unpredictable in the future
4. Initial value of the sensitivity: The equations of Chaos mapping are sensitive to the initial values where each equation takes time independent of the other in each place where values are produced.
5. Unpredictability: Any change in initial values even if slight will produce paths completely different paths than before changing. These characteristics make these systems impossible to predict in the long term
6. Chaos maps are deterministic, which means that their behavior is predetermined by mathematical equations.

$$x[i+1] = s \cdot (k[i] - 0.5 * x[i] + y[i] + x[i])$$
$$y[i+1] = (p[i] - 0.3 * k[i] \cdot q[i] + r \cdot x[i] - y[i])$$
$$z[i+1] = (x[i] \cdot w[i] + b \cdot k[i]) + 0.002 * v[i]$$
$$k[i+1] = (r \cdot x[i] - u \cdot k[i] + r \cdot y[i] \cdot z[i]) + q[i]$$
$$p[i+1] = (r \cdot w[i] - z[i] \cdot w[i] + v[i] + 0.003 * q[i]$$
$$v[i+1] = (w[i])^2 - b \cdot q[i] + 0.25 * z[i] + y[i]$$
$$q[i+1] = s \cdot z[i] \cdot k[i] + v[i] + 0.006 * w[i] \quad +x[i]$$

$$w[i+1] = -u \cdot z[i] + y[i] - 0.01 * v[i] + (p[i])^2 \quad \text{...(3)}$$

Where b=8.0/3.0, r=3.8, s=1.15, u=10 as parameters of this proposed system, While the xt(0), yt(0), zt(0), kt(0) ,w(0),p(0),v(0)and q(0) are initial values with period from (-1,1).

VI. PROPOSED MECHANISM FOR IOT SECURITY

V. PROPOSED CHAOTIC SYSTEM

A. The 8-D Chaos Keys Generation Stage

Due to the randomness features of the chaotic systems output numbers, many researchers suggest to embedded the chaotic system in their works. The chaos keys were used extensively in encryption operations in several researches during the last years.

Many renowned chaotic systems are logistic, Lorenz, Hanon, Chen, cat, …etc. The logistic has chaos positive Lyapunov, while the Lorenz system has Lyapunov (2.16, 0, -32.4) mean it has one positive dimension exponent. Many researches try to modified the Lorenz System in order to improve its Lyapunov exponent.

The proposed chaotic system was used 8-D chaos keys (K1, K2, …., K8) in their security operations. It is contained in the chaos key generator stage a chaotic system.

The proposed chaotic system is the proposed new 8-D chaotic system. To improve the system Lyapunov exponent values (as shown in equation (3)). The new 8-D chaotic system tested and get Lyapunov exponent vales (1.9, 0.94, 0.33, 6.38, 7.13, 0.302, 1.95 and 0.92). Figure (3) shows the map results of the new 8-D chaotic system.

This mechanism is depend on Hummingbird algorithm and the new 8-D chaos keys, these keys were divided into two parts the first four keys were used as initial value for the hummingbird algorithm and the other four keys were used for encryption by xoring them with output of the hummingbird algorithm to get filly the cipher text. The block diagram of this mechanism is shown in figure (3).

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 8 Aug 2021, pp: 1770-1776 www.ijaem.net ISSN: 2395-5252

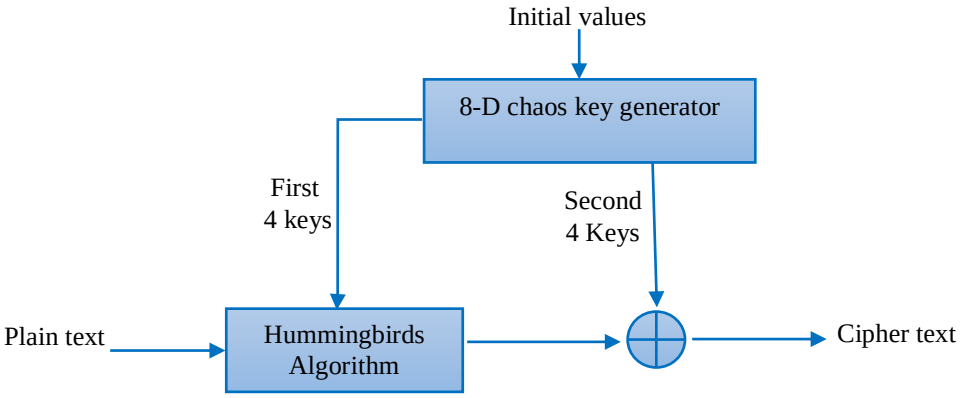

Figure (3) The block diagram of the proposed security mechanism

The first 4 keys data passed as blocks (with size 256-bits each block) to the Hummingbirds Algorithm as a key. The second 4-keys that generated from the proposed chaotic system xoring with output of the Hummingbirds Algorithm to generate the cipher text to increase the complexity of the algorithm and have an adequate encryption time.

VII. RESULTS

The generated chaos keys (K1, K2, K3, K4, K5, K6, K7, and K8) are used in any encryption algorithm and will stored in the file to be easier to use in the other operations. Figure (4) shows the map of the proposed new 8 -D chaotic system.

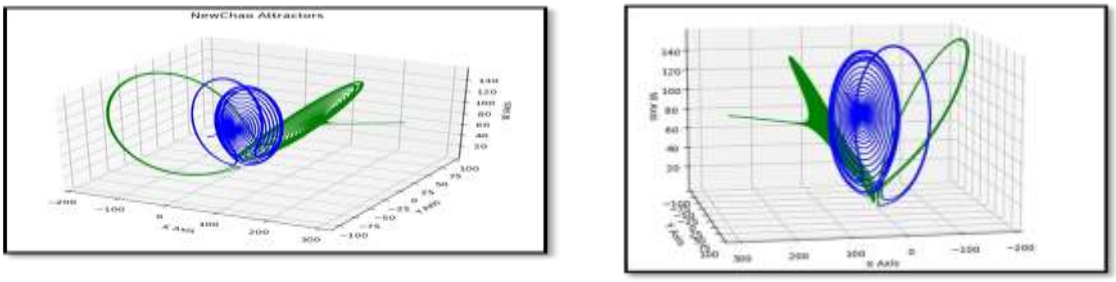

Figure (4): The map of the of the proposed new 8-D chaotic system.

The proposed new 8-D chaotic system was used as Chaos keys to other encryption algorithms such as AES , GOST, Speck and other encryption algorithms. The output of this new chaotic system is (K1, K2, K3,K4…. and K8) has Lyapunov values in 8 dimensional (6.125,7.125, 0.250, -8.125, -5.250,0 , -0.125 and 0) using parameters= b=.5, r=0.15, s=0.10, and u=10, the proposed chaotic system initial period [-1,1]

When testing, standard tests are used for testing encryption such as time tests and NIST tests. Table (1) demonstrates the proposed encryption mechanism encryption time of files of various sizes. The tests obtained as follows:

Table (1): benchmarking performance of the proposed security mechanism average time (in msec) using the random input data

Operation	Proposed encryption mechanism time (msec)
Encryption(1 KB)	0.149
Decryption (1KB)	0.140
Encryption (10KB)	1.432

Decryption (10KB)	1.399
Encryption (100KB)	2.9875
Decryption (100KB)	2.9786
Encryption (1MB)	20.0653
Decryption (1MB)	20.0097
Encryption (10MB)	199.3421
Decryption (10MB)	199.2211

Table (2) demonstrates the NIST tests of the proposed encryption mechanism, The tests obtained as follows:

Table (2): NIST tests results of the proposed security mechanism -256bit

NIST statistical tests Results Name	**Proposed security mechanism -256bit**
Frequency (Monobit) test	**0.925**
Runs test	**0.982**
Discrete Fourier transform	**0.973**
Block frequency	**0.896**
Longest runs test	**0.945**
Cumulative sums test	**0.899**
Serial test	**0.897**
Matrix rank test	**0.805**
Overlapping template test	**0.892**
Linear complexity test	**0.897**
Nonoverlapping template test	**0.903**
Random excursions variant test	**1.392**
Random excursions test	**0.987**

VIII. CONCLUSION AND FUTURE WORKS

From the test results and the evaluations of the proposed system which is presented in this paper, the gaols of the proposed system were achieved and satisfied as shown below:

1. The positive Lyapunov extensions of the 8D Hybrid chaotic system getting from many modifications to proposed new chaotic system, give results keys randomness and powerful to use in encryption algorithm,
2. Generated Chaos keys be more satisfy to embedded in to IoT devices and sensors for power consuming due to fasting keys generation.
3. The obtained Lyapunov extensions when applied to the proposed new chaotic system, which made the key more random. That makes them acceptable when used on encrypting data that need to used them in the IoT because they save time, which can be executed when scheduling keys are generated.

REFERENCES

[1]. Nathan Holt, **"Chaotic Cryptography: Applications of Chaos Theory to Cryptography"**, SemanticScholar,2017.https://www.semanticscholar.org/paper/Chaotic-Cryptography-%3A-Applications-of-Chaos-Theory-Holt/

[2]. L. Kocarev, S. Lian, **"Chaos-based Cryptography: Theory, Algorithms and Applications"**, Springer, Series: Studies in Computational Intelligence, Vol. 354, 2011.

[3]. Albhrany, Ekhlas Abass, Luma Fayeq Jalil, and Hilal Hadi Saleh. "New Text Encryption Algorithm Based on Block Cipher and Chaotic Maps." Int. J. Sci. Res. Sci. Eng. Technol.(IJSRSET) 2 (2016): 67-73.

[4]. Murillo-Escobar, M. A., F. Abundiz-Pérez, C. Cruz-Hernández, and R. M. López-Gutiérrez. "A novel symmetric text encryption algorithm based on logistic map." In Proceedings of the international conference on communications, signal processing and computers, vol. 4953. 2014.

[5]. Volos, Ch K., I. M. Kyprianidis, and I. N. Stouboulos. "Text Encryption Scheme Realized with a Chaotic Pseudo-Random Bit Generator." Journal of Engineering Science & Technology Review 6, no. 4 (2013).

[6]. Kocarev, Ljupco, Janusz Szczepanski, José María Amigó, and Igor Tomovski. "Discrete chaos-i: Theory." IEEE Transactions on Circuits and Systems I: Regular Papers 53, no. 6 (2006): 1300-1309.

[7]. Amber Shaukat Nasim, **"Chaos Based Cryptography and Image Encryption"**, Thesis ,2015.

[8]. Etienne Ghys, "The Lorenz Attractor, a Paradigm for Chaos", Springer Basel AG, 2013.http://perso.ens-lyon.fr/ghys/articles/lorenzparadigm-english.pdf

[9]. Piyush Kumar Shukla, Ankur Khare, Murtaza Abbas Rizvi, Shalini Stalin and Sanjay Kumar, **"Applied Cryptography Using Chaos Function for Fast DigitalLogic-Based Systems in Ubiquitous Computing**", Entropy, VOL 17, pp 1387-1410; doi:10.3390/e17031387, 2015.

[10]. Sundarapandian Vaidyanathan, **"Hybrid Synchronization of Lorenz and Pehlivan Chaotic Systems by Active Nonlinear Control"**, International Journal of Advances in Science and Technology, Vol. 2, No.6, 2011

[11]. Ling Bin, Liu Lichen, and Zhang Jan," **Image encryption algorithm based on chaotic map and S-DES"**, 2nd International Conference on Advanced Computer Control(ICACC),vol. 5. IEEE,2010.

[12]. Jolan Rokan Naif Al-Khazraji, Ghassan H.Abdul-Majeed and Alaa Khadhim Farhan "Design And Implementation Of Secure IoT for Emergency Response System Using Wireless Sensor Network and Chaotic", Ph.D. dissertation , Iraqi commission for computers and informatics , informatics institute for postgraduate studies, 2019.

[13]. Ahmed Majed, Haider Kadhim Hoomod:" Secure Email of Things Based on Hyper Chaotic system", Al-Mustansiriyah University, Baghdad, Iraq, M.Sc. Thesis ,2020.

[14]. Hoomod, Haider K., and A. M. Radi. "New Secure E-mail System Based on Bio-Chaos Key Generation and Modified AES Algorithm." In Journal of Physics: Conference Series, vol. 1003, no. 1, p. 012025. IOP Publishing, 2018.

[15]. Kubba, Zaid M. Jawad, and Haider K. Hoomod. "A Hybrid Modified Lightweight Algorithm Combined of Two Cryptography Algorithms PRESENT and Salsa20 Using Chaotic System." In 2019 First International Conference of Computer and Applied Sciences (CAS), pp. 199-203. IEEE, 2019.

[16]. Hoomod, Haider K., Jolan Rokan Naif, and Israa S. Ahmed. "Modify Speck-SHA3 (SSHA) for data integrity in WoT networking based on 4-D chaotic system." Periodicals of Engineering and Natural Sciences (PEN) 8, no. 4 (2020): 2379-2388.

[17]. Hoomod, Haider K., Jolan Rokan Naif, and Israa S. Ahmed. "A new intelligent hybrid encryption algorithm for IoT data based on modified PRESENT-Speck and novel 5D chaotic system." Periodicals of Engineering and Natural Sciences (PEN) 8, no. 4 (2020): 2333-2345.

[18]. Kubba, Zaid M. Jawad, and Haider K. Hoomod. "Modified PRESENT Encryption algorithm based on new 5D Chaotic system." In IOP Conference Series: Materials Science and Engineering, vol. 928, no. 3, p. 032023. IOP Publishing, 2020.