IJCTA, 10(03), 2017, pp. 105-117

Data Space and Processing Time Trade Off for Data Security in Cloud Computing

G. Venifa Mini* and K. S. Angel Viji**

Abstract : Data Security is the critical aspect in cloud. Various encryption systems should be used to promise data confidentiality on transmit or on rest. A survey between Advanced Encryption Standard (AES) and Chaos Based Cryptosystem can be carried out based on their processing time. Various encryption techniques such as addition, subtraction, multiplication, XOR and division were employed in Logistics and Henon mapping based cryptography. Of which, best encryption method based on processing time and data space requirement were analyzed. Results show that there was an inverse relation between the processing time and data space requirement of the employed techniques. The experimental analysis shows that the chaos based cryptosystem qualify exciting features such as minimized processing time and secure evaluation. This scheme leverages the potential for users of the Cloud to upload and transfer data in the knowledge that they are encrypting their data, thereby defeating a brute force attack.

Keywords : Cloud security, chaos, encryption, logistic map, data storage.

1. INTRODUCTION

Now a day, there was a widespread conversion from in-house computing into resource-warehousing based cloud computing. A large number of computing utilities across remote computing systems are used with the help of simple browsers over internet. In cloud computing, computing utilities such as processor time, memory, storage, graphics processing, other hardware usages and software etc. can be delivered in a trusted on demand basis [1]. However data security, privacy and data lock-in issues are the commonly prevailing problems encountered by cloud service providers, programmers and end users. Resources are distributed to cloud customers in virtualized manner. Virtualization is a key idea persistent in cloud computing. Virtualization [2] and cloud computing can be used to enable resource pooling and expand the elasticity of the IT environment. It can be migrated from one physical server to another in a live migration. Software as a service (SaaS), Platform as a service (PaaS), and Infrastructure as a service (IaaS) are three main layered architecture constructed in Cloud. The term 'as a service' is the concept of reusability of fine grained components over provider's network. The users can access and utilize these services depending upon their requirement. Users store their data that are maintained by the service providers in cloud storages. Since users lose their control over their data with the service providers, it could make security and privacy issues. iCloud privacy breach is one of the most recent security breaches related to cloud [3]. Some celebrities' personal photos are exposed to the public. This will lead a great attention towards strong authentication techniques and the efficiency of the applied encryption method.

Cloud security and privacy concerns are increasing among end users as customer's data and application were residing in provider's premises. Security and privacy are the top concerns of end users in cloud

* Assistant Professor, Department of Computer Science and Engineering, Noorul Islam University, Kumaracoil, India. *E-mail: venifamini@yahoo.co.in,*

** Associate Professor, Department of Computer Science and Engineering, College of Engineering, Kidangoor, India. *E-mail : angelhevin@yahoo.com*

computing as surveyed by International Data Corporation (IDC) as shown in Figure.1. In order to provide data security and privacy for customer data, a number of encryption algorithms were employed by cloud providers.

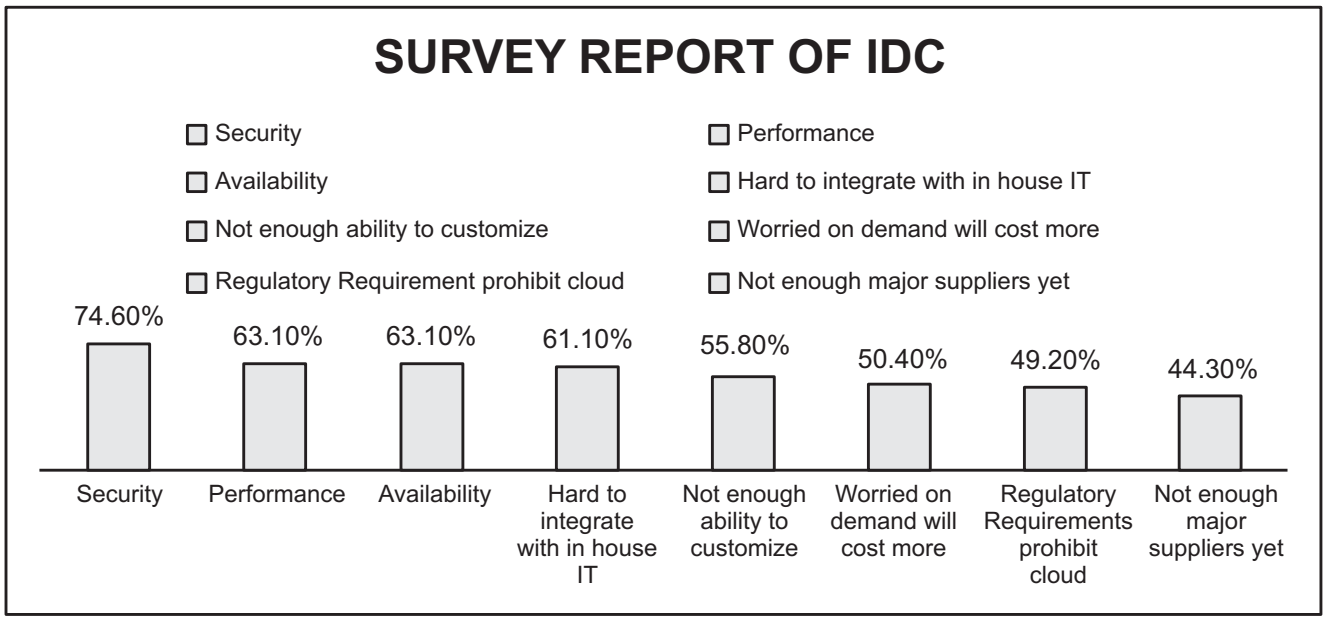

Figure 1: Survey Report of IDC

Traditional data encryption algorithms such as Data Encryption Standard (DES), Triple DES (3DES), Advanced Encryption Standard (AES), International Data Encryption Algorithm (IDEA), and linear feedback shift register (LFSR), consider plaintext as either block cipher or data stream and are not suitable for fast encryption of large data such as color image. Their implementation, when they are realized by software, of traditional algorithms for image encryption is even more complicated because of high correlation between image pixels; in other words, these mechanisms are not appropriate for encrypting digital pictures, especially in the case of smart devices [4]. These techniques are expensive in terms of consumed time, computational resources, and power consumption. Additionally, applying these techniques to large pictures is not as efficient as it is to small pictures. For that, chaos techniques are better for picture encryption, and can provide security, speed, power and computational resource savings.

Due to the limitations such as complex computation requirement, lack of processing time, low randomness, and data space constraint in existing encryption techniques, novel chaos based cryptography was proposed. Chaos is an active research area in all major fields of science and engineering. Further, Chaos is used to treat stochastic and unpredictable phenomena and solves numerous real life engineering problems. This stochastic like behavior that chaotic oscillations presents has been used to hide information in order to safely transmit secret message. Conventional cryptographic techniques use number theory and computation theory to derive secret code and it resist linear and differential cryptanalysis. These safeguards can also become the role model of chaotic cryptosystem with confusion and diffusion.

This article analyses utility of chaos functions such as Henon Map and Logistics Map that are strong candidates of key generation for text and image encryption. Various encryption methods for chaos based cryptography were analyzed in terms of encryption processing time and encrypted data size with MATLAB simulation.

2. LITERATURE SURVEY

Cryptography protects data and privacy that must be transferred and saved over long periods in dynamic environment under hostile conditions.Conventional encryption algorithm mainly depends upon discrete mathematics. Data Encryption Standard (DES) is a secret block cipher adopted by National Institute of

Standards and Technology (NIST). On encryption, 64 bit input blocks are converted to 64 bit output blocks using 56-bit key. Due to its small key size, it is not secure and slow for image encryption. Advanced Encryption Standard (AES) is fast and flexible standard for secure storage applications with high processing time. It was developed to replace DES, published by NIST. It increases length of key as 128,192 or 256 bits. Depending on key size 128 bits data blocks were encrypted in 10, 12, 14 rounds. High key size leads to more battery and time consumption. As the throughput increases, power consumption decreases ([5]-[7]).

The public cloud services utilized by e-commerce and business field cannot squeeze benefits, without taking some security considerations into account. Users do not have any control on the processing that was maintained by cloud [8]. They don't know about the technique, encryption method and version of software. Unencrypted data was intercepted by unauthorized third parties.

Comparative analyses of blowfish, AES, DES and RC4 were discussed in [9].DES consumes less encryption time, but the key size is too short. Symmetric key encryption is more superior to Asymmetric algorithm [10].Symmetric Algorithm uses same key to encrypt and decrypt and it can be embedded in hardware easily. Memory usage is lower [11]. Also it runs faster and provide high security than Asymmetric algorithm. Conventional encryption schemes DES, DES, TDES and AES do not provide a mechanism for computation on encrypted data. AES is widely used for security of cloud. It is transparent and can be integrated quickly and easily without any alteration to the application.

When data is encrypted using these algorithm, the only permitted operation on it is decryption by using secret key. This implies AES to provide a secure storage, but not a secure computation on encrypted data [12].Moreover it is not suitable for Wireless Sensor Network (WSN) due to the demand for more hardware resources. Due to computation burden and number of rounds it consume lot of energy. This paper [13, 14] discussed the comparison of data encryption algorithms. The results shows that, AES produce poor performance when compared to other algorithms due to its high processing power.

[15] Described an efficient encryption and decryption service, which was separated from the storage service of data. Service Provider operates conversion and other provider operates storage services. It provide high security, but very expensive in terms of multiple service provider. This study [16] propose an integrated approach of Attribute Based Encryption (ABE) System and Fully Holomorphic encryption(FHE). It formalize securely outsourcing computation using linear programming in cloud environment. But this method require large amount of computing resources. Ensuring Data Security in cloud computing [17] analyze various issues like byzantine failure, data modification attacks and vulnerability from cloud service provider. It does not support dynamic operations. So, it is limited applicable for cloud storage. The cipher text space for AES is higher than DES and TDES [18]. It's three to four times greater than plain text space. In [19], DES architecture was designed to eliminate vulnerable attacks in cloud. The demerit of this approach is computing power increases and level of encryption stepped up. TelosB motes evaluated AES and chaotic cryptographic algorithms with equal quality and the analysis shows that chaotic algorithm is much faster than conventional algorithm [20].

Chaotic maps play a vital role in non-linear dynamics, correlated to the mapping of time series. In chaotic world, Logistic map is an equation of discrete-time version, relating the map *g:* X -> X developed by Pierre in 1845 [21]. Henon map derived by Henon as a simplified model [22] of the Poincare section of Lorenz system in 1963. The dimensions of maps are categorized by 1-dimensional, 2-dimensional, 3-dimensional etc. are also useful for block encryption ciphers with exponential and logistic map [23, 24]. Chaos based encryption systems have simplicity and unpredictability than conventional encryption algorithms [25].It has special features like sensitivity to small changes of initial conditions and system variables and this concept is very much suitable for cryptographic algorithms.

In reality, Chaos Based Algorithm expose some important properties regarding computation, processing time, power, simplicity, security, speed etc. [26, 27, 28], so it is practically used in secure communication.

Cryptanalysis [29] shows that no known attack to ciphers in a network. In Wireless-Fidelity (Wi-Fi) networks [30], the requirement of high speed and security with large key size and low memory capacity were satisfied with fast transformation.

Block cipher feasible to describe efficiency of maintenance and it contain acceptable processing speed [31]. The implementation of algorithm is complex and the key is large enough to enhance security. It prevent the deciphering of original message by all four attacks [32, 33]. The techniques like PLCM map, Baker map, unicity distance and Huffman coding are reliable, fast and secure for verifying and validating a person or network (authentication), unaltered data during transmission (integration) and refusing an object and obligation (repudiation) [34,35].

Chebyshev polynomial embedded with asymmetric algorithm for information encryption and protects the cryptanalysis attack using digital signature and hash algorithm [34]. Chaotic art of creating and solving codes are combined with hash function to generate Message Authentication Code [MAC], used in practical applications. Instead of unicity distance, wei scheme was introduced for practical applications [36].Chaotic masking leverage the reliability and feasibility of block enciphering system in dynamic environment [37].

Comparing to the traditional encryption schemes, chaos based encryption schemes have several advantages [38]. Chaos based encryption schemes can be defined over continuous number field but traditional encryption schemes are limited to integer number fields. chaos based encryption can be implemented directly using high speed analog component (optical or electrical) such as lasers, etc. but Traditional encryption schemes can be implemented only by using digital hardware. Encoding and broadband modulation in chaos based encryption schemes can be implemented using a single circuit. In traditional encryption two circuits are needed: A digital circuit for encryption, and an analog circuit for broadband modulation. Non-periodic pseudo random waveforms that can be used to mask a message continuous waveform can be generated by chaotic dynamics. Pseudo-random sequences generated by traditional encryption schemes end up being periodic as they are implemented using digital hardware.

3. ADVANCED ENCRYPTION STANDARD (AES) ALGORITHM

AES (Figure 2) algorithm is a symmetric key algorithm embedded with four layers that was repeated up to (n – 1) rounds. The first stepis the nonlinear confusion process between cipher text and key. Byte-by-Byte substitution of the blocks is performed in this step. Computation on S-box is very intensive connected with affine transformation. This requires extra hardware resources.

Input : Plain text (P,), *key* (K)
Output : *Encryption / Decryption*
sec retmsg ← *currstate* (P_i, K)
initkey ← (sec *retmsg*, K_0)
for each i **to** *round* (n – 1) **do**
Substitute bytes (sec *retmsg*) //S-box is used to perform substitution of block
Shiftrows (sec *retmsg*) //simple permutation
Mixcolumns (sec *retmsg*) // Substitution by the use of arithmetic over GF (2^8)
Addroundkey(sec *retmsg*) //Bitwise XOR with present block with expanded key
end for
repeat round (n – 1)
end

Figure 2: Advanced Encryption Algorithm, reverse process is Decryption

4. CLOUD COMPUTING AND ENCRYPTION USING CHAOS

The Data owner or end user's system identifies a chaos function normally generated from real life situation such as an ECG, EEG, Pulse wave form etc. Then a phase space is constructed in order to find the initial value of the chaos normally identified by calculating Lyapunov exponent usually a positive value. The initial condition is applied on Logistic or Henon functions to derive the keys. Constructs the phase space and generates key with the help of logistic and Henon function. The data is encrypted by the key series generated and it is transmitted to the cloud for storage as illustrated in Figure 3.

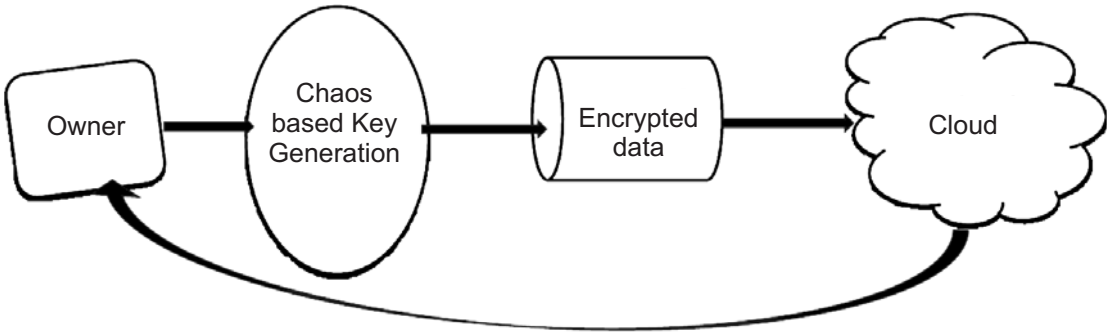

Figure 3: Key generation in cloud

4.1. Construct Phase Space

Phase space provides a visual tool for analyzing the dynamics of a nonlinear system, where each point gives multiple states of a system variable.

The dimension d represent number of points $\{\vec{x}(n)\}$ of the system, each point is given by

$$\vec{z}(n) = [Z(n), Z(n + n_T), \ldots, Z(n + (d-1)n_T)] \quad (1)$$

Where, n represent the time moment, $n_T = \frac{T}{\Delta}$ with Δ denotes the sampling period is the time period between two consecutive measurements for constructing phase plot.

4.2. Initial value calculation by Lyapunov Exponent Spectrum

Lyapunov exponent provides the global stability analysis of the nonlinear dynamical system, which is very sensitive to the initial conditions. A slight difference between initial conditions are clearly reflected by the chaotic system. It is defined as the long term average exponential rates of divergence of neighbor states. If a system contains at least one positive lyapunov exponent, then the system is chaotic in nature. The exponents are ordered as $\lambda_1, \lambda_2, \lambda_3, \ldots, \lambda_n$ where λ_1 and λ_n are the most diverging and converging principal axes. The positive exponent λ_1 is calculated from person's ECG signal with wolf algorithm.

Steps :

1. Find the difference d_0 of neighboring points in the orbit
2. If the distance is short, then connect both points along the orbit
3. Compute the new difference d_1
4. If d_1 becomes too large ,choose an alternate replacement for other point8
5. Repeat the above steps for s traversals

Positive exponent λ_1 is computed as follows

$$\lambda_1 = \frac{1}{t_s - t_s} \sum_{k=1}^{s} ln\left(\frac{d_1(t_k)}{d_0(t_{k-1})}\right), \quad (2)$$

Where $t_k = k\Delta$

4.3. Logistic map

Logistic mapping [39] is a one-dimensional quadratic polynomial mapping, which is a classic example of chaotic phenomena by a simple non-linear equation as follows.

$$L_{n+1} = AL_n(1 - L_n) \quad (3)$$

$A \epsilon [0, 4]$, $L_n \epsilon [0,1]$ where A is the logistic parameter, which decide the distribution patterns of the equation. $L_n \epsilon [0,1]$ is the condition of a chaotic state that is sensitive to the initial condition L_0. When $3.5699456 < A < 4$.

4.4. Henon Map

Henon map is a most popular invertible 2-dimensional map. A map is invertible if a state x_{n+1} has a unique pre-image $\{x_n \mid x_n = f^{-1}(x_{n+1})\}$. It has a dimension greater than one.

4.5. Data Encryption Algorithm

Text and image reverted into secret code with figure 4. Minimum rounds will yield great performance in cloud with low communication and computational cost.

Function : Data_Encryption_text_image(p_i) **returns** *Ciphertext*(C_i), or failure
Input : λ //calculate positive lyapunov exponent
Output : C_i
generate random key series $k_1, k_2, k_3, \ldots$
for each random key in keyseries (*k*) do
    if key is consistent with assignment based on constraints
    Enc_text(C_i) ← *Data_Encryption_text*(p_i, *k*)
    Enc_image(C_i) ← *Data_Encryption_text*(p_i, *k*)
    if *Enc_image*(C_i) ≠ *failure* **then**
    return *Composeddata*
    end if
  end if
end for

Figure 4: Chaos Data Encryption and Decryption is reverse process

5. KEY SECURITY ANALYSIS

In this section, the key series generated for the best encryption and decryption system have been conducted to evaluate performance of the proposed encryption system and it should be hard against brute force attack. Figure 5 present the iteration process that split into two divergence (Bifurcation Parameter) for Logistic Map. For the comparison, choose wrong key deliberately and a correct key to the chaotic based decryption algorithm. It must be noted that the chaos based key generation system is extremely case sensitive. It seems that the proposed system is reasonably sensitive to the secret key, so that it can generate enough key serial space against the brute-force attack.

Theorem 1: (Brute Force Theorem) *The chaos crypto system is ξ – computationally secure against brute force attack for all possible keys 'k' with lyapunov exponent 'λ'. Let x_0 [correct] and x_0' [wrong] be the initial condition over space 'S' of dimension 'd' for the sampling period 'T', shows that the key space is nonlinear to derive an unpredictable orbit say S^d .*

Proof : Assume that key $k = (x_0, \varphi, T_0)$ where 'x_0' as initial condition, 'φ' as activation component, 'T_0' as Transient (initial time of sampling period)

i.e., $$|x_0 - x_0'| \geq \xi \quad (4)$$

Cipher text 'Ci' of message Pi is deduced as

$$C_i = E(k, [C_{i-1} \oplus P_i]) \quad (5)$$

For space 'S', $$\exists_x \{x \in S \mid L(x_0) = S\} \quad (6)$$

$$\forall_{x0} \in [0, N^s) \quad (7)$$

Where N shows the number of values with respect to diffusion nature.

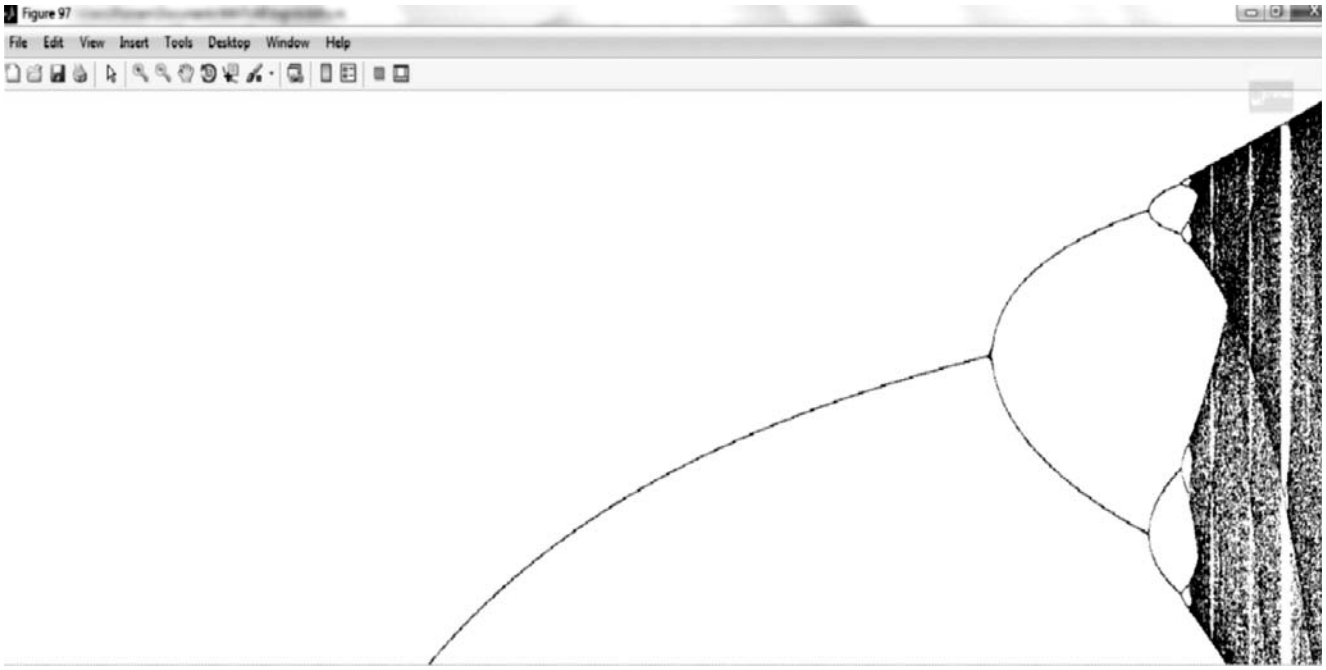

Figure 5: Bifurcation Parameter for Logistic Map

Therefore, if $0 < \xi < S$ is the distance between two keys x_0 and x_0', then maximal security is attained after initial transient ie $T > T_0$.

An estimation for T_0 is taken from ξ. $N^{S.\,T0} = N^S$ which gives large number of keys, deriving that, it is hard to succeed brute force attack.

$$T_0 = \frac{x_0 - \log \xi}{S} \quad (8)$$

6. SIMULATION RESULTS

6.1. Experimental Analysis of Crypto Processing Time and Encrypted Data Space

To evaluate the performance of encryption and decryption time for logistic and henon map, we have implemented the chaos based encryption and decryption module in MATLAB 2012a. The module was simulated with the help of a Pentium Dual Core Processor, 2.30 GHz speed, 2 GB memory. The encryption and decryption of uniform data was implemented using simple encryption methods such as addition, subtraction, multiplication, division and XOR. The total time for encryption and decryption is computed and plotted as shown in figure 6.

Encryption Time for Logistic Map

It is evident from the figure that XOR took much time for encryption and decryption than other methods. An encryption and decryption using a division operation takes minimum processing time than subtraction, addition, multiplication and XOR.

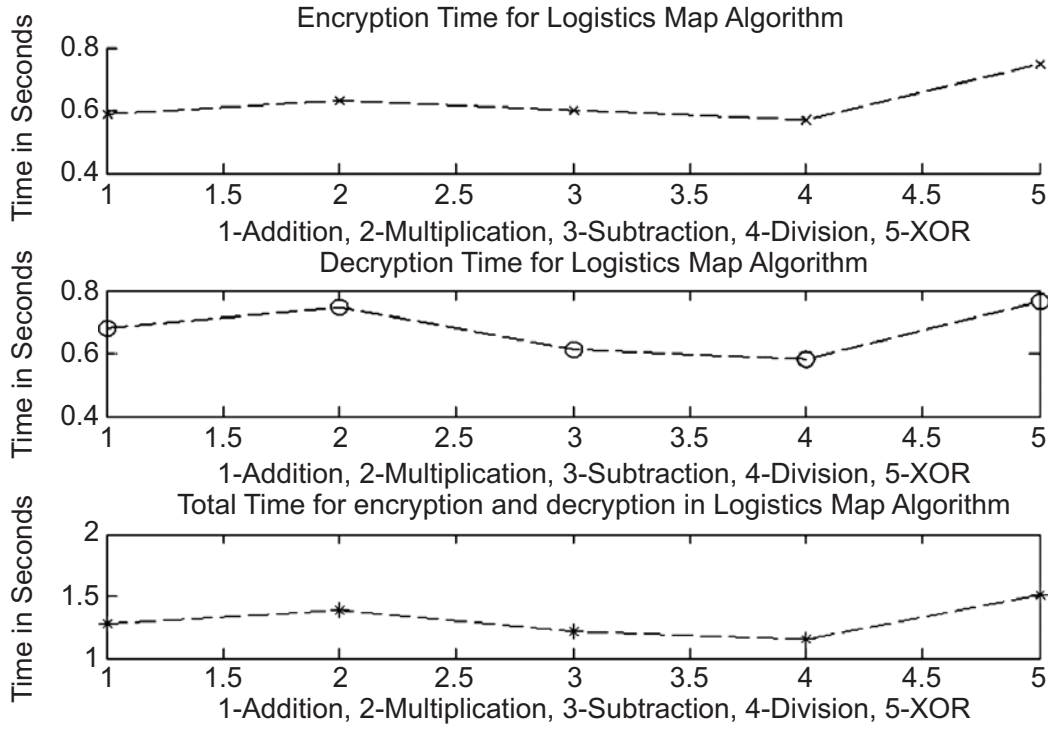

Figure 6: Encryption on various operations for Logistic map

Encryption Time for Henon Map

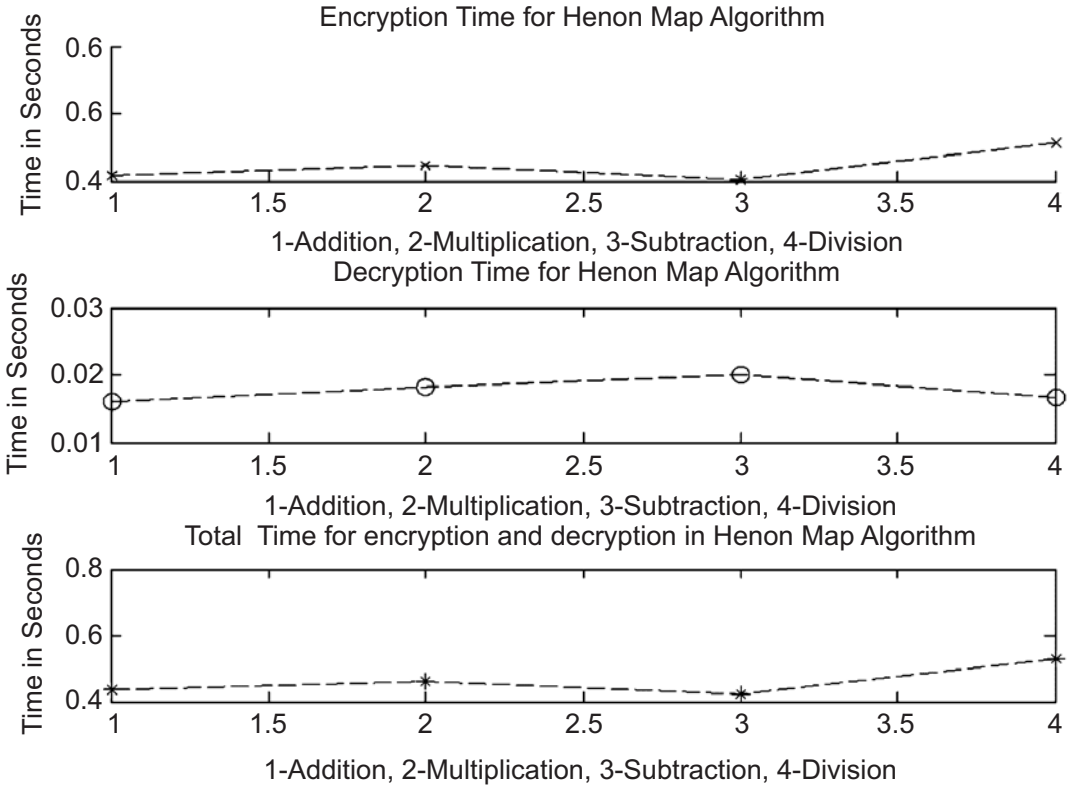

Figure 7: Encryption on various operations for Henon map

The decryption and encryption time of different encryption operations such as addition, subtraction, multiplication and division on keys generated with Henon map is depicted in Figure 7. Analysis shows that encryption and decryption by subtraction gives less time than other operations. It is interesting to note that XOR is not a viable option and hence omitted in this analysis.

Processing time between AES and Chaos

A comparison of the processing time of conventional known best encryption method AES and proposed logistics based key generated encryption is tabulated in Table 1

Table 1

Processing time between AES and Chaos

Text to encrypt [Length 16;Size 128bytes]	*Identifier*	*AES Time(Sec)*	*Logistics time*
11;12;11;11;00;13;12;13;11;31;11;11;14;15;13;01	Data-1	4.808249	0.089893
07;03;16;02;00;01;12;06;98;03;11;04;14;12;09;13	Data-2	5.189445	0.084248
05;08;13;04;11;12;15;06;11;12;15;03;09;13;22;44	Data-3	5.629122	0.051778
72;52;83;93;39;92;65;76;11;12;15;23;69;15;43;73	Data-4	5.490347	0.077906
09;07;09;02;17;16;12;36;32;16;98;12;33;99;92;97	Data-5	3.625118	0.066796
24;18;43;34;21;42;55;46;21;42;85;73;29;33;62;34	Data-6	4.57274	0.080631
73;25;63;37;27;52;73;84;32;39;93;27;25;56;64;54	Data-7	5.497268	0.075971
82;45;52;55;14;92;79;77;44;73;83;82;73;91;62;62	Data-8	5.086616	0.072614
05;08;13;04;11;12;15;06;11;12;15;03;09;13;22;44	Data-9	5.215482	0.075417

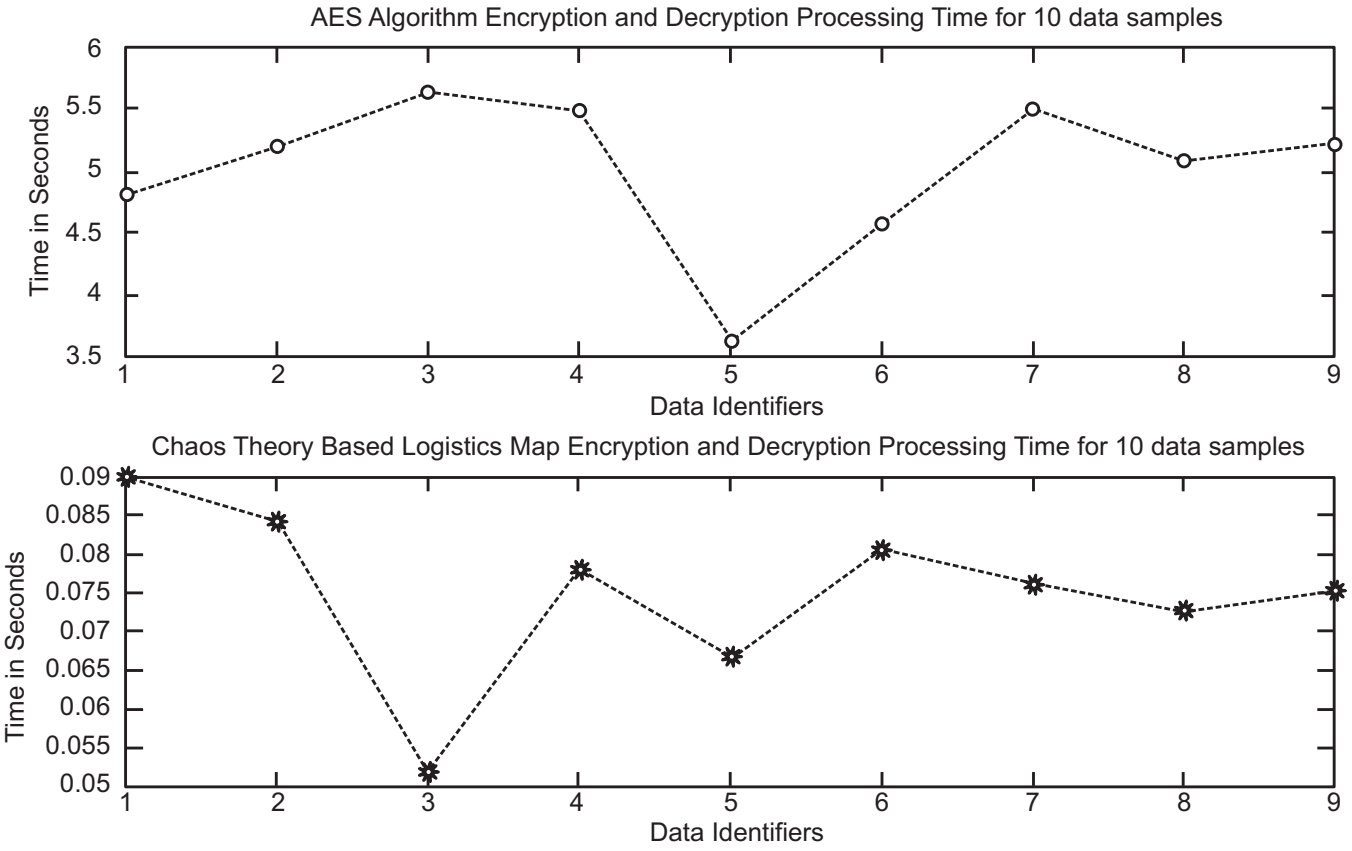

Figure 8: Comparisons of AES and Chaos Theory

In this section Figure 8, the performance of processing time for 10 data samples between the conventional AES scheme and the chaos scheme have been analyzed by with MATLAB simulations. The results predict that chaos based encryption is best for dynamic environment with low processing time and high security than conventional AES. Figure 10 and Figure 11 shows the results of encrypted data size.

6.2. Encrypted Data space for Logistics Map based Key Generated encryption with various methods

From figure 9 it is found that an encryption with Division occupies more space than other techniques. However it is to be noted that division operation took only minimal time compared to other operations. When comparing the data space and processing times of various encryption methods implemented with Keys generated with Logistics Map, the two results are almost inversely proposal to each other. Even though XOR operation based encryption took much processing time it occupies comparatively minimal space next to addition than other operations.

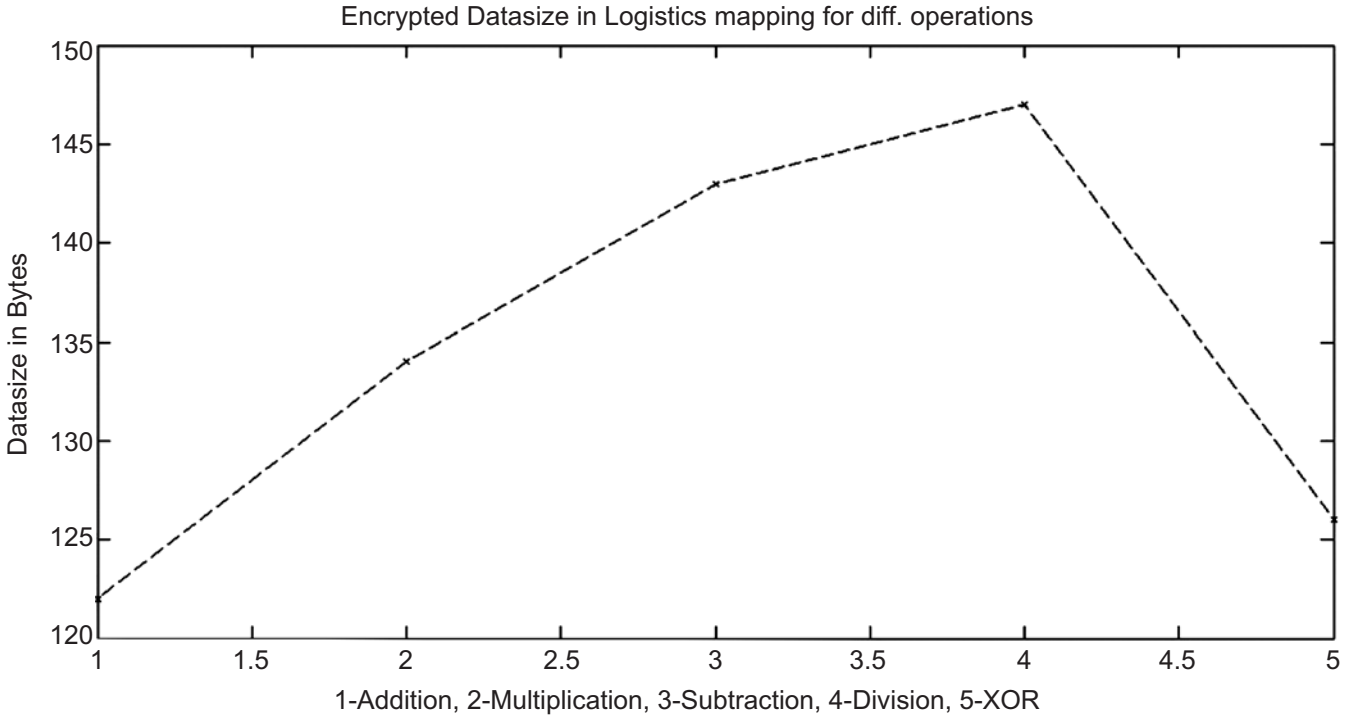

Figure 9: Encrypted Data size in Logistic Map

Encrypted Data space for Henon Map based Key Generated encryption with various methods

Figure 10 reveals that multiplication operation for encryption consumes less space compared to other operations. Even though subtraction occupies space for storing the encrypted data its low processing time consumption is to be noted. Like Logistics map, in Henon Map also we can see an inverse relation between processing time and data space requirement. However multiplication is outperformed by subtraction operation in terms of processing time.

7. CONCLUSION

Chaos has lot of merits like unpredictability, pseudo randomness and sensitivity to initial state. These characteristics are very useful for secure and faster encryption and decryption of text and image. Apart from this chaos theory based cryptography provides a large key range that makes it a strong candidate against brute force attack. . The confusion and diffusion of chaos function yield better key management and high security. In this paper we have proposed novel chaos based key generation and various methods for encryption and decryption of data with the keys generated with chaos theory. AES is compared with chaos based cryptography and found that the overall processing time for encryption and decryption is much lower for chaos. Suitable encryption methods such as addition, subtraction, multiplication, division and XOR were performed with keys generated by the chaos based key generation and concluded that division operation for Logistics Mapping (Used in Text Cryptography) and subtraction for Henon Mapping (Used in Image Cryptography) are suitable candidates in terms of processing time. However in terms of storage space occupied by the encrypted data with various encryption techniques, Addition and Multiplication

are suitable methods for Logistics and Henon Mapping respectively. It is interesting to note that the processing time and data space of various encryption techniques are almost inverse relation to each other. It is up to the end user to select the best method between processing time and data storage space depends upon the cost tradeoff between these two parameters.

In the future, this work will be elaborated by embedding human variable within the equation.

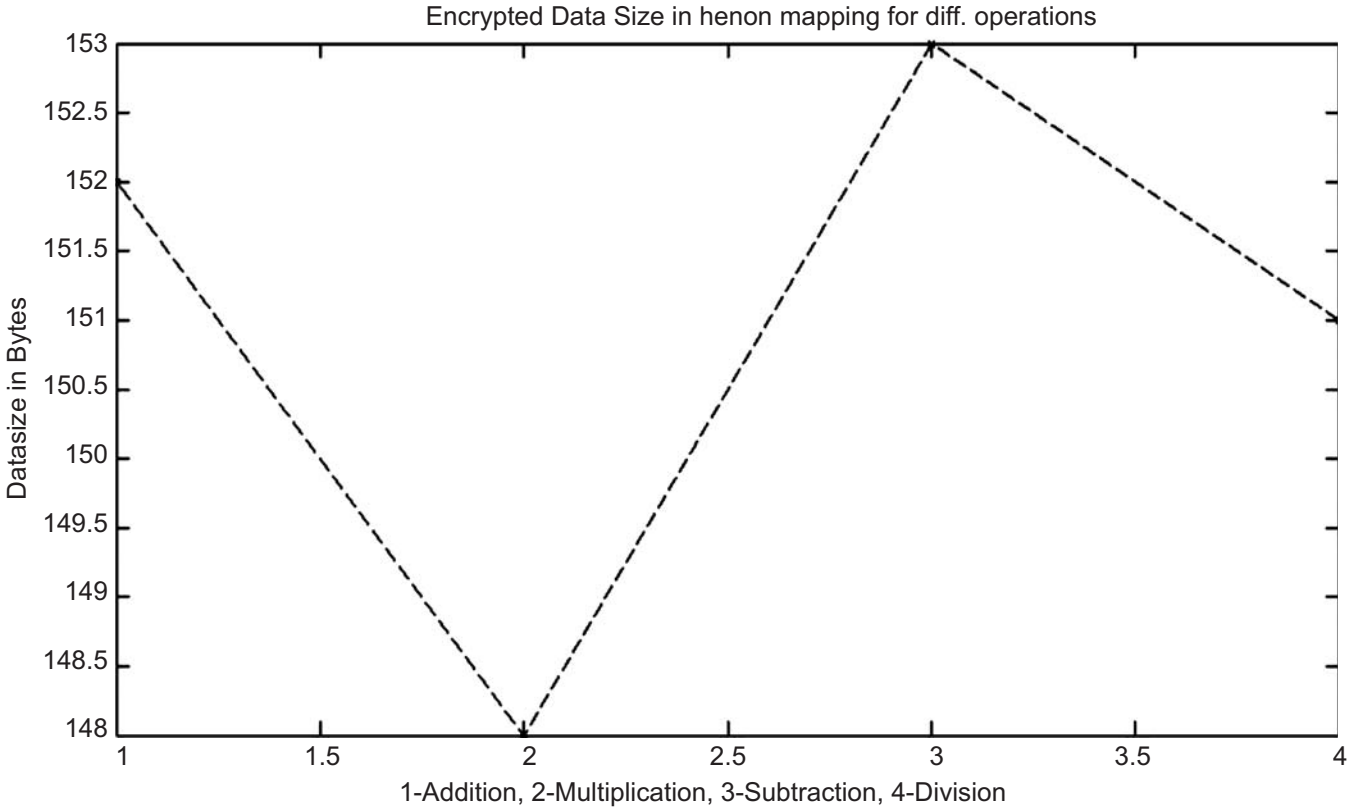

Figure 10: Encrypted Data size in Henon Map

8. REFERENCES

1. Raj Kumar Buyya, James Broberg, Andrzej Goscinski (2011),"Cloud computing-Principles and paradigms", JohnWiley's publications.
2. SrinivasJ, Venkata Subba Reddy K and Dr. Moiz QyserA (2012),"Cloud Computing Basics", International Journal of Advanced Research in Computer and Communication Engineering,Vol.1, Issue 5, pp. 343-347.
3. Kelion, L., (2014). Apple toughens iCloud security after celebrity breach, Available at: http://goo.gl/vyxS3S.
4. Ismail, I.A., Amin, M. & Diab, H. (2010), "A Digital Image Encryption Algorithm Based on Composition of Two Chaotic Logistic Maps.", Int. J. Network Security, vol. 11, no. 1, pp. 1-10.
5. Elminaam Diaa Salama Abdual., Kader Hatem Mohamed Abdual and Hadhoud Mohiy Mohamed (2009), "Tradeoffs between Energy Consumption and Security of Symmetric Encryption Algorithms", International Journal of Computer Theory and Engineering, Vol. 1, No. 3, pp. 325-333.
6. Elminaam Diaa Salama Abdual., Kader Hatem Mohamed Abdual and Hadhoud Mohiy Mohamed (2010), "Evaluating the Performance of Symmetric Encryption Algorithms", International Journal of Network Security, Vol.10, No.3, pp.213- 219.
7. Elminaam Diaa Salama Abdual., Kader Hatem Mohamed Abdual and Hadhoud Mohiy Mohamed (2010), "Evaluating the Effects of Symmetric Cryptography Algorithms on Power Consumption for Different Data Types", International Journal of Network Security, Vol.11, No.2, pp.78- 87.
8. Anthony Bisongl and Syed (shawon) M. Rahman (2011), An overview of the security concerns n enterprise cloud computing", International Journal of Network Security and its Application's p(IJNSA),Vol.3,N0.1,DOI :10.5121/ijnsa.2011.3103.

9. Seth S.M. and R. Mishra (2011)," Comparative analysis of encryption algorithms for data communication", Int. J. Comput. Sci. Telecommun., 2:292-294.
10. Elminaam D.S.A., H.M. Abdul-Kader and M. M. Hadhoud (2010),"Evaluating the performance of symmetric encryption algorithms", Int. J. Network Sec., 10:216-222.
11. Anjali Patil, Rajeswari Goudar (2013),"A Comparative survey of symmetric encryption techniques for wireless devices", Vol.2, issue 3.
12. Ovunc Kocabas, Tolga Soyata (2015),"Emerging Security Mechanisms for Medical Cyber Physical Systems", IEEE/ ACM Transactions on Computational Biology and Bioinformatics, pp.1-16, DOI: 10.1109/TCBB. 2016.2520933.
13. Singh S.P. and R. Maini (2011),"Comparison of data encryption algorithms", Int. J. Comput. Sci. Commun., 2, pp.125-127.
14. Verma O.P, R. Agarwal, D. Dafouti and S. Tyagi (2011),"Performance analysis of data encryption algorithms", Proceedings of the 3rd International Conference on Electronics Computer Technology, April 8-10, 2011, Kanyakumari, pp.399-403.
15. Lokhande V. and P.P.Kumar (2012),"Efficient encryption and decryption services for cloud computing", Int. J. Social Appl. Comput. Sc., 1, pp.71-75.
16. Kumar, S.K. and S. Venkateswarlu (2013), "Efficiently providing data security and linear programming in cloud computing", Int. J. Comput. Sci. Res. Technol., 4:630-632.
17. Wang C., Q. Wang, K. Ren and W. Lou (2009),"Ensuring data storage security in cloud computing", Charleston, SC., USA. pp.1-9.
18. MD Asif Mushtaque, Harsh Dhiman, Shahnawaz Hussain, Shivangi Maheshwari (2014), "Evaluation of DES, TDES, AES, Blowfish and Two fish Encryption Algorithm: Based on Space Complexity", International Journal of Engineering Research & Technology (IJERT), Vol. 3 Issue 4, ISSN: 2278-0181,pp.283-286.
19. Jain N.and G.Kaur (2012), "Implementing DES algorithm in cloud for data security", VSRD Int. J. Comput. Sci. Inform.Technol, 2, pp.316-321.
20. Mansour I, Chalhoub G, Barkhache B (2012),"Evaluation of a fast symmetric cryptographic algorithm based on the chaos theory for wireless sensor networks", In Proceedings of the IEEE 11th International Conference on Trust,Securty, and privacy n computing and communcatons,Liverpool,UK,25-27 June 2012,pp.913-919.
21. Verhulst, P.F (1847)," Deuxieme memoire sur la loi d'accroissement de la population", Mem. Del' Academie Royale des Sci., des letters et des Beaux-Arts de Belgique 20, pp.1–32.
22. Henon, M (1976), "A two-dimensional mapping with a strange attractor. Communications", Math. Phys. 50, pp.69–77.
23 Jakimoski G, Kocarev L (2001),"Chaos and Cryptography: Block encryption ciphers based on chaotic maps", IEEE trans. circ. Syst. fund. Theor. Appl. 48, pp.163-169.
24. Rani P. J, Bhavani S.D (2012),"Symmetric encryption using logistic map", International conference on recent advances in information Technology(RAIT),Dhanbad,India,15-17,pp.1-5.
25. Kamil I.A, Fakolujo O.A (2008),"Lorenz-Based Chaotic Secure Communication Schemes, Ubiquitous Comput. Commun. J.", 7,148-154.
26. Kocarev L (2001), "Chaos based cryptography: A brief overview", IEEE circ. Syst. Mag, 1, 1-16.
27. Li, S., Zheng, X (2002),"Cryptanalysis of a Chaotic Image Encryption Method", In: IEEE Int. Symp. Circuits and Systems, vol. 2, pp. 708–711.
28. Yen, J., Guo, J (2000),"A new chaotic key-based design for image encryption and decryption", In: IEEE Int. Conf. Circuits and Systems, vol. 4, pp. 49–52.
29. Solak E (2005),"Cryptanalysis of observer based Discrete time chaotic Encryption Schemes", International Journal of Bifurcat. Chaos Appl. Sci. Eng., 15,653-658.
30. Bakhache B, Ahmed K,el Assad S (2011),"A New Chaotic Encryption Algorithm to enhance the security of zig bee and Wi-Fi Networks",Int. J. Intell. Comp. Res, 219-227.
31. Linda F. R., Hammami S., Benrejeb M., Borne P., (2012), "Synchronization of Discrete-Time Hyper chaotic Maps Based on an Aggregation Technique for Encryption", 9th International Multi-Conference on Systems, Signals and Devices, Chemnitz, Germany, pp.1-6.

32. Wei J., Zheng X., Yu J., Shuai Y, (2013),” A novel Authentication Scheme Based on Chaos”, 8th International Conference on Computer Science & Education, Colombo, Srilanka, pp.879-882.

33. Kelber K., Schwarz W., (2005), ” General Design Rules for Chaos-Based Encryption Systems, International Symposium on Non-Linear Theory and its Applications NOLTA”, Bruges, Belgium, pp.465-468.

34. Prasadh k., Ramar K., Gnanajeyaraman R., (2009), ”Public key Cryptosystems Based on Chaotic Chebyshev Polynomials”, J. Eng. Tech. Res., 1, pp.122-128.

35. Wong K.W., Yuen C.H., (2008),”Embedding Compression in Chaos-Based Cryptography”, IEEE Trans. Circ. Syst., 55, pp.1193-1197.

36. Wei J., Zheng X.,Yu J., Shuai Y, (2012), ”Application of Unicity Distance in a Cryptosystem Based on Chaos”, 7th International Conference on Computer Science & Education , Melbourne, Australia, pp.345-348.

37. Alvarez G., Li S., (2006),”Some Basic Cryptographic Requirements for Chaos-Based Cryptosystems”, Int. J. Bifurcat. Chaos Appl. Sci. Eng., 16, pp.2129-2151.

38. Tenny, R., Tsimring, L. S., Abarbanel, H. D. I., and Larson,L. E. Security of chaos-based communication and encryption. Digital Communications Using Chaos and Nonlinear Dynamics (Institute for Nonlinear Science). Springer, 2006, pp. 191–229.

39. R.M. May (1976), “Simple mathematical model with very complicated dynamics”, Nature 261,459.