International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868
Foundation of Computer Science FCS, New York, USA
International Conference and Workshop on Communication, Computing and Virtualization (ICWCCV 2015) – www.ijais.org

Development of Security Enhancement Techniques for 3G/4G Networks

Punjabi Jasbir Kaur
Information Technology
TCET, Mumbai

Vikas Kaul,
Vinayak A.Bharadi, PhD
Information Technology
TCET, Mumbai

S K Narayankhedkar, PhD
MGMCET
Navi Mumbai, India

ABSTRACT
4G, the next-generation mobile telecommunication system, is the requirement for security enhancement and reliable communication. This paper presents the design of security enhancement techniques for data transmission in LTE networks using TLS. Here AES is used for encryption. AES is enhanced by using Chaos and Dynamic S-box. By the use of chaos the shift rows is made dynamic and the key space is made infinite. S-box is made dynamic and key-dependent using cipher key.

Complexity of the system is increased by using AES in round structure.

Comparison of the traditional and enhanced AES will be made on the basis of Performance evaluation using Encryption Time, Decryption Time, Overall Time, and Throughput.

Keywords
4G; AES; S-box; Round structure; Chaos

1. INTRODUCTION
Cryptography is the practice and study of techniques for secure communication in the presence of third parties. In the present era of information technology, cryptography assumes special importance. Cryptography is now routinely used to protect data, which must be communicated and/or saved over long periods, to protect electronic fund transfers and classified communications. Current cryptographic techniques [1] are based on number theoretic or algebraic concepts.

After the release of 1G system currently 4G, the next-generation mobile telecommunication system, is the requirement for security enhancement and reliable communication. A 4G system, in addition to the usual voice and other services of 3G, provides mobile broadband Internet access, for example to laptops with wireless modems, to smartphones, and to other mobile devices. 4G wireless networks operate entirely on the TCP/IP, hence it can be said that it is completely IP based.

One of the most powerful encryption techniques is Advance Encryption Standard (AES).To provide end-to-end security for data transmission, Transport Layer Security (TLS) is used. In TLS, AES is used for providing confidentiality. But since the core structure of AES itself renders a clean, simple algebraic method, it yielding the algorithm susceptible towards algebraic based cryptanalysis attacks.

Hybridization of AES with other popular algorithms like DES,ECC, RSA [2-4] etc. can enhance its strength. AES is enhanced using dynamic S-Box and Chaos concept.

Chaos is another paradigm, which seems promising [6]. Chaos is an offshoot from the field of nonlinear dynamics and has been widely studied. A large number of applications in real systems are being investigated using this novel approach of nonlinear dynamics [7]. The chaotic behaviour is a subtle behaviour of a nonlinear system, which apparently looks random. However, this randomness has no stochastic origin. It is purely resulting from the defining deterministic processes [8]. The important characteristic of chaos is its extreme sensitivity to initial conditions of the system. Enhancement of the key generation method of AES using chaos has increased more confusion and diffusion.

Dynamic S-Box is generated using cipher key algorithm in which static S-Box is converted to dynamic to increase the cryptographic strength of AES cipher system[29]. The inverse S-box is also changed according to the S-box.Analysis of algorithm is done on the basis of various parameters. The parameters are encryption time, decryption time, overall time, throughput, avalanche effect, CPU usage, and memory consumed.

1.1 Advance Encryption Standard
The Advanced Encryption Standard, an algorithm also known as Rijndael after its inventors Vincent Rijmen and Joan Daemen. This algorithm acts on 128-bit blocks and can use a key of 128, 192 or 256 bits in length. For encryption, each round consists of the four steps: Substitute bytes, Shift rows, Mix columns, and Add round key. For decryption, each round consists of the steps: Inverse sub bytes, inverse shift rows, inverse mix columns and Add round key.

1.2 AES S-box
The Rijndael S-box is a matrix (square array of numbers) used in the Advanced Encryption Standard (AES) cryptographic algorithm. The S-box is the substitution box which serves as a lookup table. The S-box is generated by determining the multiplicative inverse for a given number in GF (2^8).

1.3 Chaos Concept
The chaos is one kind of nonlinear movement form. It is produced by a definite system, and it relies on the initial condition, and it is unpredictable. The chaos system has

several characteristics: stochastic, sensitive to initial condition, long-term unpredictability and so on. Chaos theory studies the behaviour of dynamical systems that are highly sensitive to initial conditions.

2. LITERATURE SURVEY

In 1991, Mark E. Bianco and Diamond Bar, employees of Hughes Software Company have registered a patent on Encryption System Based on Chaos Theory [14]. An encryption system and method based on the mathematics of Chaos theory, which provides protection of data from unauthorized modification and use during its storage and transmission. In year 2001, L Kocarev has enhanced the work on the concept which included chaos in cryptography [10]. Research performed by Nicolas Courtois and Josef Pieprzyk showed that the AES was designed as a set of over defined system of Multivariate Quadratic equations (MQ) [18]. In February 2001, G. Jakimoski, L. Kocarev shows the analysis of the impact of chaos-based techniques on blockencryptionciphers. It presents several chaosbasedciphers [15]. To overcome the drawback of Algebraic attacks on AES, M.B. Vishnu, S.K. Tiong, Member IEEE, M. Zaini, Member IEEE, S.P. Koh, Member IEEE, introduced a new algorithm called Hybrid AES-DES used to secure transmission of digital motion image. In September 2008, Krishnamurthy G N and V Rama swamy in this paper[23] made S-box key dependent without changing its value and without changing the inverse S-box. The paper [5] shows conversion of static S-box to dynamic based on one-dimensional chaotic maps. In 2010, two professors, Jonathan Blackledge and Nikolai Ptitsyn, have given the concept of Encryption using Deterministic Chaos in 2010. In this they answered the meaning of being 'random', 'unpredictable' and 'complex 'and what do these properties mean mathematically and how do they relate to chaos. Also showed the issues associated with designing pseudo-random number generators based on chaotic systems.RaziHosseinkhani and H. Haj SeyyedJavadi generate Dynamic S-Box using cipher key in AES Cipher System in 2012. They change static S-box into dynamic to increase the cryptographic strength of AES cipher system. In this paper [25] they described the process of generating S-Box dynamically from cipher key and finally analyze the results and experiments. In this paper [26], Julia Juremi, RamlanMahmod, SalasiahSulaiman made AES S-box key dependent to make AES stronger. Here, only the S-box is made key-dependent without changing the value. In January 2013 in this paper [27] by ShabaanSahmoud, WisamElmasry and ShadiAbdulfa proposed enhancement of the security of AES against modern attacks by using variable key block cipher.

3. PROPOSED SYSTEM

3.1 Research Gaps

In the paper, Enhancement the security of AES against modern attacks by using variable key block cipher, according to the results it appears that the algorithm is slower and has more complexity to AES.

In the paper, Security Enhancement of Digital Motion Image Transmission Using Hybrid AES-DES Algorithm, it does not provide resistant against algebraic attacks.

In the paper, AKA and Authorization Scheme For 4G Mobile Networks Based on Trusted Mobile Platform, authors explain the primary weakness in 4G security is that its use of cryptography does not provide end-to-end security. So, to secure the data, end-to-end encryption is done , e.g. Using SSL/TLS, SSH, a VPN.

3.2 Problem Definition

A cryptographic system should be designed with respect to three components:

- Cipher text generation
- Key exchange
- Authenticity

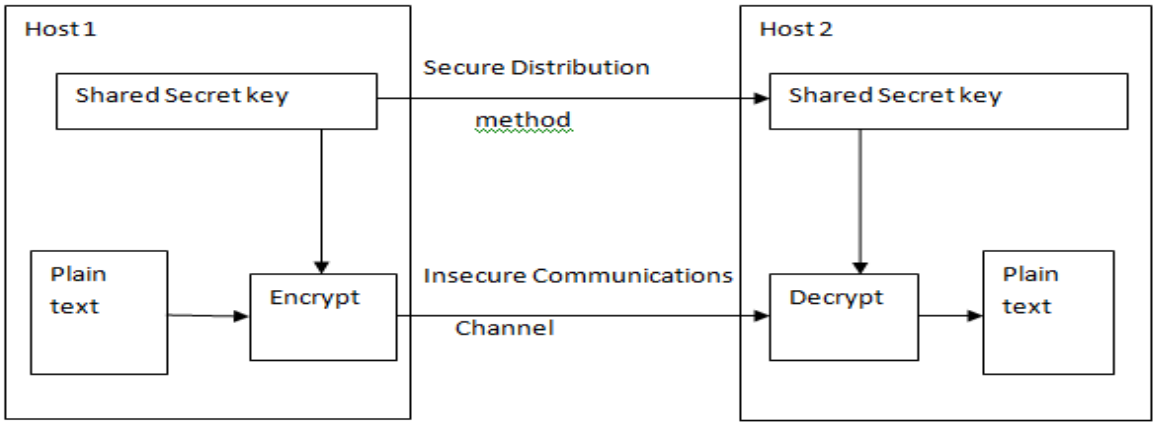

Figure 1: The Proposed System

The above diagram shows the overall security system which is inclusive of all the three aspects of secure data transmission:

Data Encryption: Using AES-128 Bit.

Message Authentication: Using SHA-256.

Key Exchange Mechanism: Using ECDHE-384.

This work is focused on enhancement on encryption algorithm but any enhancement in message authentication and key exchange is easily considerable. Further performance evaluation of selected symmetric encryption algorithms has to be done. The selected algorithms are AES, DES and DES with Feistal structure, AES with Feistal structure and Hybrid AES-DES structure. There are

certain attacks on the AES algorithm like linear, algebraic attacks hence to increase the complexity AES is used in Feistel structure. The S-box of AES algorithm is improved by making it dynamic [30]. Further performance evaluation of selected symmetric encryption algorithms has to be done. The performance evaluation has been done based on parameters: Avalanche Effect, Throughput, CPU Usage, Encryption and Decryption Time.

3.3 Model Development

Detailed Hybrid structure using chaos and dynamic S-box generation is shown in the following figure **Figure 4.1** Enhanced AES.

a) The objective is to provide end-to-end security for data transmission using TLS in which input data is converted to blocks and then can be applied to a hybrid structure in which AES is enhanced by using chaos and dynamic S-box using cipher key, within the Fiestal network .

b) The i/p data at the transmitter is converted into blocks and each block is divided into two sub blocks of exactly half the size and this is passed to a hybrid based AES which is constructed using Feistel equations and by incorporating the AES with dynamic S-box and chaos.

$$L_n = R_{n-1} \quad \text{----------} \quad (1)$$

$$R_n = \text{AES}\,(L_n \oplus f(R_{n-1}, K_n)) \quad \text{----------} \quad (2)$$

From Equation (2), each R_{n-1} and K_n is channeled into the round function, which basically revolves on aXOR function between these variables.

c) The output of the round function is then XORed with L_n - before being channeled as input data for the AES algorithm.

The key schedule process for the hybrid system uses concept of chaos. Two dimensional chaotic map [28] used here for key generation in AES. One generates the encryption key and other gives the number of shifts for the shift row round of AES. It will be enhanced by converting static S-box into dynamic which is forwarded to sub-bytes. This is done for 1, 5 and 10 rounds respectively.

d) The result from the AES process represents R_n.

e) After completing it, Equations (1) and (2) are then iterated over a number of rounds using dynamic S-box chaotic key sequences.

f) A complete Hybrid AES operation can be performed using 10 layers of Feistel calculations, including 10 sets of AES. This makes the system resistant to algebraic attacks and linear attacks.

g) Lastly, all the encrypted blocks are put serially for transmission and similar action has been performed. The inverse process can be applied similarly at the receiver end for decryption.

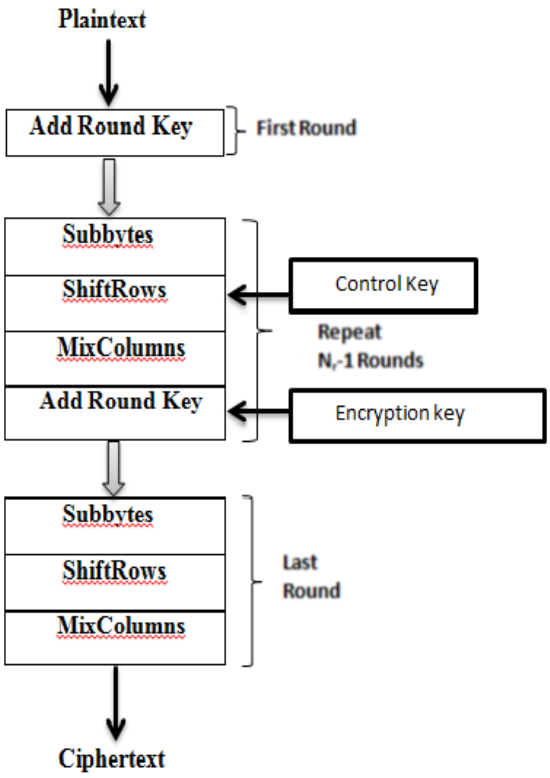

Figure 2 : AES with Chaos Concept

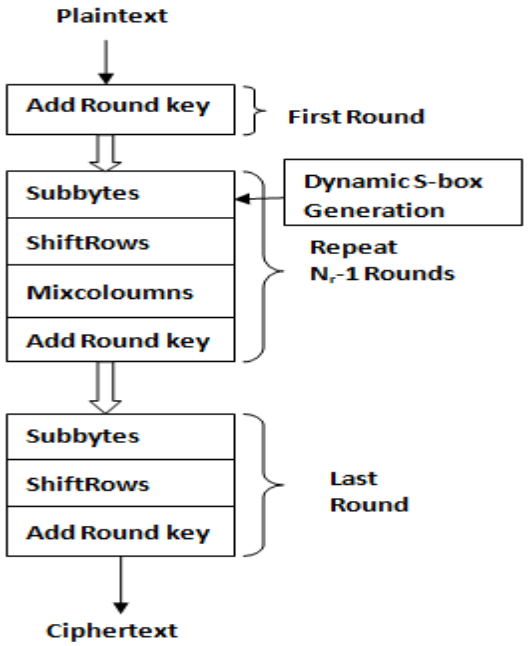

Figure 3 : AES with dynamic S-box

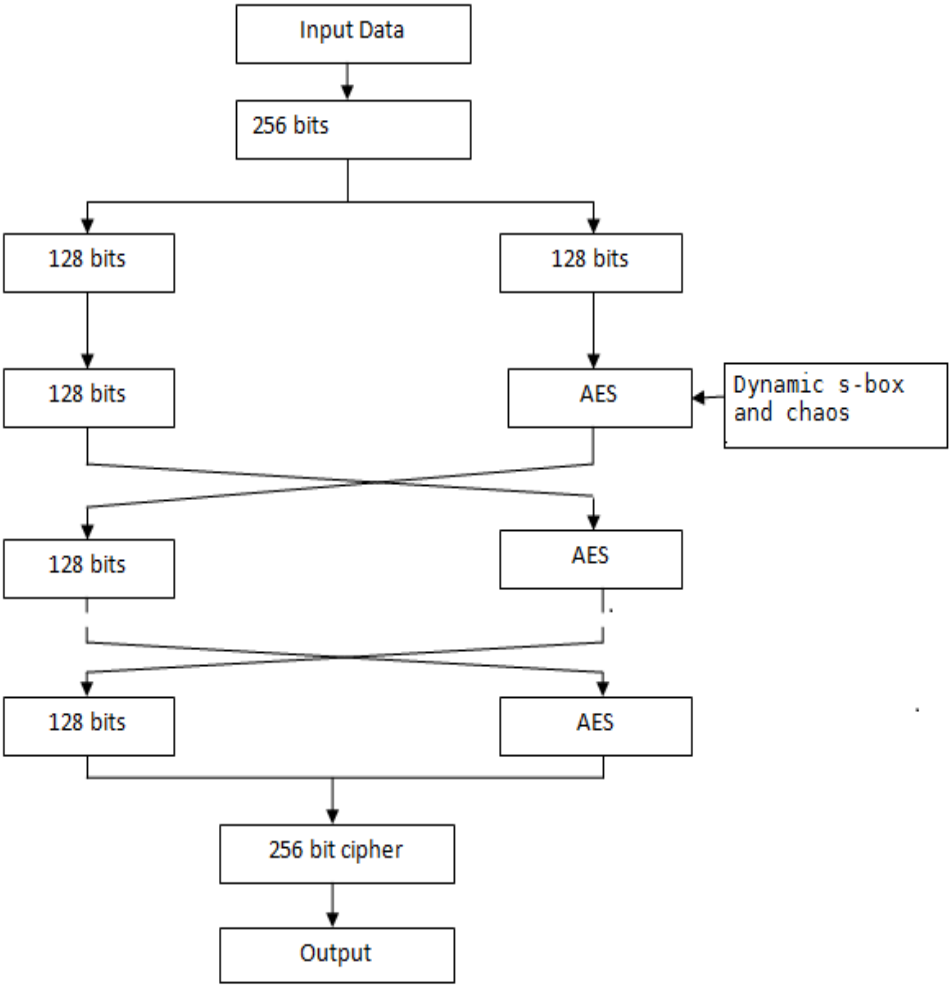

Figure 4: FiestelAES with chaos and dynamic S-box

4. EXPERIMENTAL RESULTS

The results carried out is based on encryption and decryption time. Computer Configurations used are Microsoft Windows 8.1, Intel i3 CPU 3210M @ 2.50 GHz, 4 GB RAM and Matlab 2013a. The results are tabulated as shown below.

For text file, "plaintext.txt" of 82 bytes, the number of bits is656

Table 1: Based on Encryption Time on Text file

Algorithm	Bits in one block	Total no of bits	Encryption Time	Decryption Time
AES	128	656	0.0671268	0.00580755
AES with dynamic S-box	128	656	0.151179	0.00257444
AES with chaos	128	656	0.021632	0.032344

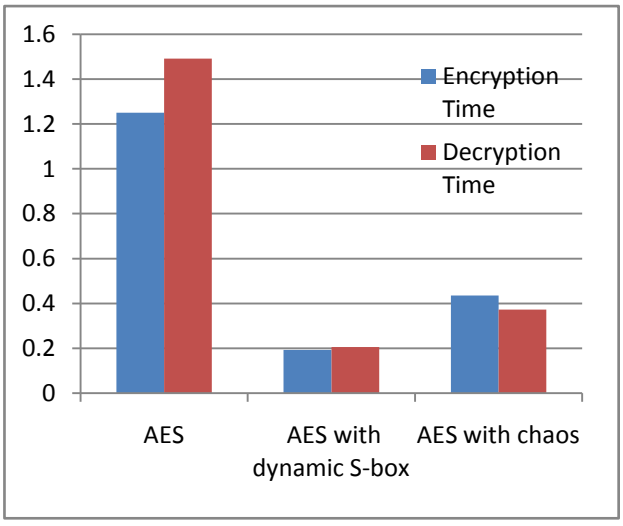

Figure 5: Graphical representation of results based on encryption time on Text file

For Image file, "smiley.jpg" of 2.35 KB, the number of bits is 19328

Table 2: Based on Encryption Time on Image file

Algorithm	Bits in one block	Total no of bits	Encryption Time	Decryption Time
AES	128	19328	1.25079	1.49089
AES with dynamic S-box	128	19328	0.193199	0.205807
AES with chaos	128	19328	0.4356	0.3732

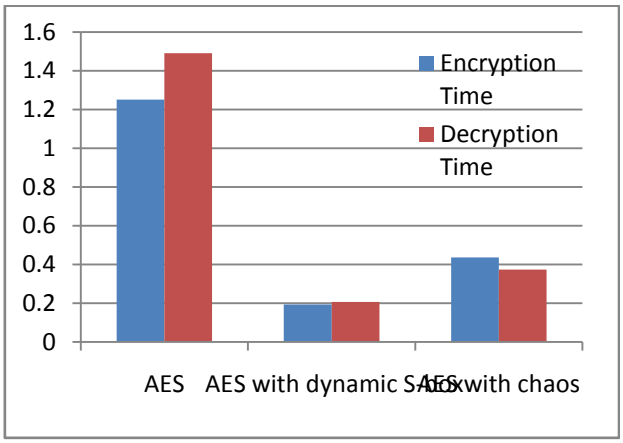

Figure 6: Graphical representation of results based on encryption time on Image file

5. CONCLUSION

4G technology offers high data rates that will generate new trends for the market and prospects for established as well as for new telecommunication businesses. The primary weakness in 4G security is that its use of cryptography does not provide end-to-end security. So to provide end-to- end security, SSL/TLS is used.

TLS is a protocol created to provide authentication, confidentiality and data integrity between two communicating applications. Hence Transport Layer Security is used for security in this project. TLS uses AES as an encryption algorithm. AES is one of the encryption techniques which is used most frequently because of its high efficiency and simplicity.

Thus the enhanced model of AES gives a better non linearity to the orignal AES and because of its round structure, there is better diffusion. Hence the possibility of an algebraic attack and linear attack on this model is reduced. It is enhanced by converting static S-box into dynamic AES itself. The S-box can be made dynamic using cipher key.

We hope to increase the complexity of system, by using an AES Round(Fiestel) structure. The reason behind increasing complexity is to make the system attack resistant and make the data secure from attackers. We also hope to evaluate the system for audio file,video file and use QPSKmodulation/demodulation along with AWGN channel to create 4G scenario. This will be the future scope of the work.

6. ACKNOWLEDGMENTS

I have immense pleasure in presenting paper on "Development of security enhancement techniques for 3G/4G networks".

With deep sense of gratitude, I acknowledge all those who have made it possible for me to have an opportunity to work on this project. I' am also grateful for the invaluable support given by my family and staff of the Information Technology department.

I also take this opportunity to convey my sincere thanks to my guide Mr. Vikas Kaul and H.O.D. Dr. Kamal Shah.

I also thank for the great computing facilities extended and the freedom allowed to me throughout by my esteemed alma mater, Thakur College of Engineering and Technology. Finally I also my express deep gratitude to my family members and friends for their patience and encouragementwithout whom, it would not have been possible to collect and assimilate the information on the Report.

7. REFERENCES

[1] Shannon C E, Communication Theory of Secrecy Systems, bell Systems Technical Journal,1949:28:656-715.

[2] M.B. Vishnu, S.K. Tiong. "Security Enhancement of Digital Motion Image Transmission Using Hybrid AES-DES Algorithm," APCC 2008 OF IEICE, 2008.

[3] Xiang Li, Junli Chen, Dinghu Qin, Wanggen Wan. "Research and Realization based on hybrid encryption algorithm of improved AES and ECC," IEEE journal 2010.

[4] Dr. E. Ramaraj, S. Karthikeyan and M. Hemalatha. "A Design of Security Protocol using Hybrid Encryption Technique (AES- Rijndael and RSA)," International Journal of The Computer, the Internet and Management Vol. 17.No.1, April 2009.

[5] GhadaZaibi, AbdennaceurKachouri, FabricePeyrard, Daniele Foumier-Prunaret, "On Dynamic chaotic S-BOX," IEEE 2009

[6] L Kocarev. "Chaos-based Cryptography:aBrief overview," IEEE Circuits and Systems Magazines,2001:1(3):6~22

[7] Gonzalo Alvarez1 and Shujun Li2, "Some Basic Cryptographic Requirements for Chaos-Based Cryptosystems," International Journal of Bifurcation and Chaos, vol. 16, no. 8, pp. 2129-2151, 2006

[8] Blackledge, J., Ptitsyn, N.: Encryption using Deterministic Chaos. "ISAST Transactions onElectronics and Signal Processing," vol. 4,issue 1, pp. 6-17. 2010.

[9] Bruce Shneier, "Applied Crptography :protocol Algorithms," and source code in C.Johnwiley&Sons,Inc, 1996.

[10] LjupcoKocarev and ShiguoLian (Eds.): "Chaos-Based cryptography, Theory," Algorithms and Applications. Studies in Computational Intelligence ISSN 1860-949X, 2011 Springer-Verlag Berlin Heidelberg.

[11] George Makris ,Ioannis Antoniou, "Cryptography with Chaos Proceedings," 5th Chaotic Modeling and Simulation, International Conference, 12 – 15 June 2012, Athens Greece.

[12] Next generation Encryption, Cisco Security Intelligence Operations, 2012,http://www.cisco.com/web/about/security/intelligence/nextgen_crypto.html

[13] Yuan Kun, Zhang Han Li Zhaohui, "An Improved AES algorithm based on chaos," International Conference on Multimedia Information Networking and Security 2009.

[14] Bianco et al, "Encryption System Based on Chaos Theory," United State Patent, Patent Number:5,048,086 Date of Patent Sep. 10, 1991.

[15] G. Jakimoski,L. Kocarev , "Chaos and Cryptography: Block Encryption Ciphers Based on Chaotic Maps," IEEE transactions on circuits and systems: Fundamental Theory and Applications, vol. 48, No2, pp. 163–169, February 2001.

[16] Chung-Ming Ou, "Design of Block Ciphers by Simple Chaotic Functions," IEEE computational intelligence magazine, pp. 54–59, May 2008.

[17] N. Masuda, K. Aihara, "Cryptosystems with discretized chaotic maps," IEEE Trans CircSyst-I 2002;49(1):2840.

[18] N. Courtois, A. Klimov, 1. Patarin, A. Shamir, "Efficient algorithm for solving overdefmed systems of muhivariate polynomial equations," Proceedings for Eurocrypt 2000, LNCS 1807, pp 392407,Springer-Verlag, 2000.

[19] Zhao Rui. Wang Qingsheng. Wen Huiping, "Design of AES Algorithm Based on Two Dimensional Logistic and Chebyshev Chaotic Mapping," 2008.

[20] Q.V. Lawande, B. R. Ivan, S. D. Dhodapkar, "Chaos Based Cryptography," A New Approach to Secure Communications, BARC News Letter, July 2005.

[21] Jing Wang, Guo-ping Jiang, "Improved DES Algorithm Based On Irrational Numbers," IEEE Int. Conference Neural Networks & Signal Processing, Zhenjiang, China, June 8~10, 2008.

[22] BassemBakhache, "A New Chaotic Encryption Algorithm to Enhance the Security of ZigBee and Wi-Fi networks," International Journal of Intelligent Computing Research (IJICR), vol.2, Dec 2011.

[23] Krishnamurthy G N, V Ramaswamy, "Making AES Stronger: AES with Key Dependent S-Box," IJCSNS International Journal of Computer Science and Network Security, vol.8 No.9, September 2008

[24] V. Sumathy& C. Navaneethan, "Enhanced AES Algorithm for Strong Encryption," International Journal of Advances in Engineering & Technology, Sept 2012. ©IJAET ISSN: 2231-1963.

[25] RaziHosseinkhani, H. Haj SeyyedJavadi, "Using Cipher Key to Generate Dynamic S-Box in AES Cipher System," International Journal of Computer Science and Security (IJCSS), Volume (6) : Issue (1) : 2012

[26] Julia Juremi, RamlanMahmod, SalasiahSulaiman, "A Proposal for Improving AES S-box with Rotation and Key-dependent," Cyber Warfare and Digital Forensic (CyberSec) international conference, 2012

[27] ShabaanSahmoud, WisamElmasry and ShadiAbdulfa, "Enhancement the security of AES against modern attacks by using variable key block cipher,"International Arab Journel of e-technology, Vol 3,No. 1, January 2013

[28] Neha Jain, Vikas Kaul and S K Karayankhedkar, "Security Enhancement Algorithm for Data Transmission for Next Generation Networks," IJCA Proceedings on International Conference and Workshop on Emerging Trends in Technology 2013ICWET(2):1-6, April 2013.

[29] Vikas Kaul, Prerana Choudhari, S K Narayankhedkar, "Security Enhancement for Data Transmission In 4G Networks," IEEE The Next Generation Information Technology Summit (Confluence), Noida, India, September 2526,2014,ISBN:9781479942374,DOI:10.1109/CONFLUENCE.2014.6949278, pp:373-378.

[30] Vikas Kaul, Prerana Choudhari, S K Narayankhedkar, "Security Enhancement for Data Transmission In 4G Networks," International Journal of Advanced Research in Computer Science and Software Engineering 4(5), May - 2014,vol. 4, pp. 1232-1239