Volume 4, Issue 5, May 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Security Enhancement Algorithms for Data Transmission In 4G Networks

Prerana Choudhari [1]
Information Technology,
Mumbai University

Vikas Kaul[2]
Information Technology,
Mumbai University

S K Narayankhedkar[3]
Information Technology
Mumbai University

Abstract—In this paper, the design and evaluation of security enhancement for data transmission in 4G networks is presented. An enhanced encryption method with AES algorithm is used here. Enhancement is done by applying dynamic S-box to Round structured AES. The static S-box is made dynamic using cipher key. The inverse S-box is also modified accordingly. Complexity is increased using Round structure to make the system attack resistant. 4G simulation model is developed by using AWGN channel and BPSK modulator/demodulator. Comparison is made between AES and the enhanced system on the basis of performance evaluation based on Runtime and Throughput.

Keywords— 4G; AES; S-box; Round structure; LTE

I. INTRODUCTION

Many new mobile generations have been developed after the release of first 1G system. 4G, the next-generation mobile telecommunication system, is being model for increased security and reliable communication. 4G wireless networks will operate entirely on the TCP/IP, so it becomes completely IP based. This makes 4G wireless technologies different from 3G and other preceding versions. Mobile TV, Web 2.0, and streaming content which are the recent expansion of wireless network technologies have led to the standardization of the Long-Term Evolution (LTE) protocol to become compatible with the 3rd Generation Partnership Project (3GPP)[1].

AES is one of the encryption techniques which are used most frequently because of its high efficiency and simplicity. It is the highly secure algorithm. Currently there are three cipher suites in 3GPP UMTS systems; including a block cipher Kasumi and two stream ciphers SNOW 3G and ZUC. Those cipher suites are used into the 4G-LTE standard. But Kasumi is replaced by AES in 4G-LTE [2]. AES represents the current recommended standard by NIST for encryptions.

128-bit Advanced Encryption Standard (AES) and SNOW3G algorithms are used in the Wireless 4G LTE network for integrity protection but 128-bit AES algorithm is the most preferred option [4]. EEA2 or EIA2 which used in LTE-SAE security are based on the Advanced Encryption Standard (AES) [7]. WiMAX standards specifies that, over-the-air transmissions should be encrypted hence it uses 168-bit Digital Encryption Standard (3-DES) or Advanced Encryption Standard (AES) [9]. Many researchers tries to combin other encryption algorithms with AES. So, it can be considered as a motivational factor for further enhancement of AES.

To enhance secure data transmission in 3G/4G, Transport Layer Security (TLS) is used here. Within TLS Advanced Encryption Standard (AES) is used for encryption. The goal of this work is to develop advanced encryption method using enhanced AES algorithm. The whole cryptographic system has been developed. This includes encryption of data, key exchange and message authentication. RSA is used for key exchange and SHA-256 for message authentication.

Then AES is used in Round structure for proposed system. The proposed algorithm generates dynamic S-box to enhance AES algorithm. In Round structured AES, S-box changes in every round. The cipher key is used to convert static S-box into dynamic. The inverse S-box is also changes according to the S-box.

Analysis of algorithm is done on the basis of various parameters. The parameters are encryption time, throughput, avalanche effect, CPU usage, and memory consumed.

A. 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.

B. 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).

C. BPSK

Phase-shift keying is a digital modulation scheme that modulates the phase of a reference signal and BPSK is the simplest form of phase shift keying (PSK). It uses two phases which are separated by 180°.

D. AWGN

AWGN is an Additive White Gaussian Noise and it implements AWGN channel. AWGN adds Gaussian noise to its input signal.

II. LITERATURE SURVEY

In September 2008, in the paper [15] S-box is made key dependent without changing its value and without changing the inverse S-box. In 2008, the paper [18] reviewed possible attacks on AES algorithm. The hybrid structure of AES-DES was proposed to overcome the weaknesses of AES algorithm. This paper presented the design and implementation of a symmetrical hybrid based 128 bit key AES-DES algorithm as a security enhancement for live motion image transmission. Feistel structure of AES and DES is used for the same. A study of security issues and vulnerability of 4G wireless network is done in the paper [11], in 2010. The authors analysed the security-related standards, architecture and design for the LTE and WiMAX technologies. They concluded that there is a strong need for continued study on 4G security issues and development. Razi Hosseinkhani and H. Haj Seyyed Javadi 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 their paper [14] they described the process of generating S-Box dynamically from cipher key and finally analyze the results and experiments. In the paper [21], Julia Juremi, Ramlan Mahmod, Salasiah Sulaiman made AES S-box key dependent to make AES stronger. Here, only the S-box is made key-dependent without changing the value.

In proposed system, we are increasing complexity of AES algorithm by using Round structure as well as enhancing AES algorithm by making S-box and inverse S-box dynamic.

III. PROPOSED SYSTEM

There are major drawbacks in other 3G/4G cipher algorithms hence AES cipher algorithm is used in the proposed system because AES is the most secure algorithm. AES is used in Round structure. There are two reasons behind doing this. First, the traditional AES algorithm uses 128 bit input data but enhanced system uses 256 bits input data and second is, there are certain attacks on the AES algorithm like linear, algebraic attacks hence to increase the complexity, AES is used in Round structure. The S-box and inverse S-box of AES algorithm is improved by making it dynamic.

This work is focused on enhancement of encryption algorithm. The whole cryptographic system has been developed in this work. This includes encryption of data, key exchange and message authentication. RSA is used for key exchange and SHA-256 for message authentication. Further performance evaluation of selected symmetric encryption algorithms has to be done. The performance evaluation will be done based on parameters: Avalanche Effect, Throughput, CPU Usage, Encryption and Decryption Time.

To create a 4G scenario AWGN channel along with BPSK modulator and demodulator is used.

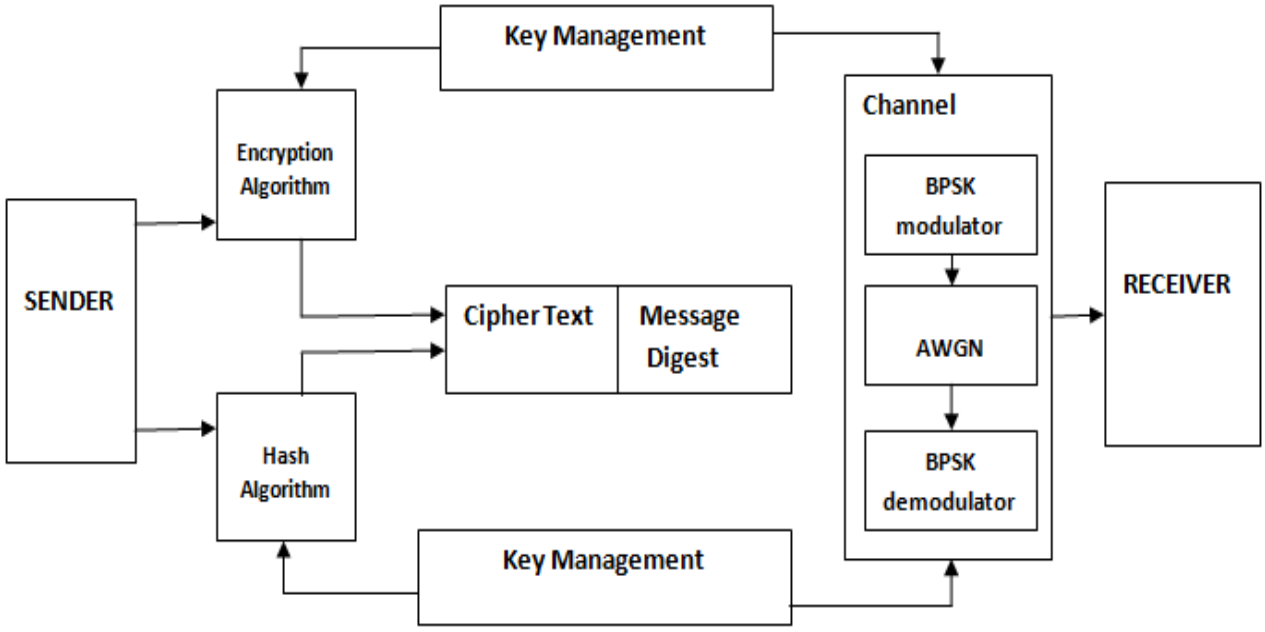

Fig.1. Proposed system

A. Model development

256 bits key length and 256 bit input data is given to the enhanced AES system. The proposed system's encryption and decryption is the same as traditional AES algorithm. The round function of encryption process is also similar as the traditional AES algorithm. The various models for developing enhanced system are as follows:

1) Dynamic S-box Generation

There is additional phase of making S-box dynamic as shown in Fig. 2. The hexadecimal digits of AES key are XORed with each other and obtained number is used as the shift value to the S-box. The S-box is rotated by that shift value.

Before sub byte stage, the static S-box is converted into dynamic using cipher key. The inverse S-box is also modified after S-box to obtain correct inverse values.

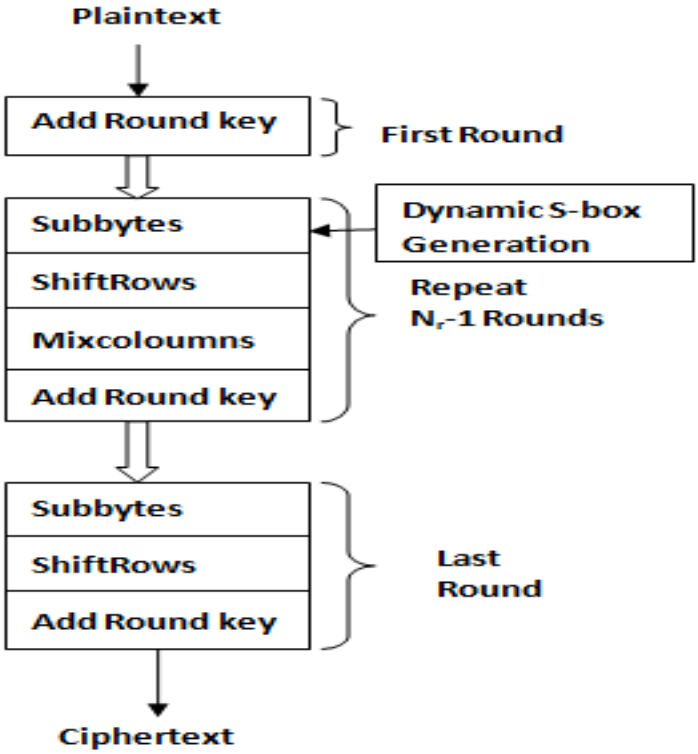

Fig.2. AES dynamic S-box

2) Round AES Generation

The Round structure of AES is used as shown in Fig. 3. Here the Input Data is split into two blocks of 128 bits each. One Block is given as Input to the AES section of the System. The other Block is given as Input to the AES section of the System in the next round as per the Round structure. This is done for all ten rounds respectively. These outputs are then combined together to form 256 bit block of encrypted data.

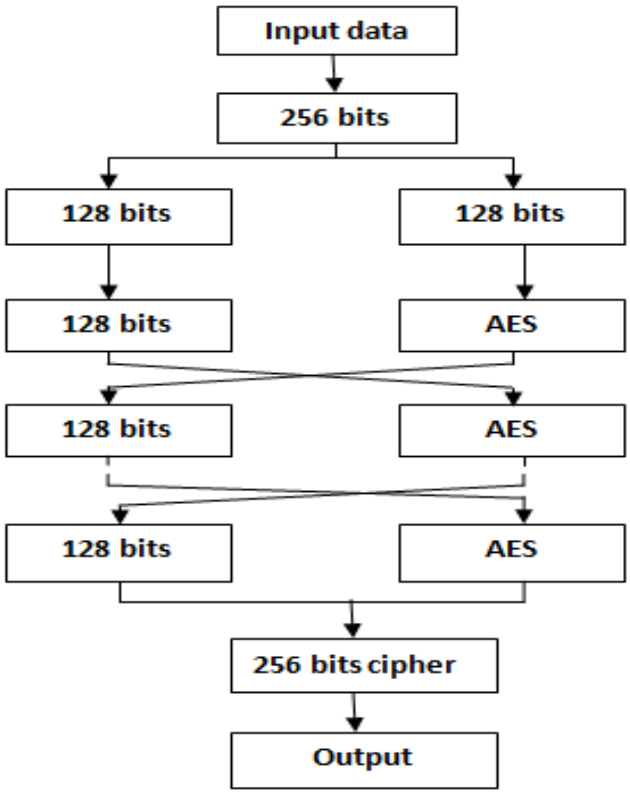

Fig .3. Round AES

3) Round AES with Dynamic S-box Generation

Dynamic S-box is applied to the Round structure of AES as shown in Fig. 4. In the round structure , ten times AES is applied to the block of data hence total ten times different S-box is created hence it is called dynamic S-box.

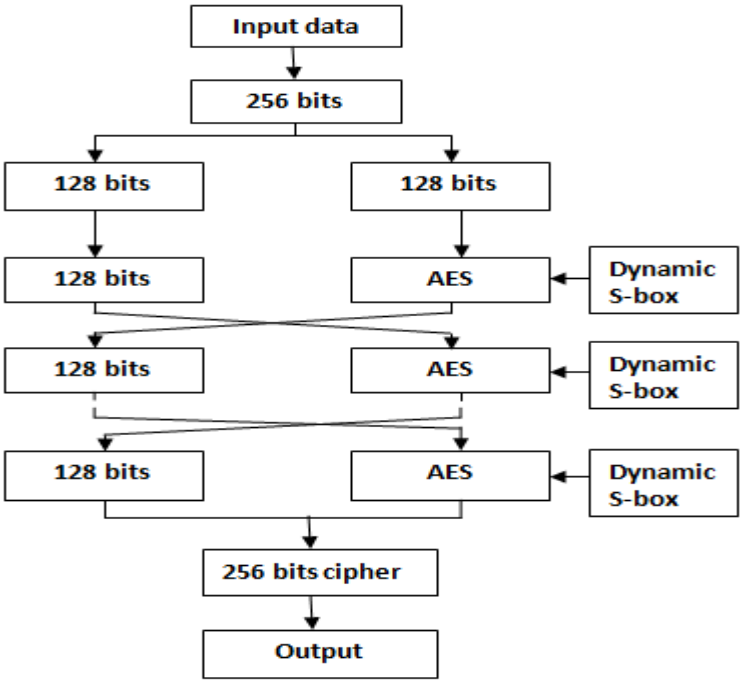

Fig. 4. Round AES with Dynamic S-box

IV. EXPERIMENTAL RESULTS

The results carried out till the date is based on encryption and decryption time and throughput. Time taken to encrypt same amount of data in one round of Round AES network will be much lesser than AES. If we use ten rounds of Round structure, we can get more complexity than AES-CBC with same encryption time. An encryption algorithm is required which can cope up with the speed because 3G and 4G networks works on high data rate.

Computer Configurations used are Microsoft Windows 7, Intel i5 CPU 3210M @ 2.50 GHz, 4 GB RAM and Matlab 2013a. The results are tabulated as shown below.

A. For input text file

For text file, "plaintext.txt" of 82 bytes, the number of bits is 656 and key is "enhanced aes key".

TABLE I

BASED ON ENCRYPTION TIME ON TEXT FILE

Algorithm	Bits in one block	Total no of bits	encryption time	decryption time
AES	128	656	0.015781	0.007095
AES with dynamic S-box	128	656	0.020823	0.015011
Round structured AES with dynamic S-box	256	656	0.117755	0.058868

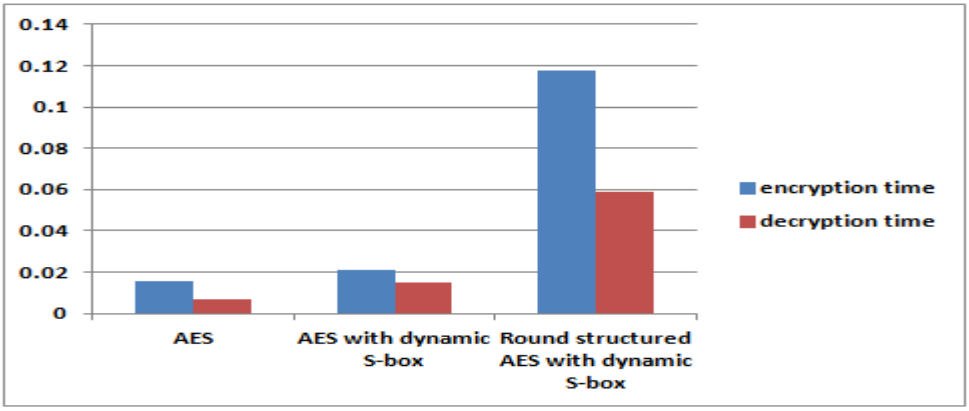

Fig. 5. Graphical representation of results based on encryption time on input text file

TABLE II

BASED ON THROUGHPUT ON INPUT TEXT FILE

Algorithm	**Bits in one block**	**Total no of Blocks**	**Throughput (kb/sec)**	
			Encryption	**Decryption**
AES	128	656	41.568	92.459
AES with dynamic S-box	128	656	31.503	43.701
Round structured AES with dynamic S-box	256	656	5.57	11.143

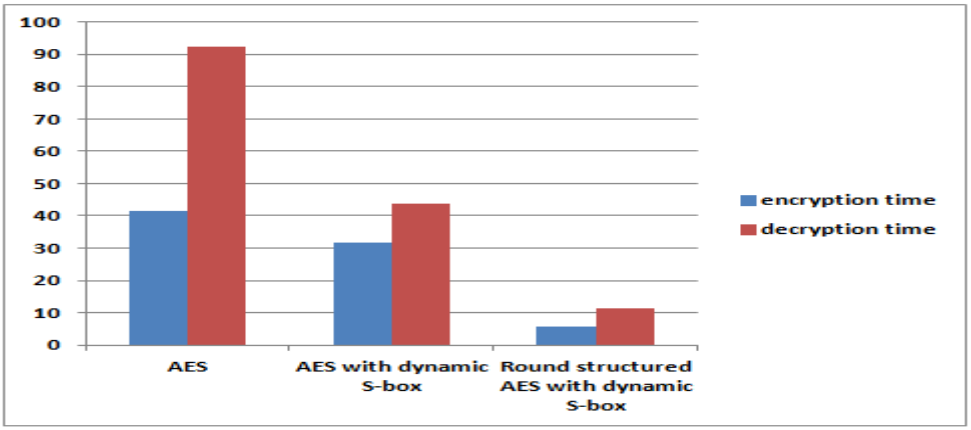

Fig. 6. Graphical representation of results based on encryption timeThroughput on input text file

B. For Input Image File

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

TABLE IIII

BASED ON ENCRYPTION TIME ON IMAGE FILE

Algorithm	**Bits in one block**	**Total no of bits**	**encryption time**	**decryption time**
AES	128	19328	0.143448	0.049601
AES with dynamic S-box	128	19328	0.131587	0.031739
Round structured AES with dynamic S-box	256	19328	0.117755	0.058868

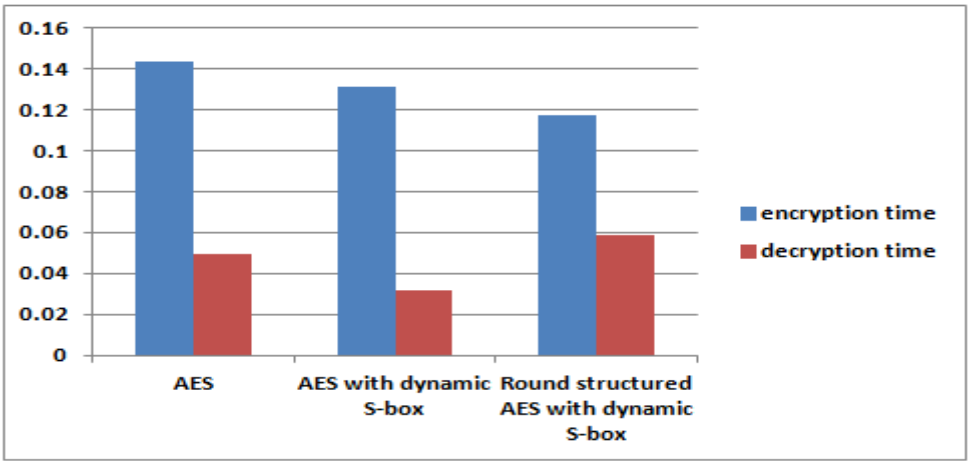

Fig. 7. Graphical representation of results based on encryption time on image file

TABLE IV

BASED ON THROUGHPUT ON IMAGE FILE

Algorithm	Bits in one block	Total no of Blocks	Throughput (kb/sec)	
			Encryption	Decryption
AES	128	19328	134.738	389.669
AES with dynamic S-box	128	19328	146.883	608.966
Round structured AES with dynamic S-box	256	19328	164.137	328.327

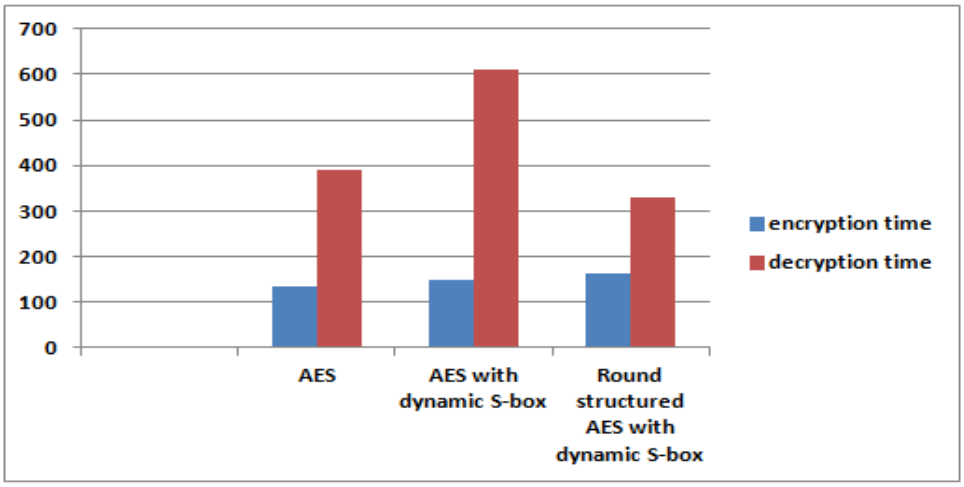

Fig. 8.Graphical representation of results based on encryption timeThroughput on image file

C. For input Audio File.

For Audio file, "Laser.wav" of 3.54 KB, the number of bits is 29040 and key is "enhanced aes key".

TABLE V

BASED ON ENCRYPTION TIME ON AUDIO FILE

Algorithm	Bits in one block	Total no of bits	encryption time	decryption time
AES	128	29040	0.303072	0.051795
AES with dynamic S-box	128	29040	0.262021	0.043913
Round structured AES with dynamic S-box	256	29040	0.249222	0.22978

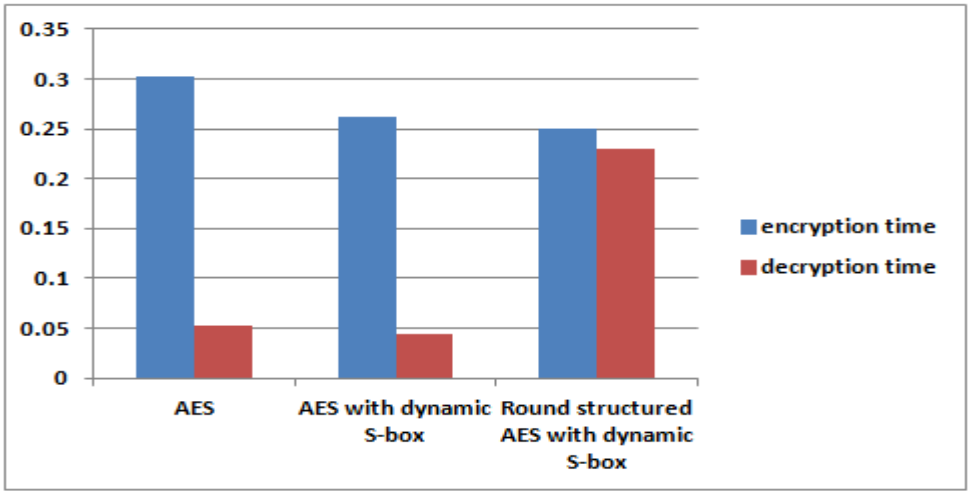

Fig. 9. Graphical representation of results based on encryption time on audio file

TABLE VI
BASED ON THROUGHPUT ON AUDIO FILE

Algorithm	Bits in one block	Total no of Blocks	Throughput (kb/sec)	
			Encryption	Decryption
AES	128	29040	95.818	560.671
AES with dynamic S-box	128	29040	110.83	661.307
Round structured AES with dynamic S-box	256	29040	116.522	126.381

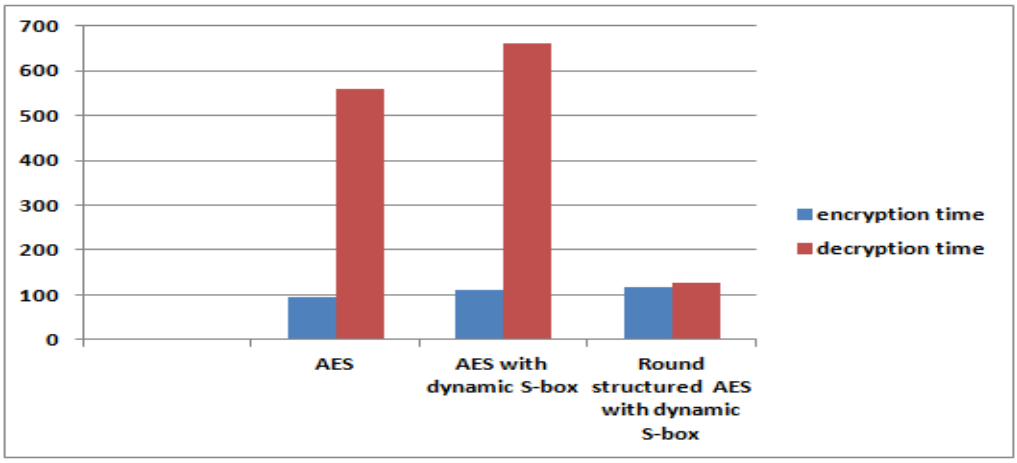

Fig. 10.Graphical representation of results based on encryption timeThroughput on audio file

V. CONCLUSION

End-to-end security has been an issue in 4G networks and hence a solution has to be proposed for the same using SSL/TLS, SSH, VPN, or a similar mechanism should be provided for security of data. Hence TLS is used here with AES as an encryption algorithm for security. To increase the complexity of system, an AES Round structure is used. The motivation behind increasing complexity is to make the system attack resistant and secure data from attackers. Hence we have concluded from the results that, when number of bits is increased, the encryption time is increased and throughput is decreased as shown in the tables. Though encryption and decryption time is increased, the complexity of network is increased with the number of bits in one block. So this system can be used in the application where time is not the constraint. 3G and 4G requires high data transmission rate in order to send image and the proposed algorithm encrypts the data in acceptable time. AES is enhanced by converting static S-box into dynamic using cipher key to make cryptography more strong.

We also hope to evaluate the system for video file and use BPSK modulation/demodulation along with AWGN channel to create 4G scenario and this will be the future scope of the work.

REFERENCES

[1] Qing Xiuhua, Cheng Chuanhui, Wang Li, ”A Study of Some Key Technologies of 4G System*”, Industrial Electronics and Applications, 2008. ICIEA 2008. 3rd IEEE Conference.

[2] Xinxin Fan, Gaung Gong, “Specification of the stream cipher WG-16 based confidentiality and integrity algorithm”, http://cacr.uwaterloo.ca/techreports/2013/cacr2013-06.pdf

[3] Sasan Adibi, Amin Mobasher, Mostafa Tofighbakhsh, Fourth-Generation Wireless Networks: Applications and Innovations, IGI Global, December 31, 2009

[4] The Verizon Wireless 4G LTE Network: Transforming Business with Next-Generation Technology, Verizon Wireless,

[5] http://business.verizonwireless.com/content /dam/b2b/resources/LTE_FutureMobileTech_WP.pdf

[6] Yu Zheng, Dake He, Xiaohu Tang and Hongxia Wang, “AKA and Authorization Scheme For 4G Mobile Networks Based on Trusted Mobile Platform”, ICICS 2005

[7] Anirudh Ramaswamy Ganesh, Naveen Manikandan P, Sethu S Pl, Sundararajan R, Pargunarajan K.,” An Improved AES-ECC Hybrid Encryption Scheme for Secure Communication in Cooperative Diversity based Wireless Sensor networks”, IEEE conference on Recent Trends in Information Technology (ICRTIT), 2011

[8] Anastasios N. Bikos, Nicolas Sklavos, “LTE/SAE Security Issues on 4G Wireless Networks”, IEEE Security & Privacy, 2013

[9] Ghada Zaibi, Abdennaceur Kachouri, Fabrice Peyrard, Daniele Foumier-Prunaret, “On Dynamic chaotic S-BOX”, IEEE 2009

[10] Mobile 4G: The Revolution Is Here Now., http://m2m.sprint.com/media/78386/4g_the_revolution_is_now.pdf
[11] Mahdi Aiash, Glenford Mapp and Aboubaker Lasebae, Raphael Phan, "Providing Security in 4G Systems: Unveiling the Challenges", IEEE 2010
[12] N. Seddigh, B. Nandy, R. Makkar, J.F. Beaumont, "Security Advances and Challenges in 4G Wireless Networks", IEEE 2010
[13] Yu Zheng, Dake He, Weichi Yu and Xiaohu Tang,"Trusted Computing-Based Security Architecture For 4G Mobile Networks", IEEE 2005
[14] Saif Al-alak, Zuriati Ahmed, Azizol Abdullah and Shamala Subramiam "AES and ECC Mixed for ZigBee Wireless Sensor Security", World Academy of Science, Engineering and Technology 2011
[15] Razi Hosseinkhani, H. Haj Seyyed Javadi, "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
[16] 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
[17] Kazys KAZLAUSKAS, Jaunius KAZLAUSKAS, "Key-Dependent S-Box Generation in AES Block Cipher System", INFORMATICA, 2009, Vol. 20, No. 1, 23–34, 2009
[18] Shirbhate D.D. , Kale A.R., "Providing Security Challenges In 4g Systems", Bioinfo Security Informatics Volume 2, Issue 1, 2012
[19] M.B. Vishnu, S.K. Tiong, M. Zaini, S.P. Koh, "Security Enhancement of Digital Motion Image Transmission Using Hybrid AES-DES Algorithm", APCC 2008
[20] M.Kaleem Iqbal, M.Bilal Iqbal, Iftikhar Rasheed, Abdullah Sandhu, "4G Evolution and Multiplexing Techniques with solution to implementation challenges", International Conference on Cyber-Enabled Distributed Computing and Knowledge Discover, 2012
[21] Shabaan Sahmoud, Wisam Elmasry and Shadi Abdulfa, "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
[22] Julia Juremi, Ramlan Mahmod, Salasiah Sulaiman, "A Proposal for Improving AES S-box with Rotation and Key-dependent", Cyber Warfare and Digital Forensic (CyberSec) international conference, 2012
[23] What are 1G, 2G, 3G and 4G networks ?
http://www.speedguide.net/faq_in_q.php?qid=365
Manuel Mogollon, Cryptography and Security Services: Mechanisms and applications, IGI Global, January 31, 2008

