International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868
Foundation of Computer Science FCS, New York, USA
International Conference & workshop on Advanced Computing 2014 (ICWAC 2014) – www.ijais.org

Security Enhancement Algorithms for Data Transmission in 4G Networks

Prerana Choudhari
Information Technology
Thakur College of Engg & Tech
Mumbai, India

Vikas Kaul
Information Technology
Thakur College of Engg & Tech
Mumbai, India

S K Narayankhedkar
3rd author's affiliation
M.G.M College of Engg & Tech
Navi Mumbai, India

ABSTRACT
This paper, presents the design and evaluation of security enhancement for data transmission in 4G networks. An advanced encryption method with AES algorithm is used here. Enhancement is done in AES by modifying the S-box. The static S-box is made dynamic using cipher key. To increase the complexity of the system, AES is used in Round structure. The performance evaluation based on Runtime, Throughput is done and comparison is made between AES and the enhanced system.

Keywords
3G; 4G; AES; S-box; Round structure

1. INTRODUCTION
Many new mobile generations have been developed after the release of first 1G system.. In wireless networks, "G" refers to the generation of the wireless network technology. On the basis of next-generation network (NGN) key architectural changes have been done in telecommunication core and access network. 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 architectural suite, 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.

Wireless 4G LTE network uses 128-bit Advanced Encryption Standard (AES) and SNOW3G algorithms for integrity protection. The 128-bit AES algorithm is the most preferred option in the Wireless 4G LTE network. AES is preferred because it has undergone closed observation than other encryption algorithms [4]. EEA2 or EIA2 is used in LTE-SAE security. They are based on the Advanced Encryption Standard (AES) [7]. The 168-bit Digital Encryption Standard (3-DES) or the newer Advanced Encryption Standard (AES) are used in WiMAX standards because it specifies that, over-the-air transmissions should be encrypted [9]. Many researchers have taken interest in the field of combining 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. The cipher key is used to convert static S-box into dynamic. This is done to make AES cryptographically strong.

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

1.1 Background
Cryptography is the art and science of keeping messages secure. The required basic definitions and concepts [23] in Cryptography are reviewed here.

- Plaintext: An original message is called Plaintext or cleartext.
- Encryption: Process of modifying a message to hide its substance.
- Ciphertext: An encrypted message is Ciphertext.
- Decryption: Process of turning Ciphertext back into Plaintext is called Decryption.
- Cryptanalysis: Cryptanalysis is the science of recovering the plaintext of a message without access to the key.

1.2 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 following four steps:

1) Substitute bytes,

2) Shift rows,

3) Mix columns, and

4) Add round key.

1.3 AES S-box

The Rijndael S-box is a matrix i.e. 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).

2. LITERATURE SURVEY

In 2006, the paper[1], shown the comparison between 3G and 4G on the basis of network structure, core network mobile terminal and the core technology. This paper also discussed some core techniques like security strategy of 4G, hybrid network in 4G, adaptive 4G network. In September 2008,in the paper [15] S-box is made key dependent without changing its value and without changing the inverse S-box. The algorithm ensures that no trapdoor was present in the cipher and expands the keyspace to slow down attacks. 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 analyzed the security-related standards, architecture and design for the LTE and WiMAX technologies. They explained security standards evolution across different generations of wireless standards. They concluded that there is a strong need for continued study on 4G security issues and development. The paper [12] proposed trusted computing based security architecture for 4G networks, in 2005. The proposed framework is the combination of password and biometric identification (BI) as well as public key-based identification. An efficient hybrid authentication and key agreement scheme is presented in the paper to resist the possible attacks, particularly the attacks on/from Mobile Equipment. 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. The paper[8]focused on the potential security issues that can occur in the deployment of the Long-Term Evolution/System Architecture Evolution protocol (LTE/SAE) in emerging 4G wireless technologies in this paper, in March/April 2013. The paper explains LTE/SAE 4G Network Security Architecture and also summarizes the LTE/SAE 3G Cryptographic Algorithms like KASUMI, SNOW-3G, Milenage and ZUC. 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. The cryptanalysis with algebraic attack is the future work of their paper.

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

3. 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. 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 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 project. 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 and number of rounds in the Round structure.

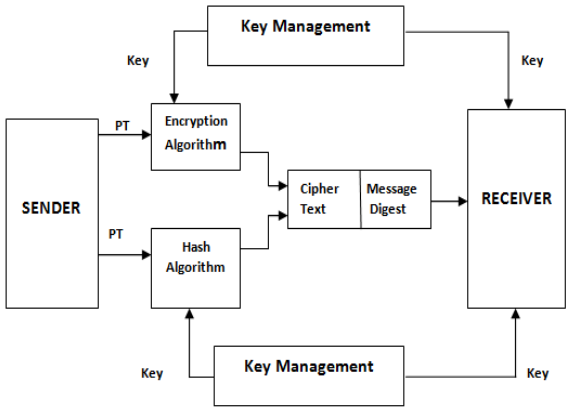

Fig 1: Proposed system

3.1 Model development

The flow of model development is as follows:

1. 128 bits key length is used for the enhanced AES algorithm.
2. The proposed system's encryption and decryption is the same as traditional AES algorithm.
3. The round function of encryption process is also similar as the traditional AES algorithm.
4. There is additional phase of making S-box dynamic as shown in Fig. 2.
5. Before sub byte stage, the static S-box is converted into dynamic using cipher key.
6. The round structure of AES is used as shown in Fig. 3
7. Dynamic S-box is applied in the round structure of AES as shown in Fig. 4 we take 256 bit data as Input to the system.
8. Here the Input Data is split into two blocks of 128 bits each.
9. One Block is given as Input to the AES section of the System.
10. The other Block is given as Input to the AES section of the System in the next round as per the round structure.
11. This is done for 1, 2, 5 and 10 rounds respectively.
12. These outputs are then combined together to form 256 bit block of encrypted data.

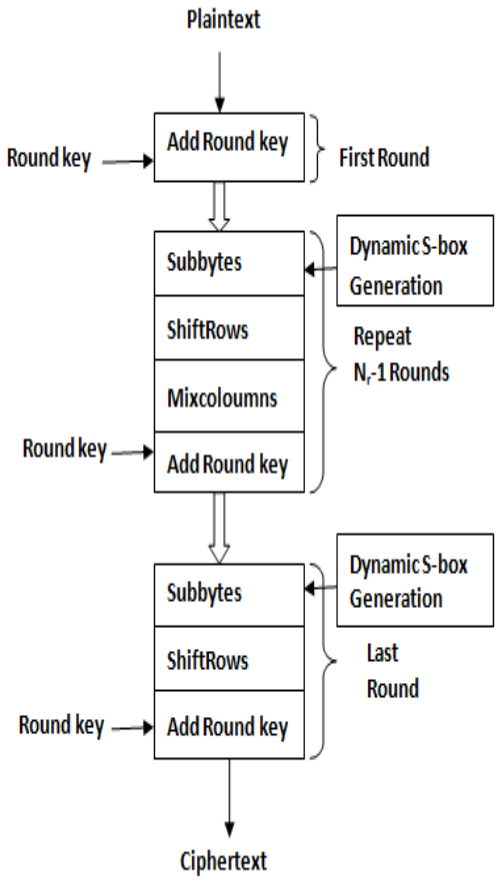

Fig 2: AES dynamic S-box

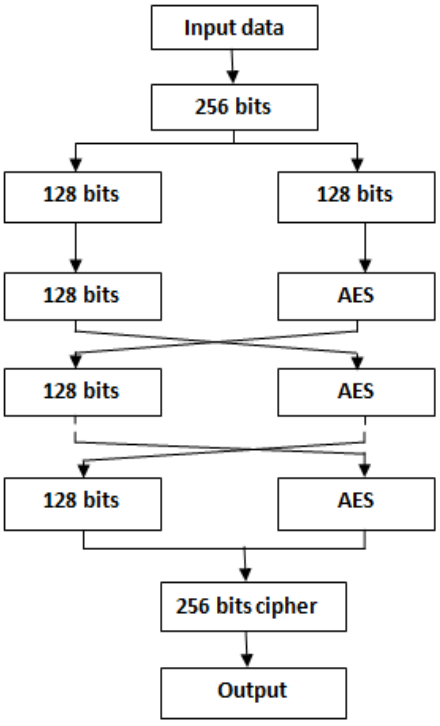

Fig 3: Round AES

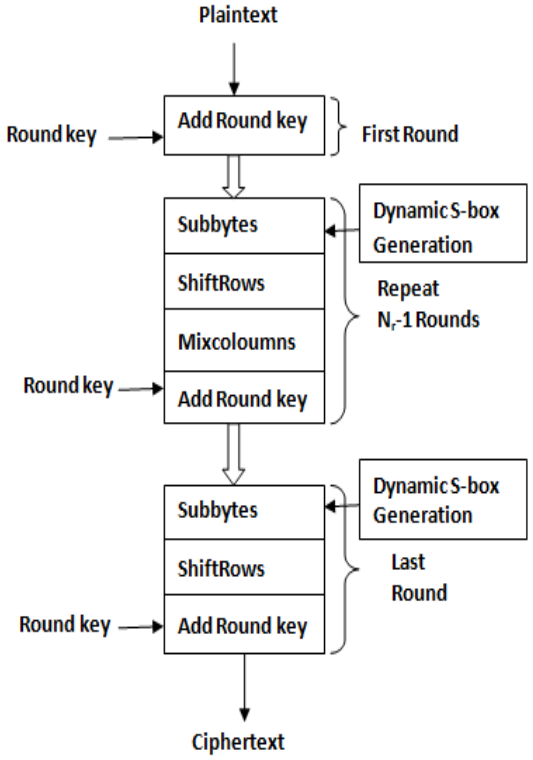

Fig 4: Round AES with Dynamic S-box

4. EXPERIMENTAL RESULTS

The results carried out till the date is based on encryption time and throughput.

4.1 Encryption time on input text file, image file and audio file

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

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

The results are tabulated as shown below.

Table 1. Based on encryption time on text file

Algorithm	Bits in one block	Total no of Blocks	Encryption Time in sec	Decryption Time in sec
AES	128	6	0.044931	0.054853
AES with dynamic S-box	128	6	0.046448	0.055075

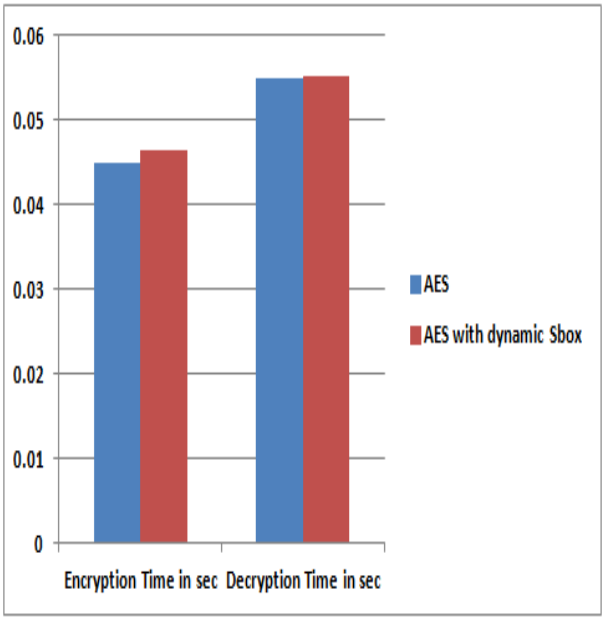

Fig 5: Graphical representation of results based on encryption time on input text file

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

Table 2.based on encryption time on image file

Algorithm	Bits in one block	Total no of Blocks	Encryption Time in sec	Decryption Time in sec
AES	128	151	1.083785	1.306551
AES with dynamic S-box	128	151	1.119398	1.377046

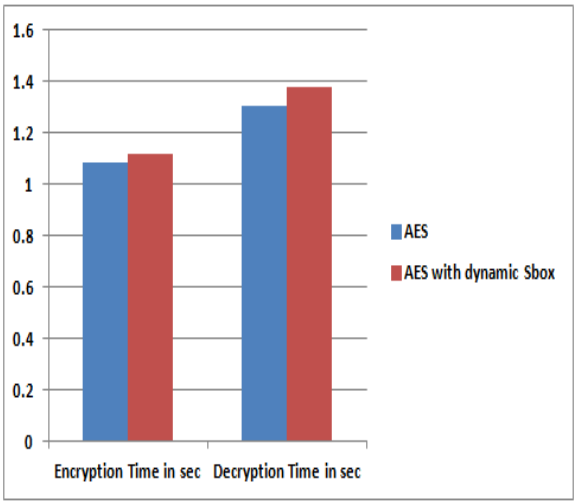

Fig 6: Graphical representation of results based on encryption time on image file

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

Table 3. Based on encryption time on audio file

Algorithm	Bits in one block	Total no of Blocks	Encryption Time in sec	Decryption Time in sec
AES	128	227	1.725907	2.158051
AES with dynamic S-box	128	227	1.765681	2.179346

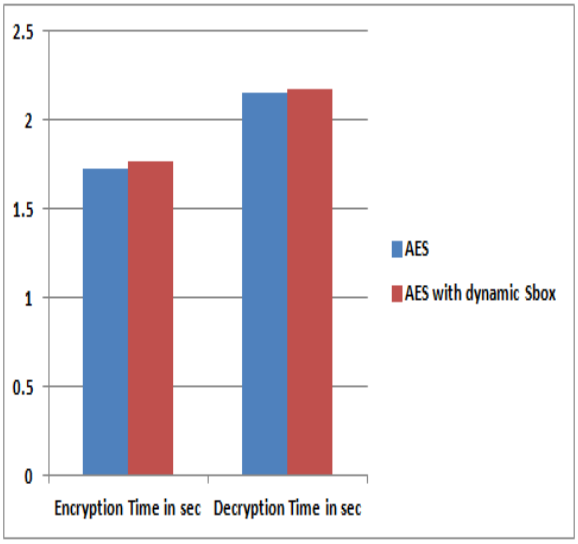

Fig 7: Graphical representation of results based on encryption time on audio file

4.2 Throughput on input text file, image file and audio file.

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.

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

Table 4. Based on throughput on input text file

Algorithm	Bits in one block	Total no of Blocks	Throughput (kb/sec)	
			Encryption	Decryption
AES	128	6	14.5646	11.9614
AES with dynamic S-box	128	6	14.1288	11.9154

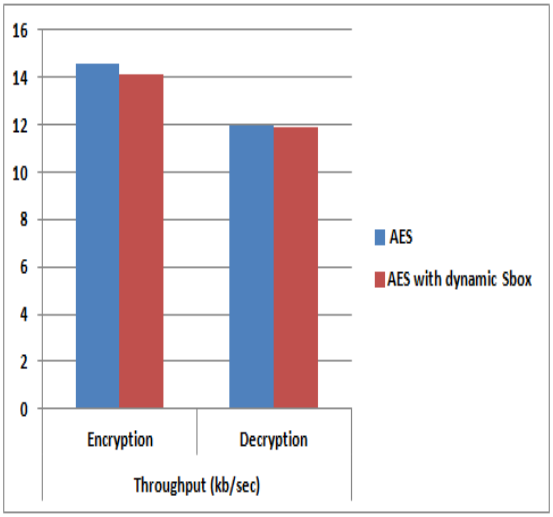

Fig 8: Graphical representation of results based on encryption timeThroughput on input text file

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

Table 5. Based on throughput on image file

Algorithm	Bits in one block	Total no of Blocks	Throughput (kb/sec)	
			Encryption	Decryption
AES	128	151	17.8348	14.9136
AES with dynamic S-box	128	151	17.2666	14.0358

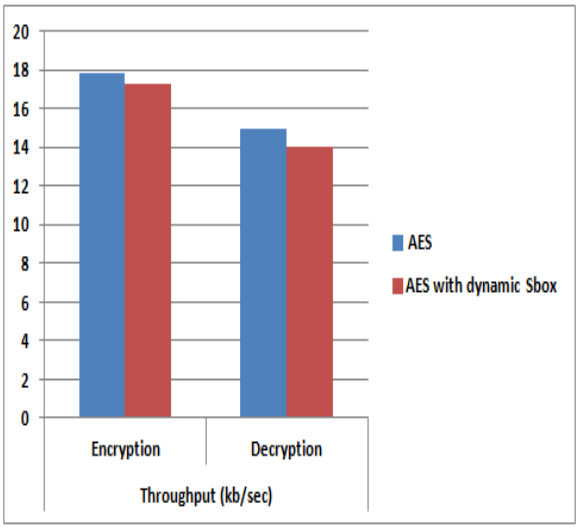

Fig 9: Graphical representation of results based on encryption timeThroughput on image file

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

Table 6. Based on throughput on audio file

Algorithm	Bits in one block	Total no of Blocks	Throughput (kb/sec)	
			Encryption	Decryption
AES	128	227	16.8274	13.4578
AES with dynamic S-box	128	227	16.458	13.32756

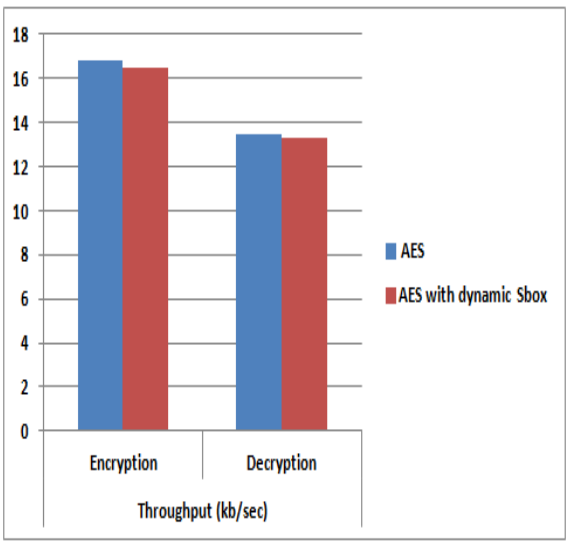

Fig 10: Graphical representation of results based on encryption timeThroughput on input audio file

5. 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 enhance AES static S-box is converted into dynamic using cipher key. 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. For the applications requiring less time the number of rounds in the system can be less. 3G and 4G requires high data transmission rate in order to send image and the proposed algorithm encrypts the data in acceptable time.

We also hope to increase the complexity of system, by using an AES Round structure. The motivation behind increasing complexity is to make the system attack resistant and secure data from attackers. This is the future scope of the work.

6. 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, http://business.verizonwireless.com/content/dam/b2b/resources/LTE_FutureMobileTech_WP.pdf

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

[6] 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

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

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

[9] Mobile 4G: The Revolution Is Here Now., http://m2m.sprint.com/media/78386/4g_the_revolution_is_now.pdf

[10] Mahdi Aiash, Glenford Mapp and Aboubaker Lasebae, Raphael Phan, "Providing Security in 4G Systems: Unveiling the Challenges", IEEE 2010

[11] N. Seddigh, B. Nandy, R. Makkar, J.F. Beaumont, "Security Advances and Challenges in 4G Wireless Networks", IEEE 2010

[12] Yu Zheng, Dake He, Weichi Yu and Xiaohu Tang,"Trusted Computing-Based Security Architecture For 4G Mobile Networks", IEEE 2005

[13] 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

[14] 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

[15] 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

[16] Kazys KAZLAUSKAS, Jaunius KAZLAUSKAS, "Key-Dependent S-Box Generation in AES Block Cipher System", INFORMATICA, 2009, Vol. 20, No. 1, 23–34, 2009

[17] Shirbhate D.D. , Kale A.R., "Providing Security Challenges In 4g Systems", Bioinfo Security Informatics Volume 2, Issue 1, 2012

[18] 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

[19] 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

[20] 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

[21] 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

[22] What are 1G, 2G, 3G and 4G networks ?

[23] http://www.speedguide.net/faq_in_q.php?qid=365

[24] Manuel Mogollon, Cryptography and Security Services: Mechanisms and applications, IGI Global, January 31, 2008