International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 01 | Jan -2017 www.irjet.net p-ISSN: 2395-0072

Security Enhancement in Next Generation Networks using Enhanced AES with RC4 and Dynamic S-box

Ripal Patel[1], Vikas kaul[2], Dr S K Narayankhedkar[3]

[1] *PG Student*
Information Technology, Thakur College of Engineering and Technology

[2] *Assistant Professor*
Information Technology, Thakur College of Engineering and Technology

[3] *Professor, MGMCOET, Navi Mumbai*

Abstract - Encryption is primary method of protecting valuable electronic information transmitted over the networks. SSL/TLS can help to secure transmitted data using various encryption algorithms. AES is one of ciphering algorithm which is used for encryption, decryption of data to provide confidentiality for end-to-end data transmission. To provide end-to–end security TLS/SSL (Transport layer security) is used.

This paper presents an enhancement of AES algorithm by converting static S-box into dynamic using RC4 and key scheduling thus making the system resistant to linear and differential cryptanalysis by preventing repetition of cipher key.

To increase the complexity of system AES is to be used in round structure. In round structure, AES S-box changes in every round.

Comparison of the traditional and enhanced AES will be made on the basis of encryption Time, decryption time, CPU usage and throughput. Here focus is to achieve speed compatible with next generation LTE network.

Key Words: LTE; AES; S-box; Round structure; RC4

1. INTRODUCTION

The mobile communication systems and the wireless communication technologies have been improving very fast day by day. During last few decades, mobile communication has been developed very rapidly. The first generation (1G) wireless mobile communication network which started at early 1980 was analog system which was used for public voice service. The second generation (2G) was launched early 1990s it was based on digital technology and network infrastructure. As compared to the first generation, the second generation supports text messaging. 2.5G networks appeared in year 1999-2000 and brought the internet into personal communication. 3G was introduced in year 2000. It provides higher data rate and broader bandwidth and also provides applications in wireless voice telephony, mobile, internet access, fixed wireless internet access, video calls and mobile TV.

After the release of previous generations of wireless networks 4G network is considered for security enhancement and reliable communication. The 4G wireless networks operates entirely on the TCP/IP, so it becomes completely IP based. It provides facility to transfer large amount of data at higher speed from anywhere and anytime. As large amount of data is transmitted, security of these data is needed over the networks.

1.1 Advanced Encryption Standard

AES is also called as Rijndael .It is developed by Joan Daemen and Vincent Rijmen. It is a symmetric-key algorithm. AES is a block cipher with a block length of 128 bits. It allows for three different key lengths: 128, 192, or 256 bits. Encryption consists of 10 rounds of processing for 128-bit keys, 12 rounds for 192- bit keys, and 14 rounds for 256-bit keys except for the last round in each case, all other rounds are identical. For encryption, each round consists four steps: Substitution bytes, Shift row, Mix column and Add round key. For decryption, each round consists of the four steps: Inverse shift rows, Inverse substitute bytes, Inverse mix columns and Add round key.

1.1 AES S-box

The Rijndael S-box (substitution box) is a matrix (square array of numbers) used in the Advanced Encryption Standard (AES) cryptographic algorithm. It

serves as a lookup table. Substitution is a nonlinear transformation which performs confusion of bits. S-box is represented as a 16x16 array, rows and columns indexed by hexadecimal bits. The S-box is generated by determining the multiplicative inverse for a given number in GF (28).

1.2 RC4

RC4 is designed by Rivest for RSA Data Security. It is a variable Key–size stream cipher with byte-oriented operations. The algorithm is used for random permutation.
RC4 is used for file encryption and also used for secure communications, as in encryption of traffic to and from secure website using the SSL/TLS protocol.

2. LITERATURE REVIEW

The whole literature review is focused on the following literary works being done by an array of scholars and researchers from the field of network and data security. The following papers are selected for review keeping in mind the traditional and conventional approaches of ciphering algorithms.
Q. Cheng, C.Chuanhui and W. Li (2006) discussed some core technology of 4G mobile system and showed the comparison between 3G and 4G on the basis of network structure, core network mobile terminal and core technology. The paper (2013) explains LTE/SAE security algorithm and procedure and also summarise the LTE/SAE 3G cryptography algorithms like KASUMI, SNOW-3G, Milenge and ZUC. Razi Hosseinkhani and H. Haj Seyyed Javadi (2012) introduced new algorithm to generate dynamic S-box from original S-box using cipher key. In year 2012, Julia Juremi, Ramlan Mahmod, Salasiah Sulaiman made AES S-box key dependent using S-box rotation property to make AES stronger. Here, only the S-box is made key-dependent without changing the value. Krishnamurthy G N and V Ramaswamy (2008) improved the security of AES by making S-box 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 keys space to slow down attacks. S Shivkumar, Dr.G.Umamaheswai (2011) used RC4 stream cipher and key expansion procedure to generate S-boxes and S-box is rotated for each round based on the value calculated from the round key. In the paper (2012), Mona Dara and Kooroush Manochehri generated key dependent flexible S-box. The Dynamic S-box is generated using RC4 and key scheduling algorithm. In the paper (2013) Vikas kaul, Prerna choudhari and S.K Narayankhedkar improved AES by converting static S-box into dynamic using cipher key. AES is used in round Structure to increase complexity of system. Comparisons was made between AES and enhanced system basis on performance evaluation based on runtime and throughput.

3. PROPOSED SYSTEM

To enhance the secure data transmission in next generation network and make system resistant to attacks, AES cipher algorithm is used in proposed system. The work focuses on enhancement of encryption algorithm. Encryption of transmitted data. To improve strength of cryptography system AES is enhanced by making static S-box into dynamic using RC4 and AES key scheduling. Round structure will be used to increase complexity of system. RSA and SHA-256 is used for key exchange and message authentication respectively.
1. End-to-End security is provided in SSL/TLS using AES for next generation networks.
2. Integrity of data can be provided using SHA-256 algorithm.
3. RSA is to be used for key exchange mechanism.
4. AES is further enhanced using making static S-box dynamic using RC4 and AES key scheduling algorithm to make more secure S-box by preventing repetition of cipher key.
5. System can be made more complex by using AES round structure**.**
6. Performance evaluation of system is to be done by measuring encryption and decryption time and throughput.

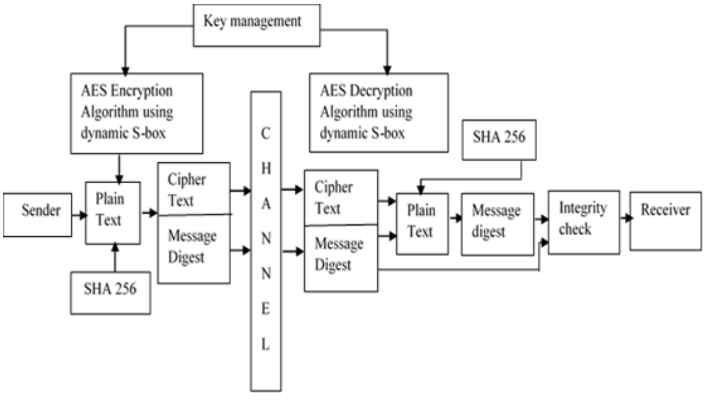

Fig -1**: Proposed System**

4. DESIGN METHODOLOGY

1. Input data and key length for enhanced AES is taken 256 bits.

2. Encryption and decryption of proposed system is same as original AES algorithm.
3. In proposed system S-box is made dynamic by using RC4 and key expansion procedure.

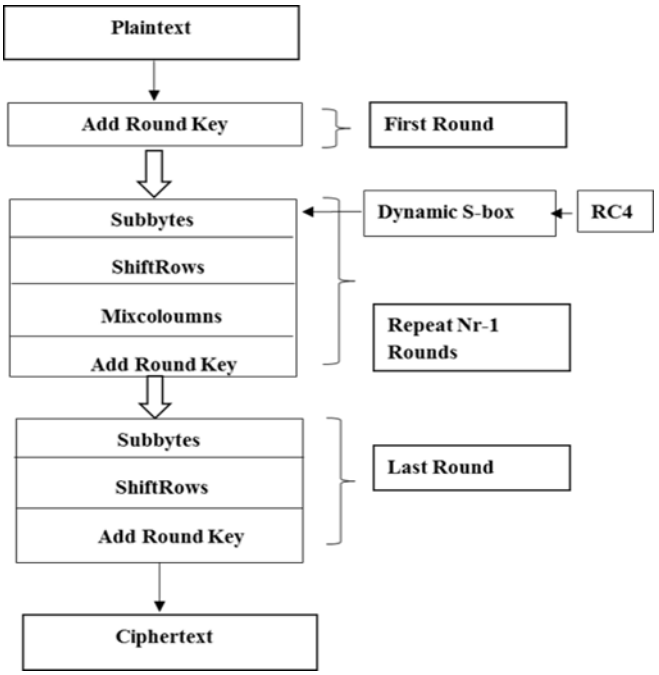

Fig -2: **AES Dynamic S-box**

4. The key Expansion transformation takes key and generates expanded key and output of the key pseudo expansion algorithm i.e. expanded key is used to generate S-box by RC4 key Schedule algorithm to prevent the repetitions.
5. RC4 cipher generate different 256 values each time depending upon input key.
6. Static S-box is converted into dynamic before sub byte transformation stage using RC4 cipher and key expansion .Inverse S-box also modified accordingly.
7. For round structure 256 bits input data is divided into two blocks of 128 bits.
8. First block is given as input to AES section of the system and second block is given as input to AES section of system in the next round as per round structure.
9. Process is continued until all the fixed number of round for AES are completed.
10. 256 bits block of encrypted data is constructed by combining these output all together.

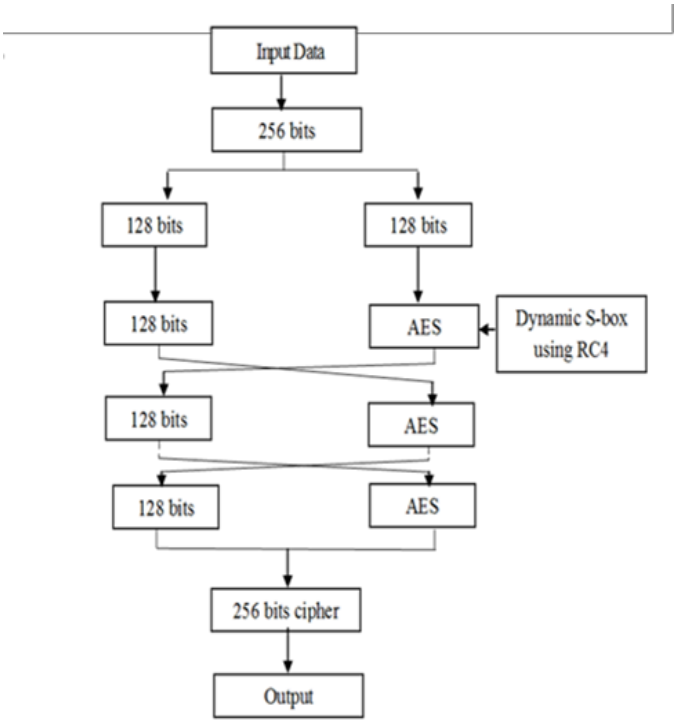

Fig -3: **AES in Round structure**

4. EXPERIMENTAL RESULTS

File: "plaintext.txt", Size: 144 bytes (1552 bits), Key: 12345678901234561234567890123456

Table -1: Comparative analysis is done based throughput using text file as input on 1) Microsoft Windows 10, Pentium, 32 bit, 4 GB RAM and 2) Microsoft windows 8 , Intel i3 ,64-bit,6 GB RAM

Sr. No	Algorithm	Block size	No. of Blocks	Encryption Time(Sec)		Decryption Time(Sec)	
				Pentium	i3	Pentium	i3
1	AES	128	12	0.067	0.028	0.082	0.033
2	Enhanced AES	128	12	0.0679	0.029	0.083	0.035
3	Round Structure (1R)	256	6	0.037	0.016	0.0455	0.017
4	Round structure with Enhanced AES(1R)	256	6	0.041	0.017	0.0481	0.019
5	Round structure with Enhanced AES(5R)	256	6	0.16142	0.066	0.19174	0.079
6	Round structure with Enhanced AES(5R)	256	6	0.16216	0.075	0.20169	0.087

7	Round Structure (10R)	256	6	0.314	0.137	0.3916	0.166
8	Round structure with Enhanced AES (10R)	256	6	0.330	0.134	0.3955	0.165

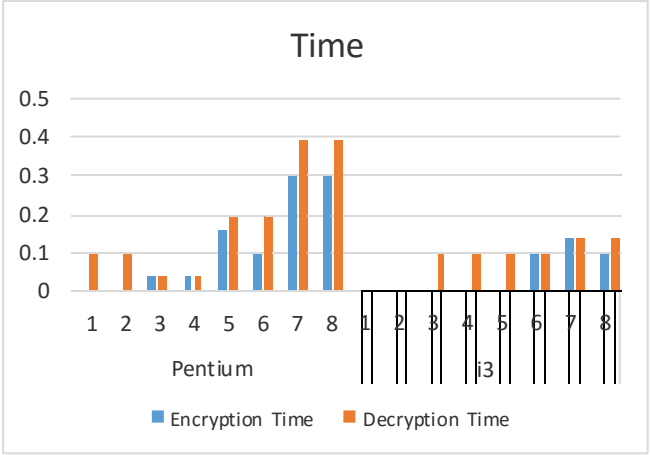

Fig -4: **Graphical representation of runtime of AES algorithm for text file**

Table -2: Comparative analysis is done based throughput using text file as input on 1) Microsoft Windows 10, Pentium, 32 bit, 4 GB RAM and 2) Microsoft windows 8 , Intel i3 ,64-bit,6 GB RAM

Sr. No	Algorithm	Block size	No. of Blocks	Throughput (kbps) Encryption Time		Throughput (kbps) Decryption Time	
				Pentium	i3	Pentium	i3
1	AES	128	12	22.94	53.75	18.77	45.78
2	Enhanced AES	128	12	22.82	52.59	18.62	43.84
3	Round Structure (1R)	256	6	41.240	92.93	34.079	114.0
4	Round structure with Enhanced AES (1R)	256	6	37.653	90.10	32.225	115.3
5	Round structure with Enhanced AES (5R)	256	6	9.6146	23.51	8.0942	19.60
6	Round structure with Enhanced AES (5R)	256	6	9.5707	20.59	7.69497	17.66
7	Round Structure (10R)	256	6	4.94	11.27	3.96	9.338
8	Round structure with Enhanced AES (10R)	256	6	4.69	11.57	3.92	9.371

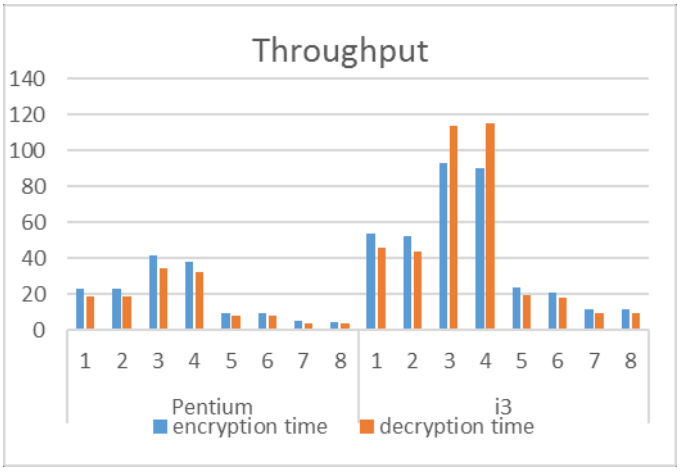

Fig -5: **Graphical representation of throughput of AES algorithm for text file**

File: "smily.jpg", Size: 2.35 KB (19328 bits), Key: 12345678901234561234567890123456

Table -3: Comparative analysis is done based throughput using text file as input on 1) Microsoft Windows 10, Pentium, 32 bit, 4 GB RAM and 2) Microsoft windows 8 , Intel i3 ,64-bit,6 GB RAM

Sr. No	Algorithm	Block size	No. of Blocks	Encryption Time (Sec)		Decryption Time (Sec)	
				Pentium	i3	Pentium	i3
1	AES	128	151	0.66	0.27	0.80	0.32
2	Enhanced AES	128	151	0.66	0.28	0.81	0.34
3	Round Structure (1R)	256	76	0.33	0.13	0.41	0.16
4	Round structure with Enhanced AES (1R)	256	76	0.34	0.14	0.42	0.18
5	Round structure with Enhanced AES (5R)	256	76	1.65	0.67	1.95	0.83
6	Round structure with Enhanced AES (5R)	256	76	1.67	0.70	2.10	0.914
7	Round Structure (10R)	256	76	3.22	1.37	3.96	1.753
8	Round structure with Enhanced AES (10R)	256	76	3.38	1.46	4.08	1.853

[5] Razi Hosseinkhani and H. Haj Seyyed Javadi, "Using Cipher Key to Generate Dynamic S-Box in AES Cipher System," International Journal of Computer Science and Security (IJCSS), vol. 6, no.1, pp.19-21, 2012.

[6] J. Juremi, R. Mahmod, S. Sulaiman, "A Proposal for Improving AES S-box with Rotation and Key-dependent," Cyber Warfare and Digital Forensic (CyberSec) international conference, 2012.

[7] Kazys KAZLAUSKAS, Jaunius KAZLAUSKAS, "Key-Dependent S-Box Generation in AES Block Cipher System," INFORMATICA, vol. 20, no. 1, pp. 23–34, 2009.

[8] 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, pp. 388-398, Sept 2008.

[9] I.Abd-ElGhafar, A. Rohiem, A. Diaa, and F.Mohammed, " Generation of AES dependent S-boxes using RC4 algorithm," 13th International Conference on Aerospace Sciences & Aviation Technology (ASAT-13), Military Technical College, Cairo, Egypt, May 26-28, 2009.

[10] Mahmoud, E.M., El Hafez, A.B., Elgarf, T.A., Zekry, A," Dynamic AES-128 with key-dependent S-box, International Journal of Engineering Research and Applications, vol. 3, Issue 1, pp.1662-1670, Jan -Feb 2013.

[11]S.Shivkumar, and G.Umamaheswari, "Performance comparison of Advanced Ecryption Standard (AES) and AES key dependent S-box simulation using matlab,"International Conference on Process Automation, Control and Computing (PACC), 2011, pp. 1–6.

[12] M. Dara, K. Manochehri, "Using RC4 and AES schedule to generate Dynamic S-box in AES," Information Security Journal: A Global Perspective, vol. 23, pp.1-9, 2014.

[13] V. Kaul, P. Choudhari, S K Narayankhedkar, "Security Enhancement for Data Transmission In 4G Networks," IEEE The Next Generation Information Technology Summit (Confluence), Sept 2014, pp. 373-378.

[14]B.Forouzan,D.Mukhopadhyay ,"Cryptography and Network Security," 2nd edition, Pearson Education , 2010.