Scientific Journal of Impact Factor (SJIF): 3.134

E-ISSN (O): 2348-4470
P-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 2, Issue 12, December -2015

To Improve Security and Performance in the NGN

Binal Shah[1], Zahir Aalam[2]

[1]Information Technology, Thakur College of Engineering and Technology
[1]Information Technology, Thakur College of Engineering and Technology

Abstract —*The common thought about Next Generation Network (NGN) is that one system transports all data and services like information, voice and video by enclosing these into packets on the Internet. Transport Layer Security (TLS) protocol provides a secure transmission between communicating applications and their users on the internet. It gives security with some encryption method such as Advanced Encryption Standard (AES). This paper presents a security and performance for data transmission in 3G/4G networks using TLS. Here AES 128 bit is used for encryption because of its high efficiency and ease. AES is modified by using permutation instead of the mix column to overcome the problem of high calculation and computational overhead. The system is further enhanced by parallel AES to improve the speed of the algorithm. In parallel computing, functions of AES are divided into two independent parts. Comparison is made between traditional AES and enhanced system on the basis of performance. Evaluation is based on Encryption Time, Decryption Time and Throughput.*

Keywords – *NGN, AES, Permutation, Parallel Computing.*

I. INTRODUCTION

The word "MAGIC" refers to 4G wireless technology, which stands for Mobile multimedia, anywhere, Global mobility solutions over, integrated wireless and Customized services [1]. Keeping in mind the end goal to enhance versatile communication services and additionally security, LTE (Long Term Evolution) technology developed to overcome numerous difficulties that remain behind the past system technology. This new technology has game changers that make it one of the freshest and most cutting edge advancements in versatile Network innovation. LTE technology, which has been developed to offer more speed and capacity over the mobile network to serve a tremendous development in mobile data and the quantity of clients. Due to the fast development of advanced communication and electronic information trade, information assurance has turned into a crucial subject in the business, business, and government. Data security is the process of protecting data. It protects its availability, privacy and integrity. Access to stored data on computer databases has increased greatly [2]. Cryptography provides essential techniques for securing information and protecting data.

LTE like its predecessors is threatened by different kinds of attacks such as imposters, eavesdroppers, viruses and other attackers. Searching on providing high security is continuous. Two standardized algorithms are provided to ensure data integrity and confidentiality protection via air interface named as EEA (EPS Encryption Algorithm) and EIA (EPS Integrity Algorithm). These two algorithms have been developed for LTE technology. The first set appeared is 128-EEA1/128-EIA1 which is based on SNOW 3G algorithm, the second is 128-EEA2/128-EIA2 which is based on AES algorithm and the third is 128EEA3/128-EIA3 which is based on ZUC algorithm [3]. This paper describes the AES Algorithm based on different evolution parameters.

II. AES ALGORITHM

AES is one of the encryption techniques which is used most frequently because of its high efficiency and simplicity. It is the highly secure algorithm. AES is the Advanced Encryption Standard, a United States government standard algorithm for encrypting and decrypting data. The AES algorithm defined by the National Institute of Standards and Technology (NIST) of the United States has been widely adopted to replace DES as the new symmetric encryption algorithm [4]. The standard comprises three block ciphers: AES-128, AES-192 and AES-256. Each AES cipher has a 128-bit block size, with key sizes of 128, 192 and 256 bits, respectively. The AES ciphers have been considered extensively and are today used worldwide, as was the case with their predecessor, the Data Encryption Standard (DES).

The AES algorithm with the 128-bit key is explained here. There are 4 different stages, one is permutation and other three are substituted as shown in Fig. 1.
For encryption, each round consists of the following four steps:

- *Substitute bytes*
- *Shift rows*
- *Mix columns*
- *Add round key.*

The last step consists of XORing the output of the previous three steps with four words from the key schedule.
For decryption, each round consists of the following four steps:

- *Inverse shifts rows*
- *Inverse substitute bytes*
- *Add round key*
- *Inverse mix columns*

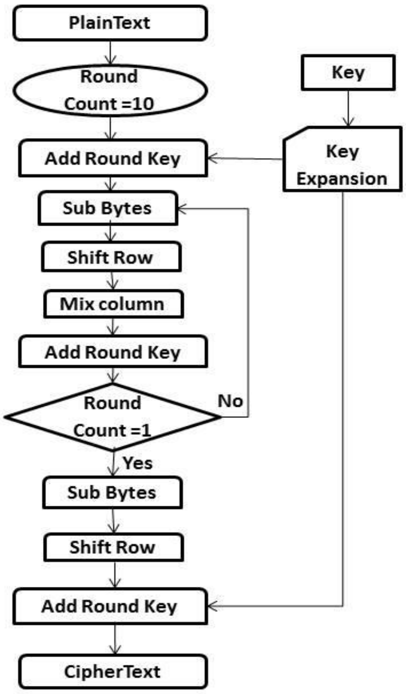

Figure 1.Flowchart of AES algorithm

III. LITERATURE SURVEY

This paper focuses on reviewing the three sets of the LTE cryptographic algorithms and their core algorithms and then comparing them based on different factors in order to understand their cons and pros and provide valuable information about LTE security [3]. The paper [6] present a view of security issues and vulnerability of the 4G wireless network. They analyzed the security-related standards, architecture and conception for the LTE and WiMAX technologies. The paper presented a hybrid AKA (authentication and key agreement) and mandate plan, in which secret word is in mix with finger impression and in addition, a public key to accomplish mutual authentication or Universal Subscriber Identity Module and that among the user or accessed network or home environment [7]. This paper gives a new architecture called Integrated Inter System Architecture (IISA), which is grounded in the Third-Generation Partnership Project [8]. The paper [9] focused on the potential security issues that can occur with the arrangement of the Long-Term Evolution/System Architecture Evolution protocol (LTE/SAE) in 4G. This paper made S-box key dependent without changing its value and without changing the inverse S-box. The algorithm guarantees that no trapdoor was present in the cipher and expands the fundamental space to slow down attacks [10]. The paper present lightweight encryption. To overcome the problem of high calculation and computational overhead, they examine the AES and alter it, to decrease the figuring of algorithm and for improving the encryption performance. To modify AES, they skip the Mix column step and Add the Permutation [11]. In this paper [12] explain the two instructions, swperm and sieve, that can be connected to effectively finish an arbitrary a bit- level permutation of a n-bit word with or without repeats. The paper present the implementation of Advance encryption (AES) algorithm using parallel computing. Flexibility & performance improvement provide in terms of speedup [13]. This paper is about the technologies of parallel computing and its optimized design for encryption. Then, they offered a novel algorithm for AES parallel encryption, and planned and implemented a fast data encryption scheme [5].

IV. RESEARCH GAP

From the above extensive literature review, it was found that in Next Generation Network need a high performance and security to perform multiple operations of data transmission. For the data transmission, there is need of cryptography algorithms those are secure and perform faster than the other algorithms for encryption/decryption process. In 3G/4G, there are lots of algorithms to perform a task for encryption and decryption like SNOW 3G, ZUC, KASUMI and Milenage. But these algorithms have some disadvantages.

V. PROPOSED SYSTEM

There are major drawbacks in other 3G/4G cipher algorithms; hence the AES cipher algorithm is used in the proposed system because it is the most secure algorithm. Figure 2 displays the proposed system for data transmission in the NGN. This work focuses on enhancement of encryption algorithm to improve performance for end to end data transmission. In this, AES algorithm is modified using permutation. Permutation is used in the place of Mix column. The further AES is enhanced using concept of parallel computing. The performance evaluation is done based on parameters: Throughput, Encryption and Decryption Time.

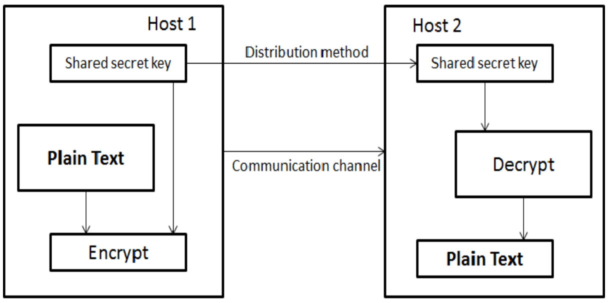

Figure 2.Proposed System

VI. MODEL DEVELOPMENT

- 128 bits key length used for the enhanced AES Algorithm. Though key is more than 128 i.e. 192 or 256, first 128 bits key will be used.
- The proposed system’s encryption and decryption are the same as the traditional AES algorithm.
- The modified AES algorithm is as shown in Figure 3.
- In the Modified AES algorithm, Mix column is replaced by Permutation.
- The modification is done by totaling the Initial Permutation step, takes from DES.
- The Modified-AES algorithm takes 128 bits as input. The functions Substitution Bytes and ShiftRows are also interpreted as 128 bits and the Permutation function also takes 128 bits.
- In the permutation table each entry indicates a specific position of a numbered input bit may also consist of 128 bits in the output.
- A parallel AES as shown in Figure 4.
- According to the proposed parallel AES algorithm, firstly store the plaintext and expanded key in the global memory space.
- The Input Data is split into blocks of 16 bytes.
- The plaintext is then split into blocks which are encrypted completely in parallel.
- At the last output of the blocks are combined as shown in Figure 4.
- Same as plaintext, ciphertext is split into the blocks which are decrypted completely in parallel.
- And at the end output blocks are combined and give the final plaintext.

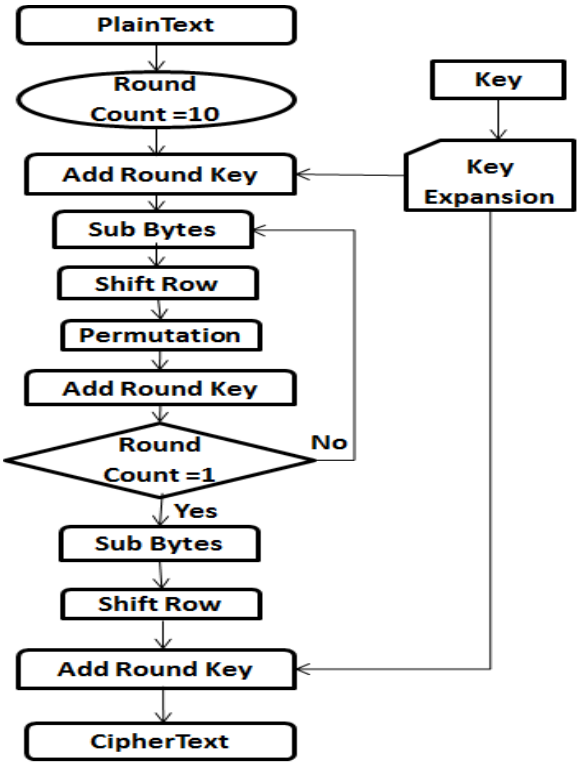

Figure 3.Flowchart of modified AES

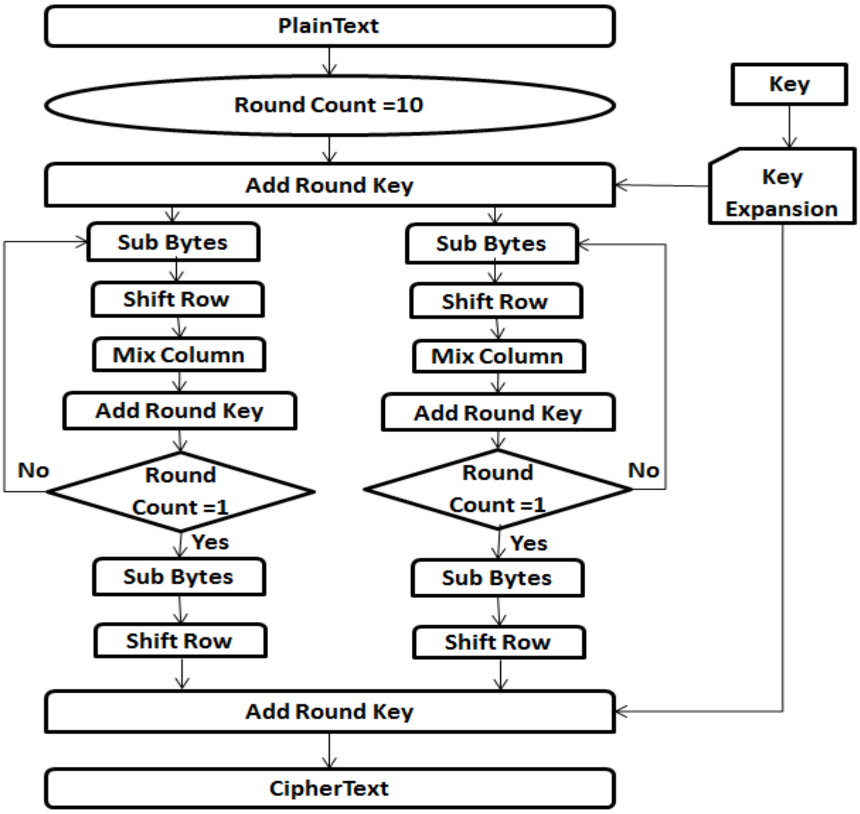

Figure 4.Parallel Standard AES

VII. EXPERIMENTAL RESULTS

The result carried out is based on Encryption and Decryption time and Throughput. Computer Configurations used are Microsoft Windows 8.1, Intel (R) Core (TM) i5-4210U CPU @ 1.70 GHz, 2.40GHz with 8 GB RAM.

The Software used to generate these results is Microsoft visual studio 2010.
The results are tabulated as shown below**.**

5.1 Encryption Time and Decryption Time

Encryption Time: Encryption is the conversion of electronic data into another form, called ciphertext, which cannot be easily understood by anyone except authorized parties. It may also be performed with a set of keys or passwords. The time taken to encrypt any file is called Encryption Time. Here, Encryption Time is measured in milliseconds (ms).

Decryption Time: Decryption is the process of transforming data that have been rendered unreadable through encryption back to its unencrypted form. During decryption, the system extracts and converts the cipher data and transforms it to texts and images that are easily understandable not only by the reader but also by the system. It may also be performed with a set of keys or passwords. The time taken to decrypt any file is called Decryption Time. Here, Encryption Time is measured in milliseconds (ms).

5.1.1 Encryption and Decryption Time for TEXT File:

Table 1 gives the basic information of the Text file (such as file size, no. of bits and total no. of blocks) which is going to be used for the encryption and decryption.

Table 1 Basic information about TEXT file

File Size	18.6 KB
Total number of bits	152371 bits
Number of bits in one block	128 bits
Total number of blocks	1191

Table 2 provides the encryption time and decryption time of Text file taken by AES algorithm and modified AES algorithm.

Table 2 Encryption Time and Decryption Time of TEXT file

Algorithm	**Encryption Time(ms)**	**Decryption Time(ms)**
AES	26	53
Modified AES	11	9

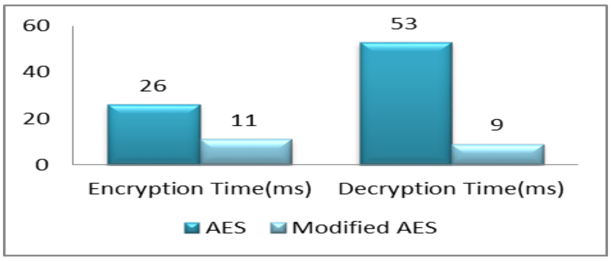

Figure.5 Graphical representation of Encryption Time and Decryption Time of TEXT file

Figure.5 explain the comparison of encryption time and decryption time of Text file taken by AES algorithm and modified AES algorithm. It shows that the Modified AES takes less time to encrypt and decrypt the file than the Standard AES.

5.1.2 Encryption and Decryption Time for IMAGE File:

Table 3 gives the basic information of the image file (such as file size, no. of bits and total no. of blocks) which is going to be used for the encryption and decryption.

Table 3 Basic information about IMAGE file

File Size	39.7 KB
Total number of bits	325222 bits
Number of bits in one block	128 bits
Total number of blocks	2541

Table 4 provides the encryption time and decryption time of image file taken by AES algorithm and modified AES algorithm.

Table 4 Encryption Time and Decryption Time of IMAGE file

Algorithm	**Encryption Time(ms)**	**Decryption Time(ms)**
AES	69	113
Modified AES	20	18

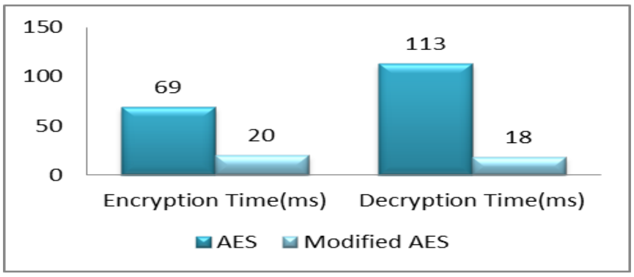

Figure.6 Graphical representation of Encryption Time and Decryption Time of IMAGE file

Figure.6 explain the comparison of encryption time and decryption time of Image file taken by AES algorithm and modified AES algorithm. It shows that the Modified AES takes less time to encrypt and decrypt the file than the Standard AES.

5.1.3 Encryption and Decryption Time for AUDIO File:

Table 5 gives the basic information of the audio file (such as file size, no. of bits and total no. of blocks) which is going to be used for the encryption and decryption

Table 5 Basic information about AUDIO file

File Size	1.44 MB
Total number of bits	12079595 bits
Number of bits in one block	128 bits

Total number of blocks	94372

Table 6 provides the encryption time and decryption time of audio file taken by AES algorithm and modified AES algorithm.

Table 6 Encryption Time and Decryption Time of AUDIO file

Algorithm	Encryption Time(ms)	Decryption Time(ms)
AES	1853	4219
Modified AES	664	641

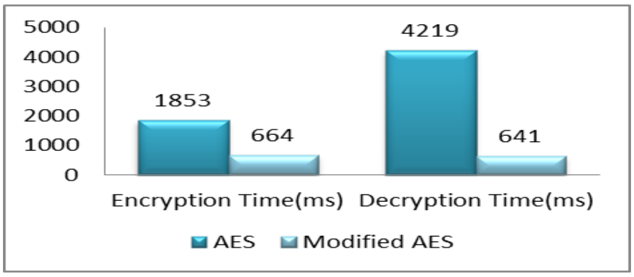

Figure.7 Graphical representation of Encryption Time and Decryption Time of AUDIO file

Figure.7 explain the comparison of encryption time and decryption time of Audio file taken by AES algorithm and modified AES algorithm. It shows that the Modified AES takes less time to encrypt and decrypt the file than the Standard AES.

5.1.4 Encryption and Decryption Time for VIDEO File:

Table 7 gives the basic information of the video file (such as file size, no. of bits and total no. of blocks) which is going to be used for the encryption and decryption.

Table 7 Basic information about VIDEO file

File Size	28 MB
Total number of bits	234881024 bits
Number of bits in one block	128 bits
Total number of blocks	1835008

Table 8 provides the encryption time and decryption time of video file taken by AES algorithm and modified AES algorithm.

Table 8 Encryption Time and Decryption Time of VIDEO file

Algorithm	Encryption Time(ms)	Decryption Time(ms)
AES	35489	83329
Modified AES	12793	12755

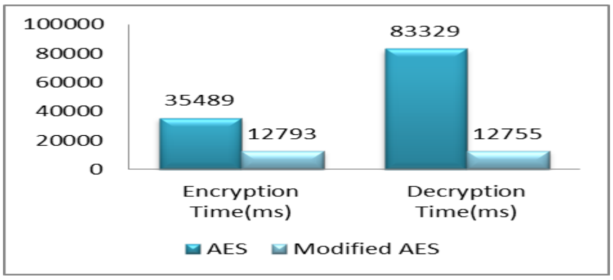

Figure.8 Graphical representation of Encryption Time and Decryption Time of VIDEO file

Figure.8 explain the comparison of encryption time and decryption time of Video file taken by AES algorithm and modified AES algorithm. It shows that the Modified AES takes less time to encrypt and decrypt the file than the Standard AES.

5.2 Throughput of input Text file, Image file, Audio file and Video file.

Throughput: Throughput is a key measure of the quality of a network. It is defined as the number of information bits received without error per second. Here, Throughput is measured in Mbps (Megabits per second).

5.2.1 Throughput of TEXT File:

Table 9 shows the throughput of encryption time and decryption time of Text file taken by AES algorithm and modified AES algorithm.

Table 9 Throughput of TEXT file

Algorithms	Throughput (Mbps)	
	Encryption	Decryption
AES	5.8	2.8
Modified AES	13.8	16.9

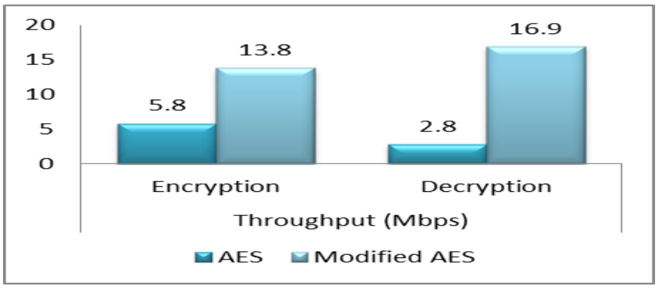

Figure.9 Graphical representation of Throughput of TEXT file

Figure. 9 presents the comparison of throughput for encryption time and decryption time of Text file taken by AES algorithm and modified AES algorithm. It shows that the Modified AES has higher throughput than the Standard AES.

5.2.2 Throughput of IMAGE File:

Table 10 shows the throughput of encryption time and decryption time of Image file taken by AES algorithm and modified AES algorithm.

Table 10 Throughput of IMAGE file

Algorithms	Throughput (Mbps)

	Encryption	Decryption
AES	4.7	2.8
Modified AES	16.2	18.0

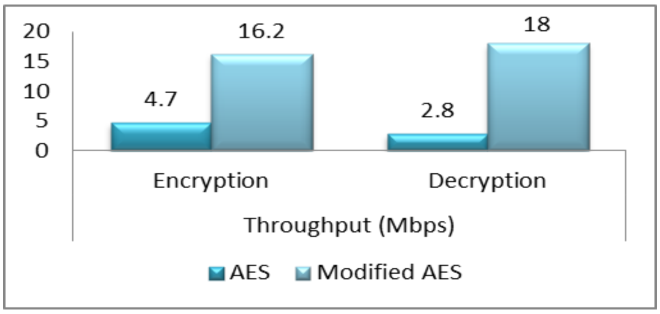

Figure.10 Graphical representation of Throughput of IMAGE file

Figure.10 presents the comparison of throughput for encryption time and decryption time of Image file taken by AES algorithm and modified AES algorithm. It shows that the Modified AES has higher throughput than the Standard AES.

5.2.3 Throughput of AUDIO File:

Table 11 shows the throughput of encryption time and decryption time of Audio file taken by AES algorithm and modified AES algorithm.

Table 11 Throughput of AUDIO file

Algorithms	**Throughput (Mbps)**	
	Encryption	**Decryption**
AES	6.9	2.8
Modified AES	18.1	18.8

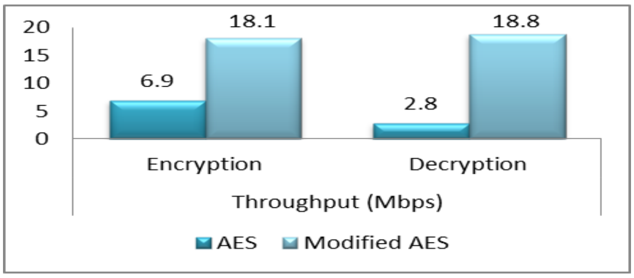

Figure.11 Graphical representation of Throughput of AUDIO file

Figure.11 presents the comparison of throughput for encryption time and decryption time of Audio file taken by AES algorithm and modified AES algorithm. It shows that the Modified AES has higher throughput than the Standard AES.

5.2.4 Encryption and Decryption Time for VIDEO File:

Table 9 shows the throughput of encryption time and decryption time of Video file taken by AES algorithm and modified AES algorithm.

Table 12 Throughput of VIDEO file

Algorithms	**Throughput (Mbps)**	
	Encryption	**Decryption**
AES	6.6	2.8
Modified AES	18.3	18.4

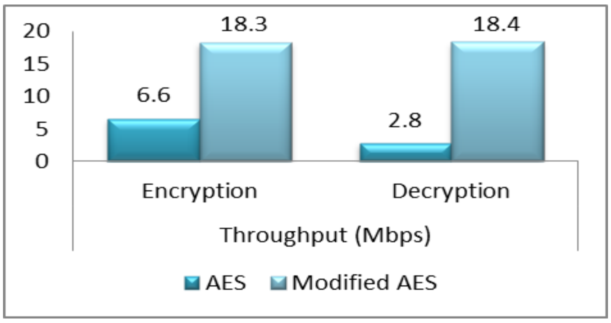

Figure.12 Graphical representation of Throughput of VIDEO file

Figure.12 presents the comparison of throughput for encryption time and decryption time of Video file taken by AES algorithm and modified AES algorithm. It shows that the Modified AES has higher throughput than the Standard AES.

VIII. CONCLUSION

Here, TLS is used with AES as an encryption algorithm to provide a security for data transmission in the NGN. Above results conclude that the proposed encryption scheme is faster than the original encryption scheme for encrypting and decrypting the data. And on the other hand it adds very less overhead to the data. Today, this is the requirement of most of the multimedia applications.

IX. ACKNOWLEDGMENT

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

X. REFERENCES

[1] B Mudit Ratana Bhalla, Anand Vardhan Bhalla, "Generations of Mobile Wireless Technology: A Survey,"International Journal of Computer Applications, Vol. 5– No.4, Aug. 2010.

[2] Vishwa Gupta, Gajendra Singh, Ravindra Gupta, "Advance cryptography algorithm for improving data security,"International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X,Vol. 2, Issue 1, Jan. 2012.

[3] Alyaa Ghanim Sulaiman and Imad Fakhri Al Shaikhli, "Comparative Study on 4G/LTE Cryptographic Algorithms Based on Different Factors," International Journal of Computer Science and Telecommunications Vol. 5, Issue 7, July 2014.

[4] Ritu Pahal, Vikas Kumar, "Efficient Implementation of AES,"International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Vol. 3, Issue 7, July 2013.

[5] Shweta Kumari, Abhishek Kumar, "Improving Speed Up of Computing Using New AES Algorithm," International Journal of Science and Research (IJSR), ISSN (Online): 2319-7064, Vol. 3, Issue 9, Sept. 2014.

[6] N. Seddigh, B. Nandy, R. Makkar J.F. Beaumont Solana Networks Defense Research & Development Canada Ottawa, Canada, "Security Advances and Challenges in 4G Wireless Networks,"2010 Eighth Annual International Conference on Privacy, Security and Trust, IEEE 2010.

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

[8] Christian Makaya, Samuel Pierre, "An Architecture for Seamless Mobility Support in IP-Based Next-Generation Wireless Networks," IEEE Transactions On Vehicular Technology, Vol. 57, pp. 1209-1225, No. 2, March 2008.

[9] Anastasios N. Bikos, Nicolas Sklavos University of Patras, “LTE/SAE Security Issues on 4G Wireless Networks,”2013 IEEE Copublished by the IEEE Computer and Reliability Societies, 2013.

[10] 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.s 2008,

[11] Pravin Kawle, Avinash Hiwase, Gautam Bagde, Ekant Tekam, Rahul Kalbande, “Modified Advanced Encryption Standard,”International Journal of Soft Computing and Engineering (IJSCE), Vol.4, Issue-1, March 2014.

[12] John P. McGregor and Ruby B, “Architectural Techniques for Accelerating Subword Permutations With Repetitions,”IEEE Transactions On Very Large Scale Integration Systems, Vol. 11, No. 3, June 2003.

[13] Bin Liu and Bevan M. Baas, “Parallel AES Encryption Engines for Many Core Processor Arrays,”IEEE Transactions On Computers, Vol. 62, No. 3, March 2013