OPEN ACCESS

International
Journal
Of Modern Engineering Research (IJMER)

A novel approach for Improving Performance and Security in the NGN

Binal Shah[1], Zahir Aalam[2]
[1]*Information Technology, Thakur College of Engineering and Technology, India*
[2]*Information Technology, Thakur College of Engineering and Technology, India*

ABSTRACT: *The basic survey of the Next Generation Network (NGN) is that one framework transports all information and administrations like data, voice and video by encasing these into packets on the Internet. Transport Layer Security (TLS) convention gives a safe transmission between conveying applications and their clients on the web. Advanced Encryption Standard (AES) is the encryption technique provided by TLS to give security. This paper shows an execution assessment for information transmission in 3G/4G systems utilizing TLS. Here AES 128 bit is utilized for encryption due to its high effectiveness and simplicity. AES is modified by using permutation instead of the mix column to overcome the problem of high calculation and computational overhead. The framework is further upgraded by parallel AES to enhance the rate of the calculation. In parallel AES, elements of AES has been partition into two autonomous parts. The outcomes demonstrate that parallel modified AES has a superior execution than the standard AES calculation. Assessment is done in view of Encryption Time, Decryption Time and Throughput.*

Keywords : *AES, MAES, NGN, Parallel Computing, Permutation*

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 had been 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 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*

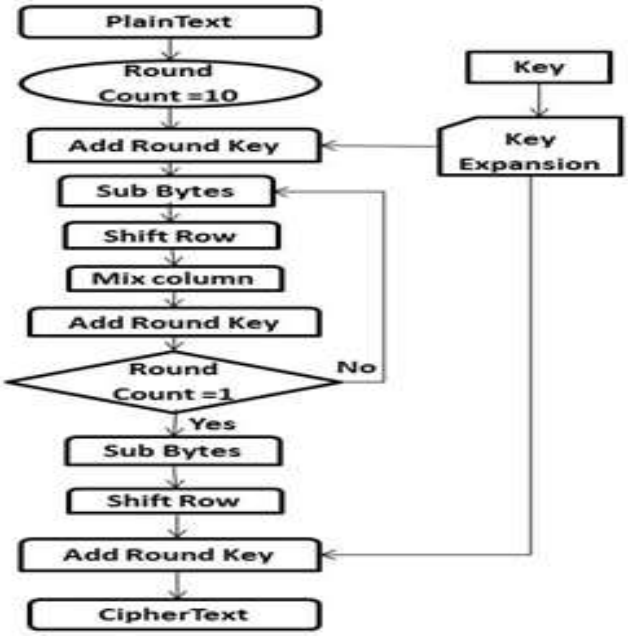

Fig. 1. Flowchart of AES algorithm [5]

III. 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.

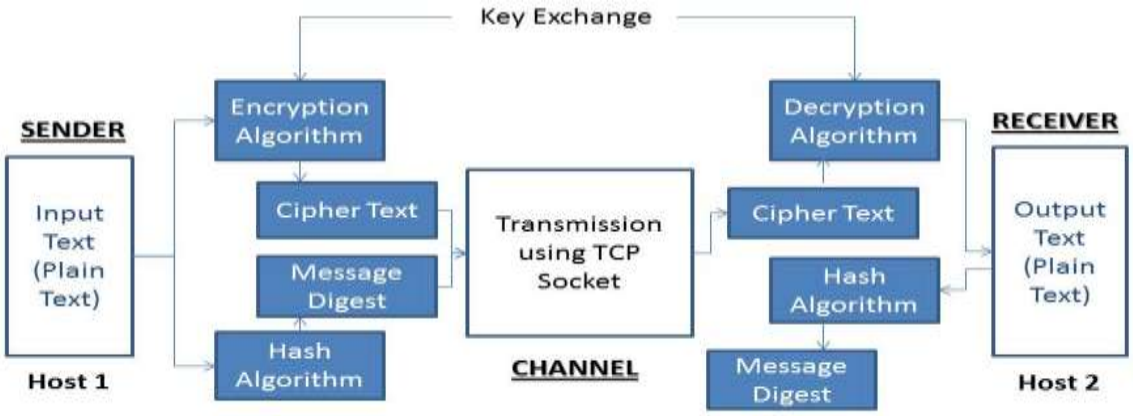

Fig 2. Proposed System

IV. METHEDOLOGY

- 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 Fig. 3.
- In the Modified AES algorithm, Mix column is replaced by Permutation.
- The modification is done by totaling the Initial Permutation step, taken 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, which may also consist of 128 bits in the output. While reading the table from left to right and then from top to bottom, the 242th bit of the 256-bit block is in first position, the 226th is in second position and so forth. After applying the permutation on 128 bits, then again a set of 128 bits is finished and then next remaining functions of the algorithm are performed.
- A parallel AES is as shown in Fig. 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 two parts. And the block size is 128 bits.
- The plaintext is then split into blocks which are encrypted completely in parallel.
- At last, output of the blocks are combined as shown in Fig. 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.
- A modified parallel AES is the combination of modified AES and parallel AES as shown in Fig. 5.

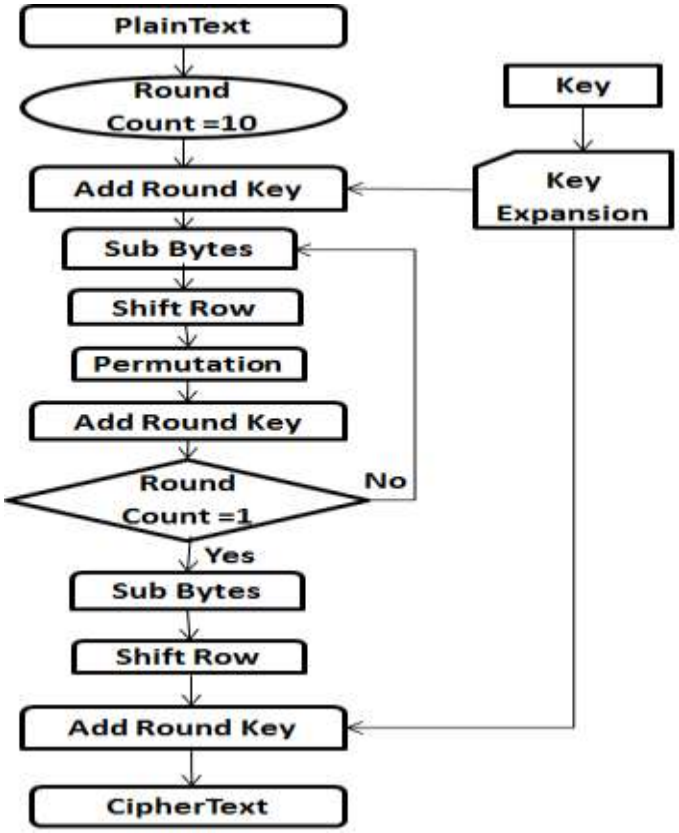

Fig 3. Flowchart of modified AES [5]

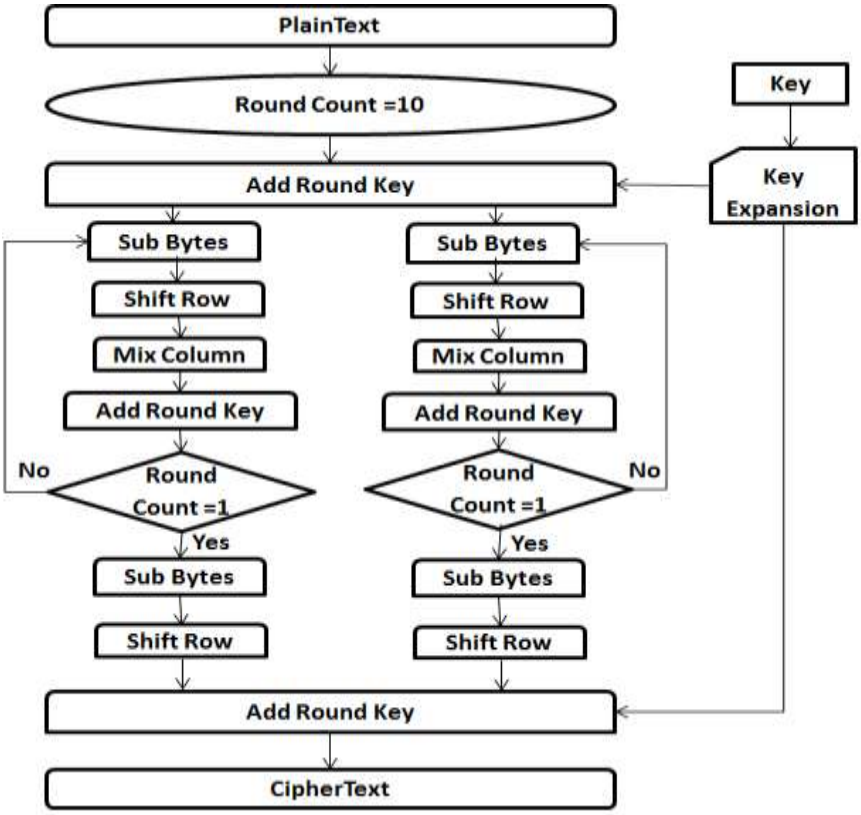

Fig 4.Parallel Standard AES

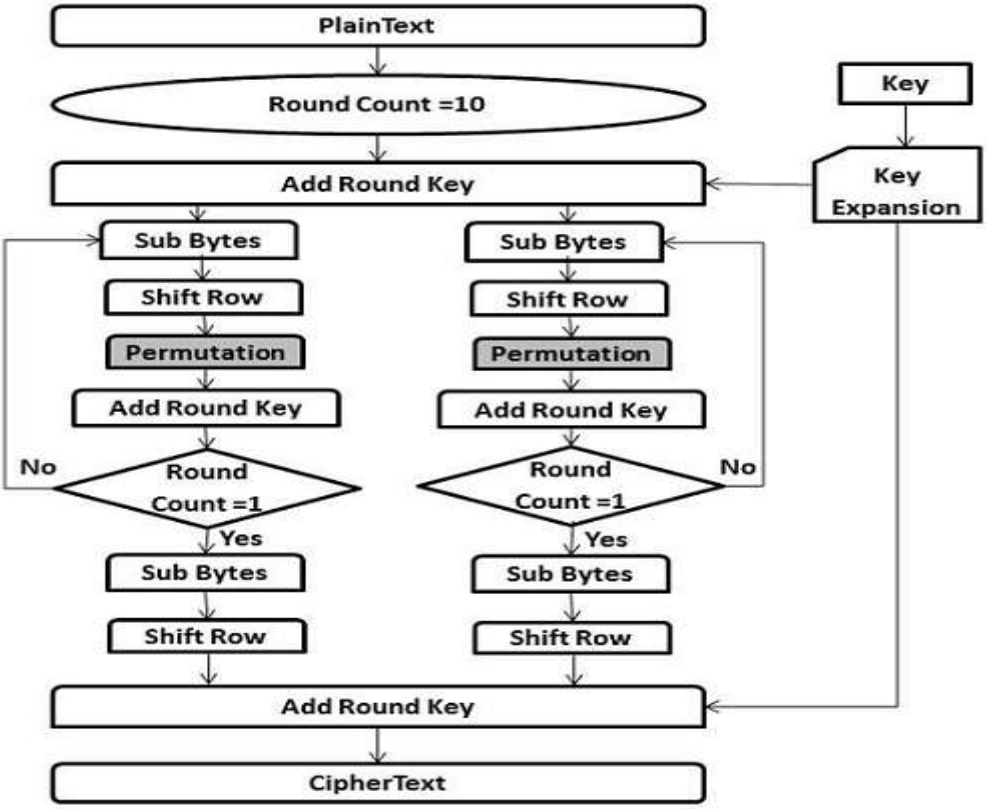

Fig 5.Modified Parallel AES [5]

V. 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)[5].
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].

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, modified AES algorithm, Parallel AES and modified Parallel AES.

Table 2 Encryption Time and Decryption Time of TEXT file

Algorithm	**Encryption Time (s)**	**Decryption Time (s)**
AES	0.023	0.051
Modified AES	0.011	0.011
Parallel AES	0.023	0.041
Modified Parallel AES	0.010	0.008

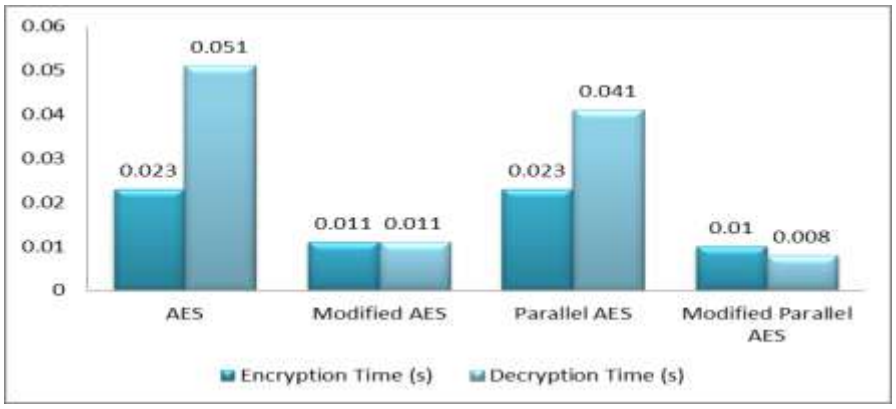

Fig.6 Graphical representation of Encryption Time and Decryption Time of TEXT file

Fig.6 explain the comparison of encryption time and decryption time of Text file taken by AES algorithm, modified AES algorithm, Parallel AES and modified Parallel AES. It shows that the Modified Parallel 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	2.62 MB
Total number of bits	21978153 bits
Number of bits in one block	128 bits
Total number of blocks	171704

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

Table 4 Encryption Time and Decryption Time of IMAGE file

Algorithm	**Encryption Time (s)**	**Decryption Time (s)**
AES	3	6
Modified AES	1.240	1.167
Parallel AES	2.055	4.615
Modified Parallel AES	0.790	0.753

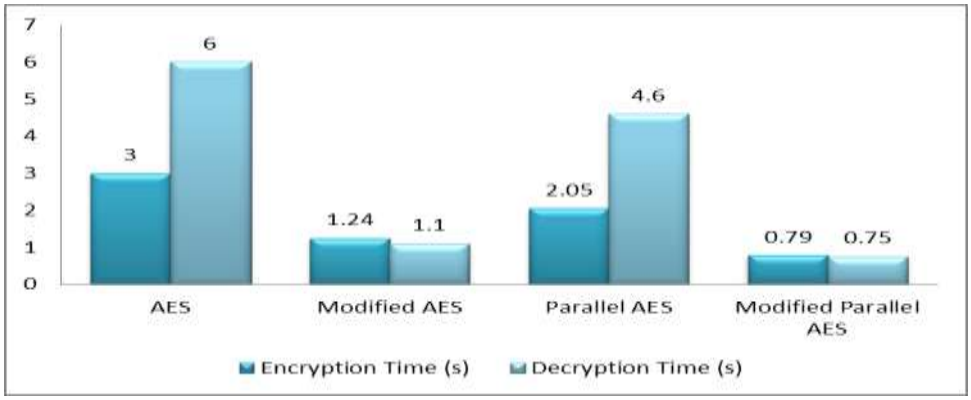

Fig.7 Graphical representation of Encryption Time and Decryption Time of IMAGE file

Fig.7 explain the comparison of encryption time and decryption time of Image file taken by AES algorithm, modified AES algorithm, Parallel AES and modified Parallel AES. It shows that the Modified Parallel 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	6.21 MB
Total number of bits	52093255 bits
Number of bits in one block	128 bits
Total number of blocks	406978

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

Table 6 Encryption Time and Decryption Time of AUDIO file

Algorithm	Encryption Time (s)	Decryption Time (s)
AES	7	16
Modified AES	2.893	2.712
Parallel AES	4.737	10.939
Modified Parallel AES	1.912	1.834

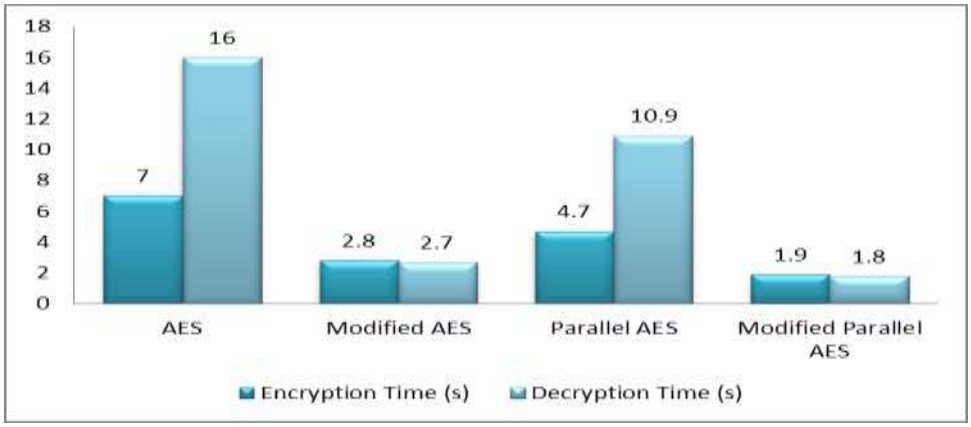

Fig.8 Graphical representation of Encryption Time and Decryption Time of AUDIO file

Fig.8 explain the comparison of encryption time and decryption time of Audio file taken by AES algorithm, modified AES algorithm, Parallel AES and modified Parallel AES. It shows that the Modified Parallel 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	93.6 MB
Total number of bits	78517309 bits
Number of bits in one block	128 bits
Total number of blocks	6134169

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

Table 8 Encryption Time and Decryption Time of VIDEO file

Algorithm	Encryption Time (ms)	Decryption Time (ms)
AES	87	288
Modified AES	44.3	42.5
Parallel AES	70.1	164.0
Modified Parallel AES	27.6	27.4

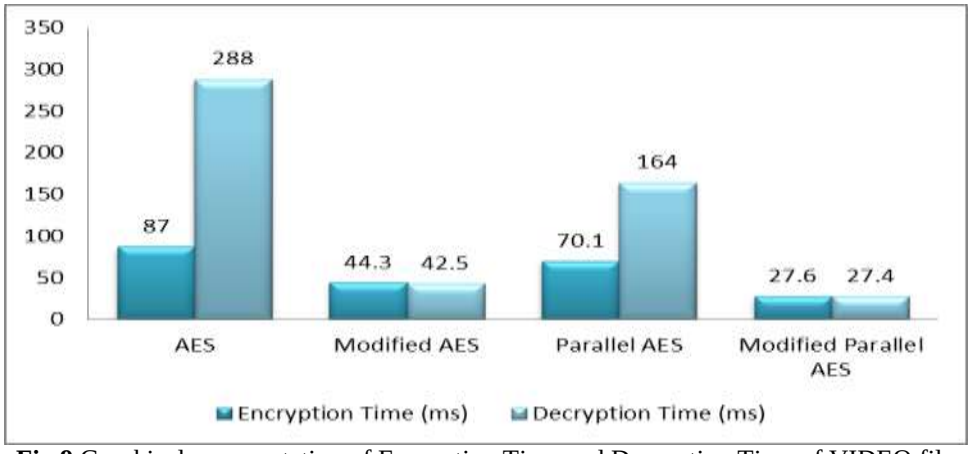

Fig.9 Graphical representation of Encryption Time and Decryption Time of VIDEO file

Fig..9 explain the comparison of encryption time and decryption time of Video file taken by AES algorithm, modified AES algorithm, Parallel AES and modified Parallel AES. It shows that the Modified Parallel 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].

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, modified AES algorithm, Parallel AES and modified Parallel AES.

Table 9 Throughput of TEXT file

Algorithms	**Throughput (Mbps)**	
	Encryption	**Decryption**
AES	7.2	3.2
Modified AES	17.6	18.1
Parallel AES	9.2	4.4
Modified Parallel AES	20.6	21.7

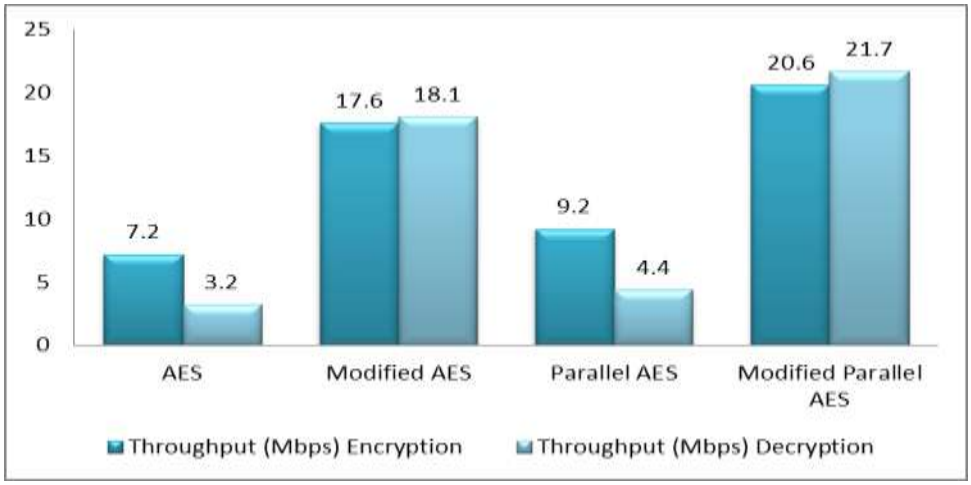

Fig.10 Graphical representation of Throughput of TEXT file

Fig.10 presents the comparison of throughput for encryption time and decryption time of Text file taken by AES algorithm , modified AES algorithm, Parallel AES and modified Parallel AES. It shows that the Modified Parallel 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, modified AES algorithm, Parallel AES and modified Parallel AES.

Table 10 Throughput of IMAGE file

Algorithms	**Throughput (Mbps)**	
	Encryption	**Decryption**
AES	7.3	3.6
Modified AES	17.7	18.8
Parallel AES	10.6	4.7
Modified Parallel AES	27.8	29.18

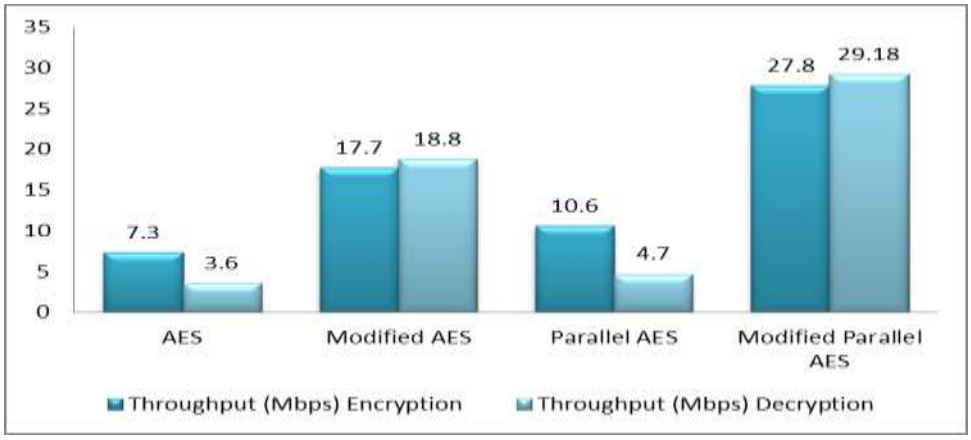

Fig.11 Graphical representation of Throughput of IMAGE file

Fig.11 presents the comparison of throughput for encryption time and decryption time of Image file taken by AES algorithm , modified AES algorithm, Parallel AES and modified Parallel AES. It shows that the Modified Parallel 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 , modified AES algorithm, Parallel AES and modified Parallel AES.

Table 11 Throughput of AUDIO file

Algorithms	**Throughput (Mbps)**	
	Encryption	**Decryption**
AES	7.4	3.2
Modified AES	18.0	19.2
Parallel AES	10.9	4.7
Modified Parallel AES	27.2	28.4

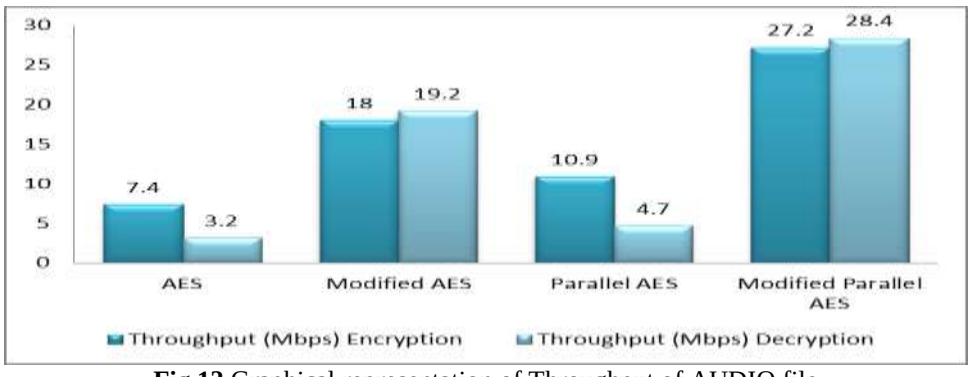

Fig.12 Graphical representation of Throughput of AUDIO file

Fig.12 presents the comparison of throughput for encryption time and decryption time of Audio file taken by AES algorithm, modified AES algorithm, Parallel AES and modified Parallel AES. It shows that the Modified Parallel 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 , modified AES algorithm, Parallel AES and modified Parallel AES.

Table 12 Throughput of VIDEO file

Algorithms	**Throughput (Mbps)**	
	Encryption	**Decryption**
AES	9.0	2.7
Modified AES	17.7	18.4
Parallel AES	11.2	4.7
Modified Parallel AES	28.3	28.6

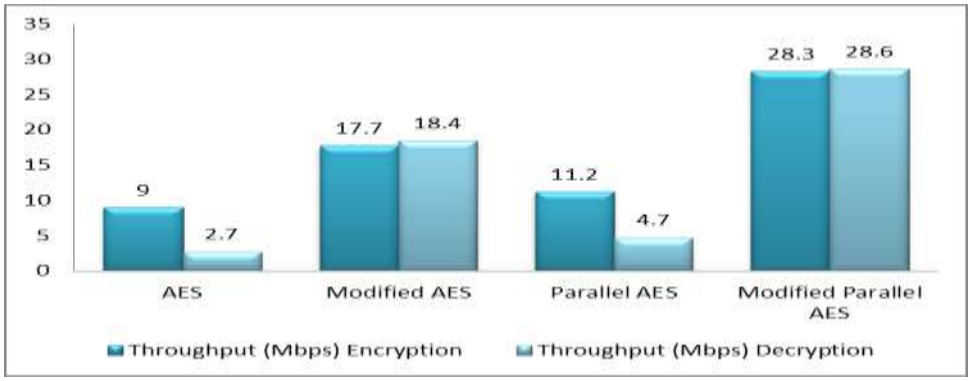

Fig.13 Graphical representation of Throughput of VIDEO file

Fig.13 presents the comparison of throughput for encryption time and decryption time of Video file taken by AES algorithm, modified AES algorithm, Parallel AES and modified Parallel AES. It shows that the Modified Parallel AES has higher throughput than the Standard AES.

VI. 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.

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.

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]. Binal Shah,Zahir Aalam, "To Improve Security and Performance in the NGN," International Journal of Advance Engineering and Research Development (IJAERD), Vol. 02, Issue 12, December 2015.