Enhancement of Security in Message Confidentiality Algorithm for Data Transmission in Next Generation Networks using TLS 1.0

Shruti Mishra [1] Dilasha Jain [2] Sayali Govilkar [3]
[1, 2, 3] TCET Mumbai

Abstract---TLS is a standardized network layer protocol designed to provide communication security over the internet. Transport Layer Security (TLS) is a protocol that ensures privacy between communicating applications and their users on the Internet. TLS 1.0 provides confidentiality, authentication and key exchange. It achieves message confidentiality by means of secure encryption algorithms. The current algorithm that is widely used is AES-128 encryption algorithm. Though it is one of the most trusted and most efficient techniques, it is prone to numerous linear attacks. This project proposes an improvement in the current AES algorithm by means of a new design of the algorithm. The AES algorithm in use presently has an entirely linear structure which makes it easier for the attacker to break it down. The improved design contains the Feistel Network incorporated in AES algorithm along with certain key changes incorporated in each operation of the AES algorithm, which are further modified. This makes it non-linear and prevents it from various algebraic and linear attacks. An attempt is further made to compare the performance of improved AES algorithm with the existing one which proves that the modified AES algorithm is more efficient. The main objective of this project is to enhance the message confidentiality algorithm in TLS 1.0 which is the AES-128 bit block algorithm. The prime focus is to remove the pre-existing vulnerabilities in the present AES algorithm and make it more attack resistant. The project also tries to accomplish the goals of the TLS protocol which include cryptographic security, interoperability, extensibility, and relative efficiency.

I. INTRODUCTION

Secure communication is when two entities are communicating and do not want a third party to listen in. For that they need to communicate in a way not susceptible to eavesdropping or interception. Secure communication includes means by which people can share information with varying degrees of certainty that third parties cannot intercept what was said. Other than spoken face-to-face communication with no possible eavesdropper, it is probably safe to say that no communication is guaranteed secure in this sense, although practical obstacles such as legislation, resources, technical issues (interception and encryption), and the sheer volume of communication serve to limit surveillance. With many communications taking place over long distance and mediated by technology, and increasing awareness of the importance of interception issues, technology and its compromise are at the heart of this debate. For this reason, this article focuses on communications mediated or intercepted by technology.

TLS is a network layer protocol that is used to provide message encryption and authentication between applications and servers where data is send through insecure channel. TLS was released in response to the Internet community's demands for a standardized protocol. When a server and client communicate, TLS ensures that no third party may eavesdrop or tamper with any message. TLS is the successor to the Secure Sockets Layer (SSL) .TLS provides Message Authentication, Message Confidentiality and Key Exchange.

Message Confidentiality

It means no unauthorized person has access to the secured or protected data .AES Algorithm is used to encrypt the data and thereby provide message confidentiality.

The Advanced Encryption Standard (AES), defined in 2001 by NIST renders the work of providing message confidentiality in TLS 1.0 protocol. AES renders an efficient method of encryption through its various rounds. The core structure of AES is analogues to a simple algebraic method. This makes the algorithm prone to linear differential attacks making the AES system inefficient. Fiestel network gives a non-linear model and hence combining AES with the Fiestel network brings about non-linearity in AES. This makes it robust, secure, flexible and trustworthy in all respects.

II. BACKGROUND

A. Literature Survey

(1) International Journal of Computer Applications, 2012(IJCA) Title is Security Enhancement Algorithm for Data Transmission for Next Generation Networks. It proposes the Combination of 128 bit AES and Fiestel Cipher. A Double key Encryption algorithm is used which is based on chaos. The paper proposes Improvement in Encryption time, CPU usage and Avalanche effect.

(2) International Journal of Advances in Engineering & Technology, Sept 2012(IJAET) Title is Enhanced AES Algorithm for Strong Encryption. In this paper, In 128 bit AES changes are made in the 3 operations. Modifications are as follows (1) First and second Row of Cipher key matrix is used to modify Sub Bytes (2)Third row is used to modify Shift Rows operation.(3)Fourth row is used to modify Mix Columns Operation. Proposed Modifications multiplies the complexity of the Algorithm.

(3) Intel Corporation Mobility Group, Israel Development Center, Haifa, Israel, 2012. Title is Intel's new AES Instructions for Enhanced Performance and Security. Intel Proposed 6 new Instructions for encryption , decryption and Key Exchange. AESENC, AESENCLAST, AESIMC, AESKEYGENASSIST, AESDEC, AESDECLAST are the Instructions proposed.

(4) International Journal of Computer Applications in Engineering Sciences, 2012.Title is Enhanced AES Algorithm (Throughput). Proposed work includes full pipelined architecture for AES encryption.

B. AES

Advanced Encryption Standard (AES), a symmetric 128-bit block data encryption technique developed by Belgian cryptographers Joan Daemen and Vincent Rijmen. While the terms AES and Rijndael are used interchangeably, there are some differences between the two.

AES has a fixed block size of 128-bits and a key size of 128, 192, or 256-bits, whereas Rijndael can be specified with any key and block sizes in a multiple of 32-bits, with a minimum of 128-bits and a maximum of 256-bits.Figure 1 elaborates the functions of each step comprising the AES algorithm. The major steps are : Add Round Key, Sub Bytes, Shift Rows and Mix Columns.

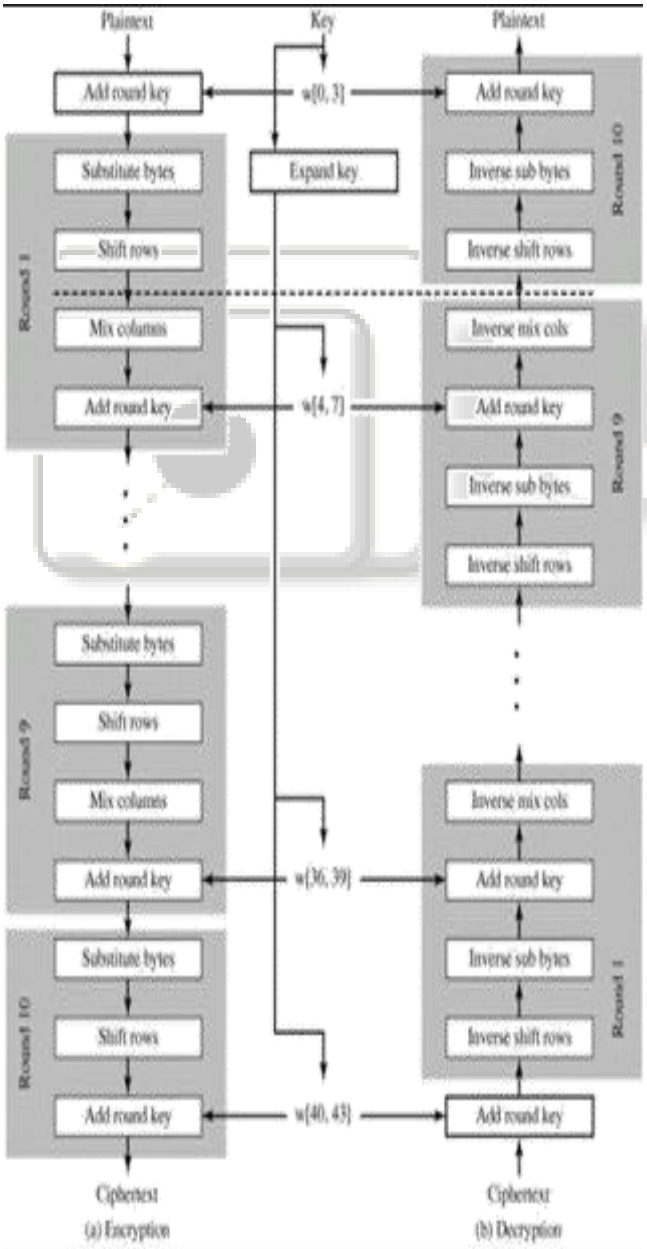

Fig. 1: AES block diagram

III. MODIFIED ALGORITHM

A. Proposed Model

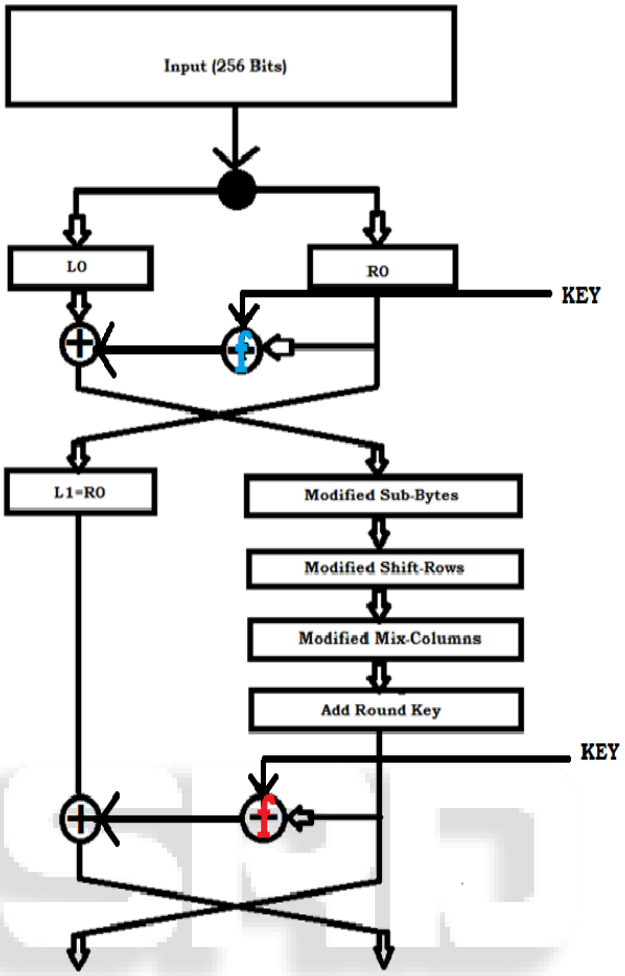

Fig. 2: Proposed Model

B. Improved AES model using Fiestel Network

Mathematically, the idea of an enhanced AES can be construed with reference to basic Fiestel equations. The repetition of these equations is based on the number of rounds as adapted by the Fiestel network. However, by incorporating the AES within these yield the following results;

$Ln = Rn$- (1)

$Rn = AES((Ln)\ \text{XOR}\ fn(Rn-l,,J))$-(2)

From Equation (2), each Rn-l and Kn is channelled into the round function, which basically revolves on a XOR function between these variables. The output of the round function is then XORed with n- before being channelled as input data for the AES algorithm. The result from the AES process represents Rn. The AES operations include the byte substitution, shift row, mix columns and add round key operations. Equations (1) and (2) are then iterated over a period of rounds, retrospective to the number of keys as generated from the key schedule process. In this algorithm the key schedule process for the hybrid system is directly adapted from the AES standard and the round keys for the AES process are directly adapted from the expanded keys.

C. Modifications on AES Round Operations

1) Modified Sub Bytes:

Converting the first row of the key matrix into its binary equivalent, four groups of 8-bit binary values are generated as shown below. The first 4-bits from each 8-bit value are separated out as shown in figure. These bits are grouped into 4 groups: g0g7, g1g6, g2g5, g3g4 where g0, g1, g2 and g3 represent the row number and g7, g6, g5 and g4 represent the column number of state matrix respectively. The data at location M (g0, g7) is substituted from S-box. The substitution i s carried out according to the original Sub Bytes round of AES algorithm. This is repeated for the remaining locations viz. M (g1, g6), M(g2, g5) and M(g3, g4). Thus, using the first row of the cipher matrix 4 data elements are substituted in the state matrix. Similarly, the entire process is carried out using the second row of cipher key matrix.

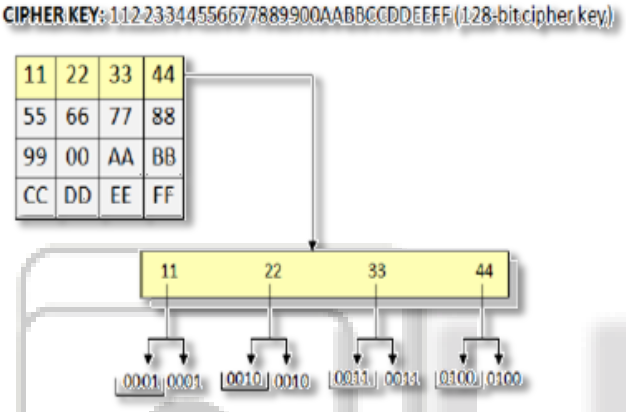

Fig. 3: Modified Sub Bytes

2) Modified Shift Rows:

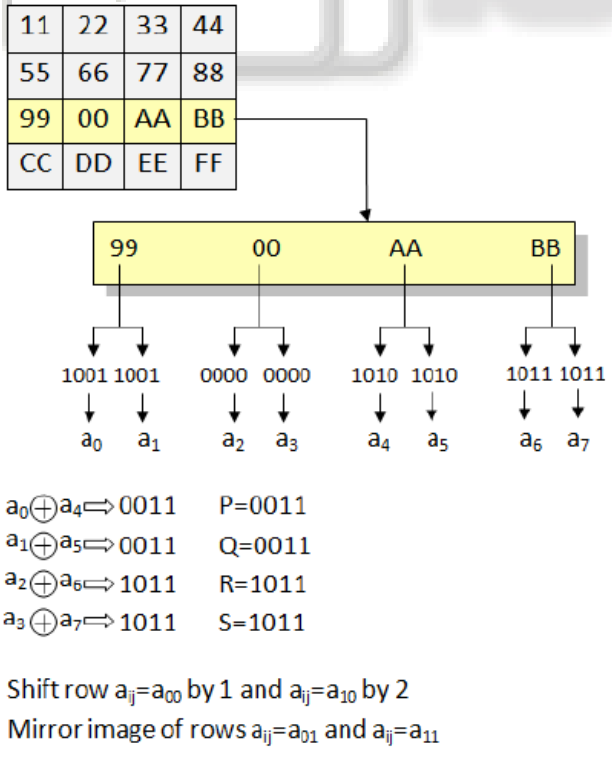

Fig. 4: Modified Shift Rows.

In this step the third row of the key is converted to its binary equivalent form. The binary string is grouped into 8 groups, each group having 4 bits starting from first bit as shown in the figure. The bits of a0 are XOR-ed with those of a4 to obtain a 4 bit binary result, P. Similarly, Q, R and S are generated from the remaining group's i.e. [a1, a5], [a2, a6] and [a3, a7] respectively. Bits of P and R is used to identify the row number whereas the bits of Q and S give the number of cyclic left shifts. The first two bits of P represent the row number which is to be cyclically left shifted. For this row one less than the number of ones in Q is calculated. This gives the number of shifts for the row represented by P. The same process is repeated for R. Here, if first two bits (say a0 and a1) represent the same row which was previously shifted then a1 and a2 are considered which is the next immediate bit. Again, if the row number is same then a2 and a3 are checked followed by a3 and a1. After checking all the bits, if the row number comes out to be the same, then the same row is shifted by one less than the number of ones in S.

3) Modified Mix Columns

In this round the elements of the fourth row of key matrix is grouped as shown in the figure. These groups are then converted into their respective decimal value and modulus-4operation is performed on each group. The remainder (r) will always lie in range of 0 to 3 i.e. 0 _ r _ 3. 0, 1, 2 and 3 represent the first, second, third and fourth column respectively. The Mix Column round of the original algorithm is carried out on the selected column. The maximum number of columns mixed in this step is 4.

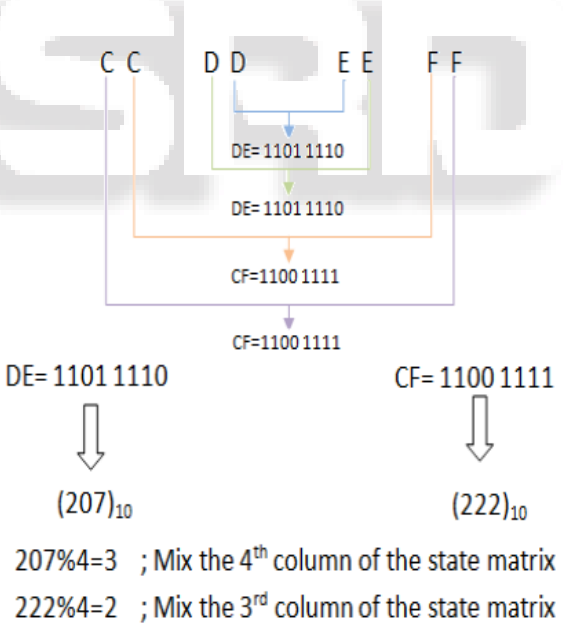

Fig 5: Modified Mix Columns

IV. SCOPE OF THE PROJECT

Firstly, Non-linearity concept of Feistel networks makes the AES an efficient and reliable encryption technique.

Secondly, The improved operations of AES makes the algorithm resistant to all sorts of algebraic attacks and linear attacks.

Thirdly, project compares the performance and efficiency of normal AES and AES with Feistel along with key changes

and modifications that are made to the operations of AES Algorithm.

Fourthly, proposed AES algorithm makes the AES structure irreversible thereby increasing its efficiency.

A. Future Scope of this project

There will be future development on the various AES algorithms (different keys- 128, 192,256) as technology advances.

4G networks are rapidly developing. There is scope for improvement of security algorithms like AES in the 4G networks. The next two to three years will see a lot of innovation in security product development and the business models of equipment vendors. A new generation of security-oriented capabilities and products is coming onto the market. Many of these have a growing number of capabilities and features that are uniquely tailored to the security needs of the mobile network.

Similarly, researchers could be developing a new AES algorithm to overcome drawbacks of AES-192 and AES-256 and further improve the current situation. Maybe in the next couple of years, a new or many other more AES algorithm versions for 4G networks will be introduced worldwide.

V. PROBLEM DEFINITION

Encrypting data eliminates the dangers associated with loss or theft. The process makes data worthless to unauthorized users. Security is a key issue in message encryption process. Various modifications of the original AES algorithm have been made in the previous years.

The chaos method incorporated with AES algorithm increases the key space but it can resist statistical analysis attacks only to a certain extent. Intel just suggested new AES instructions that can be incorporated in the hardware. Thus, AES is linear algebraic encryption method. It is very much prone to non-linear attacks because of its linearity. Murphy and Richardson deduced that it would be possible to break the AES with an effort equivalent to 2^100. Hence, this suggested the various weaknesses in the AES algorithm. Thus, there arose a need to minimize the effect of these attacks on the AES algorithm. Feistel network gives a non-linear model and hence combining AES with the Feistel network brings about non-linearity in AES. This makes it robust, secure, flexible and trustworthy in all respects.

VI. IMPLEMENTATION

(1) In the project we convert user input plain text into hex values using Integer.to toHexString(int i) It Returns a string representation of the integer argument as an unsigned integer in base 16.
(2) The hex values are thereby arranged in a 4*4 matrix known as State matrix (M).
(3) The 128-bit cipher key is arranged in a 4*4 matrix. Each row of this matrix is used for specific operations in the proposed modifications.
(4) Modified Sub-Bytes operation is performed that converts first two rows of key matrix into binary equivalent.
(5) Modified ShiftRows operation is performed that converts third row of key matrix into binary equivalent.
(6) Modified MixColumns operation is performed that converts last row of key matrix into binary equivalent.
(7) AddRoundKey operation is normally performed.
(8) After applying Modified AES encryption, Encrypted 4*4 matrix is generated which is the cipher text.
(9) Standard SHA algorithm is used for authentication purpose.
(10) Similarly normal RSA algorithm is used for key exchange purpose.
(11) Then the information bits are again converted into hexadecimal form to carry out decryption.
(12) It is performed in exactly the reverse manner of the modified operations of encryption algorithm.
(13) After performing AES decryption we get the original plain text.
(14) To check the performance of the code we try to calculate the encryption time and the decryption time and throughput using Java 2 platform.

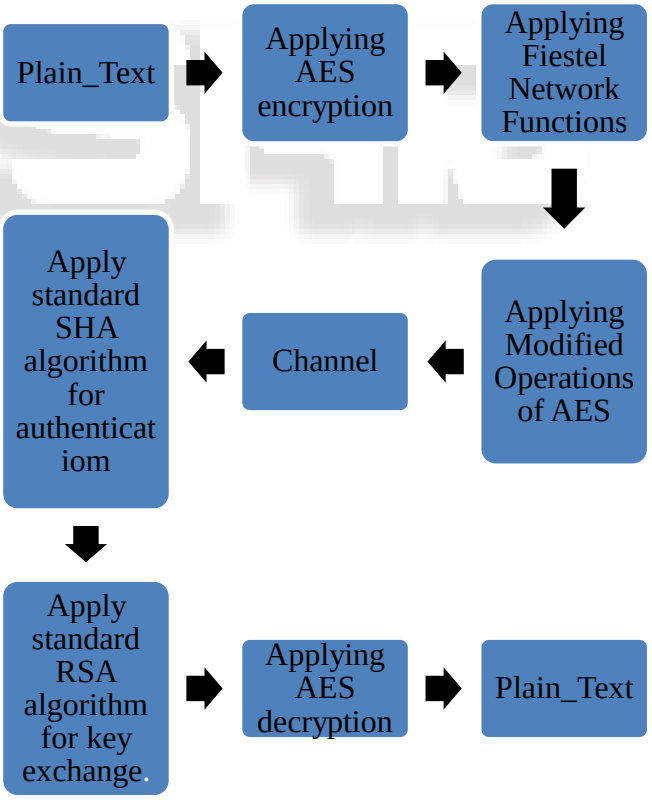

Fig. 6: Project Implementation Diagram

VII. RESULTS

Outputs when using Modified AES algorithm:

A. TEXT:

File size	Server Side Time	Client Side Time
213 KB (218,120 bytes)	157ms	234ms
599 KB (614,250 bytes)	219ms	296ms
5.48 MB (5,747,054 bytes)	140ms	172ms

Table. 1: Configuration 1

File size	Server Side Time	Client Side Time
213 KB (218,120 bytes)	14ms	62ms
599 KB (614,250 bytes)	16ms	171ms
5.48 MB (5,747,054 bytes)	15.8ms	163ms

Table. 2: Configuration 2

B. IMAGE:

File size	Server Side Time	Client Side Time
3.12 MB (3,280,813 bytes)	657ms	672ms
2.30 MB (2,413,043 bytes)	547ms	593ms
4.35 MB (4,562,177 bytes)	781ms	845ms

Table. 3: Configuration 1

File size	Server Side Time	Client Side Time
3.12 MB (3,280,813 bytes)	1187ms	1499ms
2.30 MB (2,413,043 bytes)	1000ms	1156ms
4.35 MB (4,562,177 bytes)	1438ms	1652ms

Table. 4: Configuration 2

C. Encryption Timing Comparison between Existing AES Algorithm and Modified AES algorithm for a 4KB file.

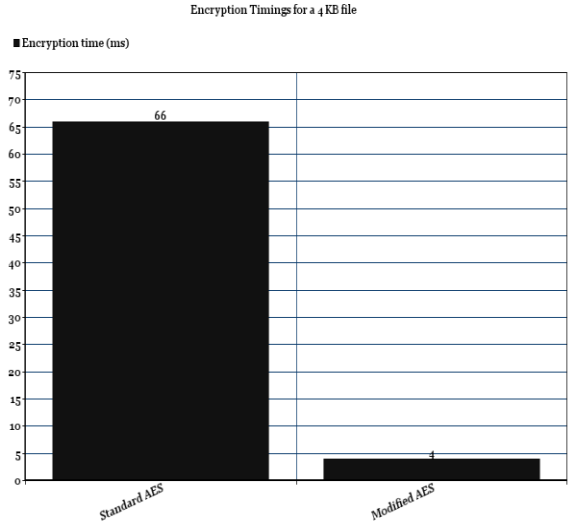

Fig. 7: Timing Comparison

Message	Standard AES	Modified AES
the lazy fox jumped over a dog	74 bits changed 46.25%	98 bits changed 55.68%

Table. 5: Bit difference comparison

D. Bit Difference Comparison between Existing AES Algorithm and Modified AES algorithm for a 4KB file.

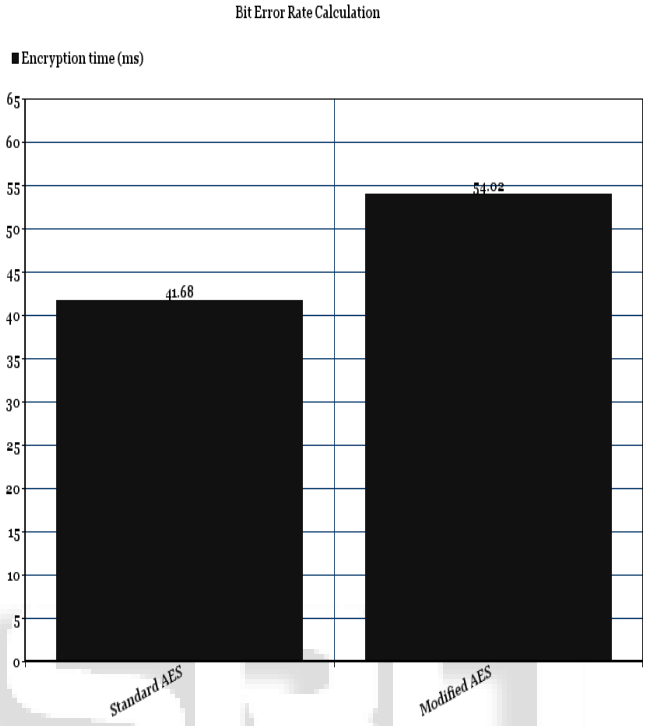

Fig. 8: Bit Difference Comparison

VIII. CONCLUSION

The aim of this project is to design a new AES algorithm that provides non-linearity to the otherwise linear original structure of AES. Although there have been numerous modifications in the original AES algorithm so far, there has hardly ever been an attempt to merge the Fiestel network and cipher-key changes. With this thesis, we hope others will find a new algorithm which will provide enhanced security and protect confidential data.

The Advantages of this design algorithm consist of the following :

(1) Increased throughput.
(2) Better encryption
(3) Works well for almost all types of data.
(4) Reduced linear attacks.

The Disadvantages of this design algorithm consist of the following:

(1) More time will be required if the number of rounds increase.

Applications:

(1) It can be used for various bank transaction sites
(2) It can be used for railway ticket booking sites.

Overall the use of this modified AES algorithm can provide better security and enhanced confidentiality.

ACKNOWLEDGMENT

We are greatly indebted to Prof. Vikas Kaul, our internal guide for his constant support, guidance, co-ordination and encouragement. We also thank him for his moral support, patience, helpful suggestions and numerous discussions during the course of the project. His expertise in the subject of Data Security was a great boost to our efforts. We extend our sincere thanks to our Head of Department, Dr. Kamal Shah. We would also like to thank our reputed principal Dr. B. K. Mishra, our project coordinators, all the staff members and lab assistants who have helped us in our project. We are grateful to our family, friends and classmates for their unconditional support and sincere feedback about out project. Our sincere thanks to the management of THAKUR COLLEGE OF ENGINEERING AND TECHNOLOGY for providing us with a platform and necessary facilities for accomplishing our project.

REFERENCES

[1] International Journal of Computer Applications, 2012 (IJCA), "Security Enhancement Algorithm for Data Transmission for Next Generation Networks".
[2] International Journal of Advances in Engineering & Technology, Sept 2012(IJAET) "Enhanced AES Algorithm for Strong Encryption."
[3] Intel Corporation, Mobility Group, Israel Development Center,Haifa,Israel,2012. "Intel's new AES Instructions for Enhanced Performance and Security".
[4] William Stallings, "Cryptography and Network Security", 4th Edition.
[5] Behrouz A. Forouzan, "Cryptography and Network Security",5th Edition.
[6] Stephen Chapman, "MATLAB Programming for Engineers",2004.
[7] https://www.coursera.org/course/crypto-preview/class/index
[8] www.cipherbyritter.com/LEARNING.HTM#Keyspace

