International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868
Foundation of Computer Science FCS, New York, USA
International Conference & workshop on Advanced Computing 2013 (ICWAC 2013) – www.ijais.org

Enhanced Data Encryption Algorithmfor Next Generation Networks

VikasKaul S K Narayankhedkar AdityaPatil
TCET, MumbaiMGMCET, Navi MumbaiRohitDube
TCET, Mumbai

ABSTRACT

In an age where data transmission over the network has become a vital aspect of communication and information sharing it is very essential to ensure robust data security. Keeping the above fact in mind, we aim to enhance the existing security standards by designing a more efficient Encryption Algorithm. In this paper we propose the idea of using a combination of AES-DES and incorporating it in the Feistal structure. Being a hybrid of two powerful encryption techniques, the algorithm would be an efficient and reliable encryption standard.

General Terms

Data Security, Hybrid Structure, Algorithm.

Keywords

AES, DES, Hybrid, Encryption Time, Avalanche Effect, Throughput, CPU Usage.

INTRODUCTION

The Internet holds an important role for data transmission and sharing. Therefore, encryption is used to secure data transmission. Encryption achieves security effects that make the secret messages unreadable.This is known as Cryptography [1].

The main objective of Cryptography is to communicate securely in such a way that the true message cannot be intercepted by an attacker.There are two types of cryptographic schemes available on the basis of key. They are:

Symmetric Key Cryptography: This cryptographic scheme makes use of a single key for the encryption and decryption of the message [1].

Asymmetric or Public Key Cryptography:This cryptographic scheme makes useof two keys for encryption and decryption of the message, known as the public key and private Key[1].

We can classify Symmetric key cryptography into two types on the basis of their operations as:

• **Stream Ciphers**: In this one byte is encrypted at a particular time[2].

• **Block Ciphers**: It takes a block of plaintext as input, and produces a corresponding output block of cipher text[2].

In this paper we have attempted to use two Symmetric Block cipher algorithms: AES and DES. We intend to develop a Hybrid structure which would improve data encryption standards for currentand future applications.

FEASABILITY

In order to understand the present trend of encryption techniques used we have listed a few prominent online services in various sectors.

Table1. Current Scenario of Encryption Techniques

Service Providers	Encryption Technique	Current Status	Alternative
Facebook	RC4	Legacy	AES
Twitter	RC4	Legacy	AES
Gmail	RC4	Legacy	AES
HDFC Bank	AES-256 CBC	Acceptable	---
Royal Bank of Scotland	3DES_EDECBC	Legacy	AES
State Bank of India	RC4	Legacy	AES
Blackberry Phones	AES-256 CBC	Acceptable	---
IRCTC	AES-128 CBC	Acceptable	---

The alternatives provided are on the basis of Cisco[3]guidelines. Here we can observe that most of the current encryption techniques are AES based or can be replaced by AES. Hence, it advocates the fact that we can make use of the proposed AES hybrid structure as explained further in this paper.

CURRENT APPLICATIONS WITH SECURITY ISSUES

There has been a considerable shift from wired to wireless mode of access to web applications. The major technologies are:

Wi-Fi:

Wi-Fi[4] is a technology that allows an electronic device to transmit and receive data through a wireless medium(using radio-waves) over acomputer network, including high-speed internet connections.

Securing: Initially, the SSID broadcast was disabled to secure the Wi-Fi Network. Another way was to allow the intended MAC addresses only. Wired Equivalent Privacy (WEP) wasused for casual spoofing.

Wi-Max:-

Wi-MAX [4] is a wireless access mechanism used for delivering high-speed connectivity over long distances, thus making it more appealing to Internet and telecommunication service providers.

Securing: With the 802.16e amendment, support for the AES cipher became available, thus ensuring confidentiality of data traffic.

Bluetooth:-

Bluetooth[5] is a prominent wireless technology standard for exchanging data over short distances (using short-wavelength radio transmissions in the ISM band from 2400–2480 MHz) from Fixed and mobile devices, creating personal area networks (PANs) with high levels of security.

Securing:In every Bluetooth device, there are four entities used for maintaining the security at the link level. Private authentication key which is a 128-bit random number is used for authentication purposes. Private Encryption key 8-128 bits in length is used for encryption.

DATA ENCRYPTION STANDARD

The Data Encryption Standard[6] (DES) algorithm was designed by IBM in the 1970's. It is a Block Cipher and has the capacity to accept 64 bits of data at a time. The key size is of 64 bits, out of which only 56 bits are used by the algorithm. Eight bits are used for checking the parity and are later discarded.There are various operations that are performed on the received block of data in DES[7]. They are as follows:

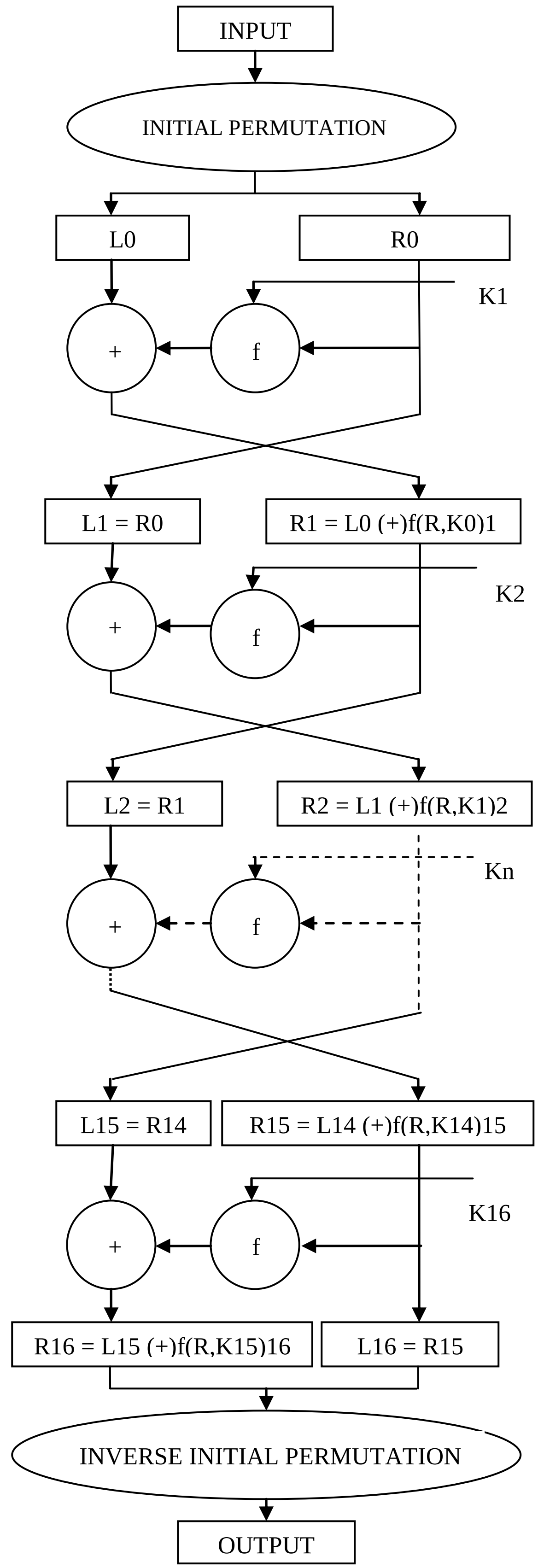

Figure1. Data Encryption Standard

Expansion: The 64 bit block of data is split into two equal parts (32 bit each). The right half block is expanded to 48 bits using the expansion operation.

Key Mixing: The 48 bit expanded block is then XORed with the sub-key (also of 48 bits) that is generated simultaneously during key expansion process
.

Substitution: The block is further divided into Eight 6-bit blocks and each block is given as input to its respective S-box, where the substitution operation is carried out. In this the 48 bit input is permuted to a 32 bit output.

Permutation: The 32 bit output of the S-boxes undergoes a rearrangement in position such that the outputs are distributed or shuffled properly, thus increasing diffusion.

Attacks on DES

Brute Force Attack: The DES algorithm is highly vulnerable to this attack due to its small key space (2^{56}). The Key spaceindicates the number of key combinations possible. Thus each combination or possibility is tried till a correct result is obtained. Smaller the Key space, less is the time required to obtain the actual key, hence compromising security.

Linear Cryptanalysis:The Linear Cryptanalysis[8] is another type of cryptanalytic attack, invented by Mitsuru Matsui. This attack uses linear approximations to describe the action of a block cipher (inthis case, DES).

Differential Cryptanalysis: TheDifferentialcryptanalysis [9]looks specifically at cipher text pairswhoseplaintexts have particular differences. It analyzes the evolution of these differences as the plaintextspropagate through the rounds of DES when they are encrypted with the same key.

TRIPLE DES

Due to the above shortcomings a stronger version of the DES was designed. Triple DES [10] is a variation of DES that is composed of 3 parts. It is slower than the regular DES but it can improve security.

Triple DES uses three 64-bit keys, thus having an overall key length of 192 bits. In the first part of the process, regular DES encryption takes place. The second part is a DES decryption, and a third part which is again ofDES encryption.

It makes use of three keys in various combinations, i.e. all three same, two of them same or all three different. Being based on the DES algorithm, it is very easy to modify existing software to use Triple DES. But even though the triple DES is a more powerful version of DES, it may not be able to provide adequate data protection for newer applications.

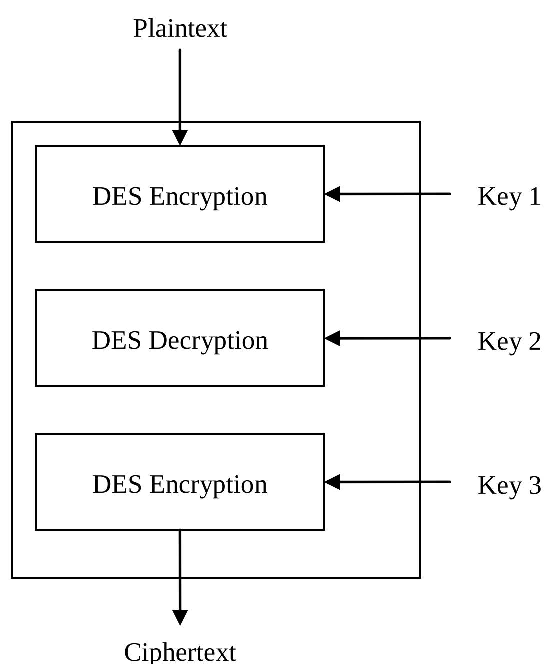

Figure 2. Triple DES

ADVANCE ENCRYPTION STANDARD

The Advanced Encryption Standard[11] [12] came into force in 2001. It is also a Block Cipher, but has a capacity of accepting 128 bits of data at a time. Unlike the DES, theAES does not make use of a Feistal structure. The AES[13] has a variable key size of 128, 192 and 256 bits. The number of rounds for an AES is decided by the Key size. They are 10, 12 and 14 rounds respectively.

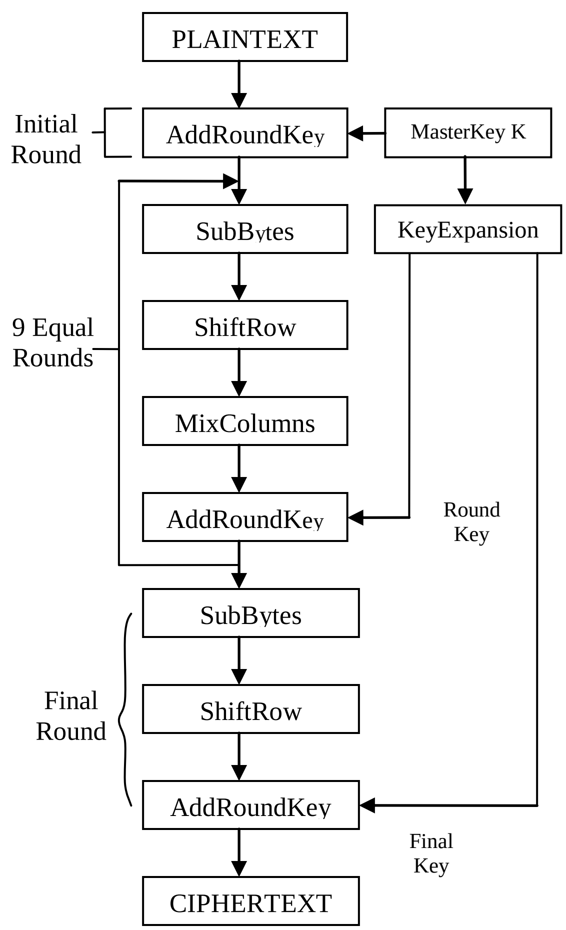

Figure3. Advanced Encryption Standard

The AES algorithm performs various operations on the received block of data. This data is stored in the form of a square matrix of size 4x4, where each unit of the matrix being one byte.

This matrix of data undergoes the following operations:

Byte Substitution: In this the bytes of the matrix undergo substitution with accordance to a lookup table known as S-box. There are two S-boxes for AES; for encryption and decryption. Here each byte is replaced by its corresponding substitute in the S-box.

Shift Rows: Herethe units of each row are shifted by certain number of positions in a cyclic manner. This increases the amount of diffusion in the encryption process.

Mix Columns: In this operation each unit of the matrix is combined with other units of the matrix column-wise.

Add Round Key: Along with the previous operations the process of Key Expansion takes place simultaneously. Each byte is combined with the round key generated using the XOR operation.

Attacks on AES

Algebraic Attack: The AES is especially vulnerable to algebraic cryptanalysis[14], which focuses on the S-box[15] as it is based on the algebraically simple inverse function. It is of prime concern as it is the main stage of converting the plain text to cipher text.Thus it is essential to safeguard the S-boxes against such attacks[16].

Side Channel Attacks: These include attacks based on the actual implementation in the system[17]. They are of two types:

- **Timing Attack:**Watches movement of data in and out of the CPU or memory[18].
- **Power Attack:**Watches power consumption by CPU or memory.

PROPOSED ENCRYPTION STRUCTURE

The below diagram (Fig. 4) shows the overall security system which is inclusive of all the three aspects of secure data transmission:

Data Encryption: Using Hybrid AES-DES algorithm

Message Authentication: Using SHA-256.

Key Exchange Mechanism: Using RSA-2048.

The mode of implementation would be in CBC (Cipher Block Chaining).

The following are a few approaches which can be implemented for encryption. A comparative analysisof these has also been done.

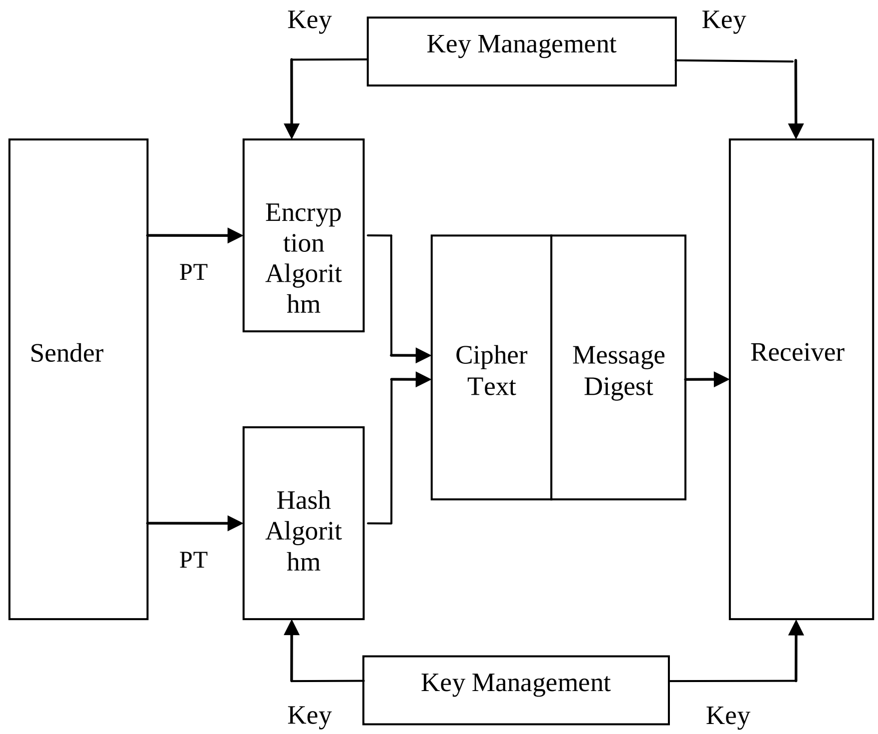

Figure4. Proposed Security System

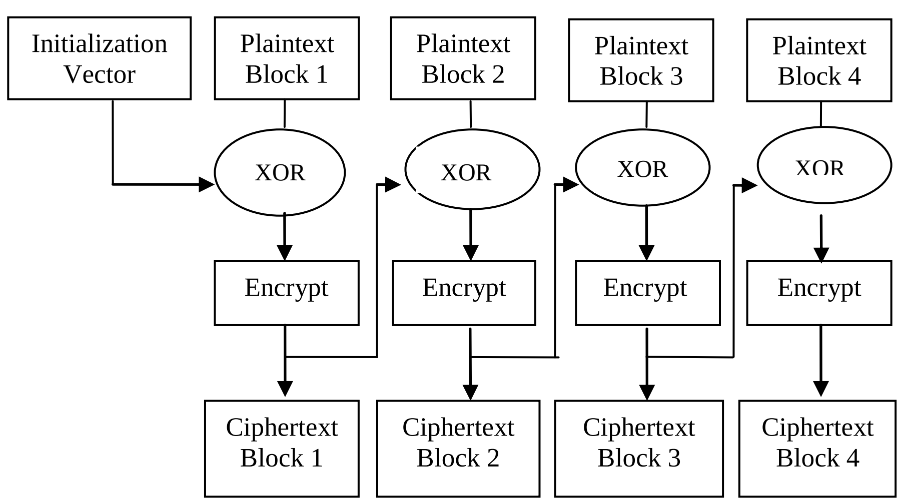

Figure5. Cipher Block Chaining

Approach 1: DES in Feistal Structure

In this approach we have incorporated the DES algorithm in a Feistalstructure of n rounds. Here the overall complexity has improved.Refer table2.

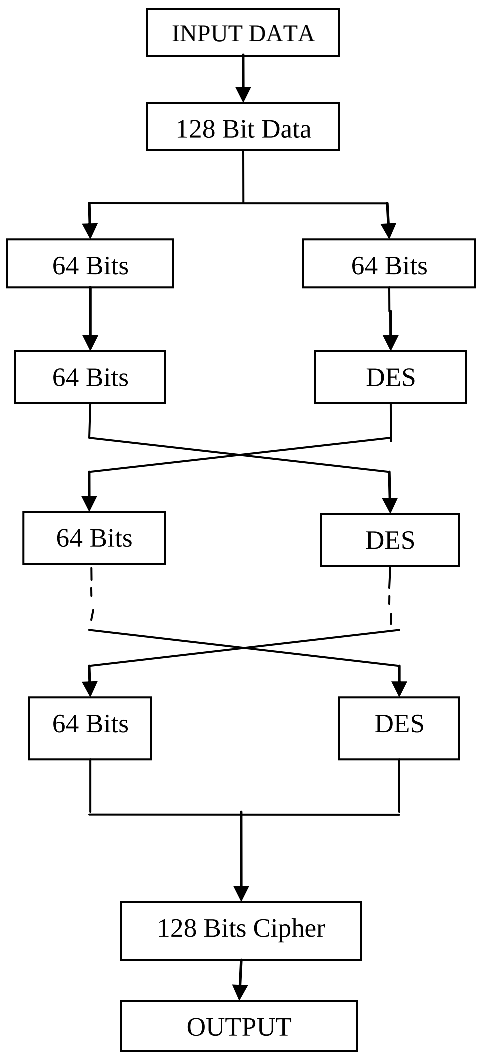

Figure 6.1 Feistal DES structure

Approach 2: AES in Feistal structure

Here, the AES algorithm has been implemented in the Feistal format to reduce the linearity of AES. Refer table 2.

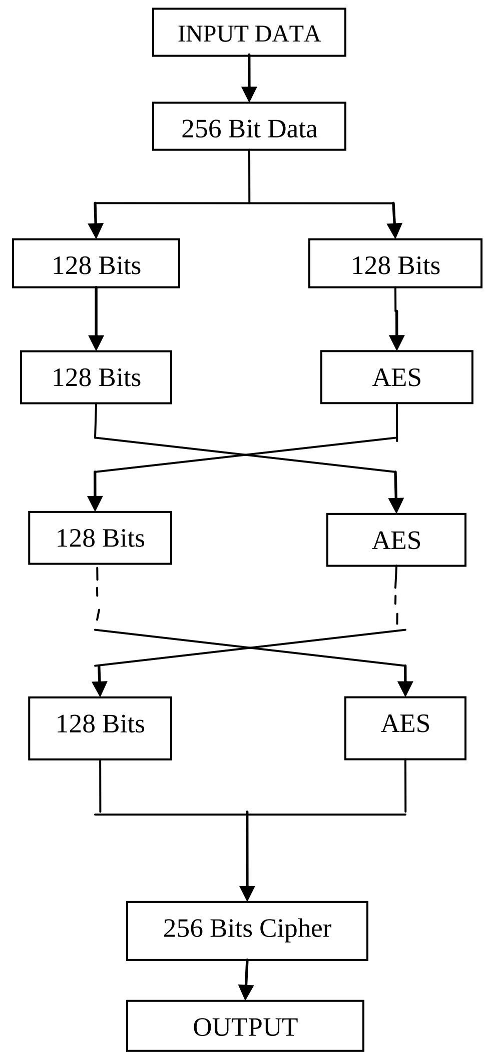

Figure 6.2 Feistal AES structure

Approach 3: Hybrid AES-DES Structure

In this approach, a unique structure of hybrid AES-DES [19]has been designed to bring about a more secured data encryption.

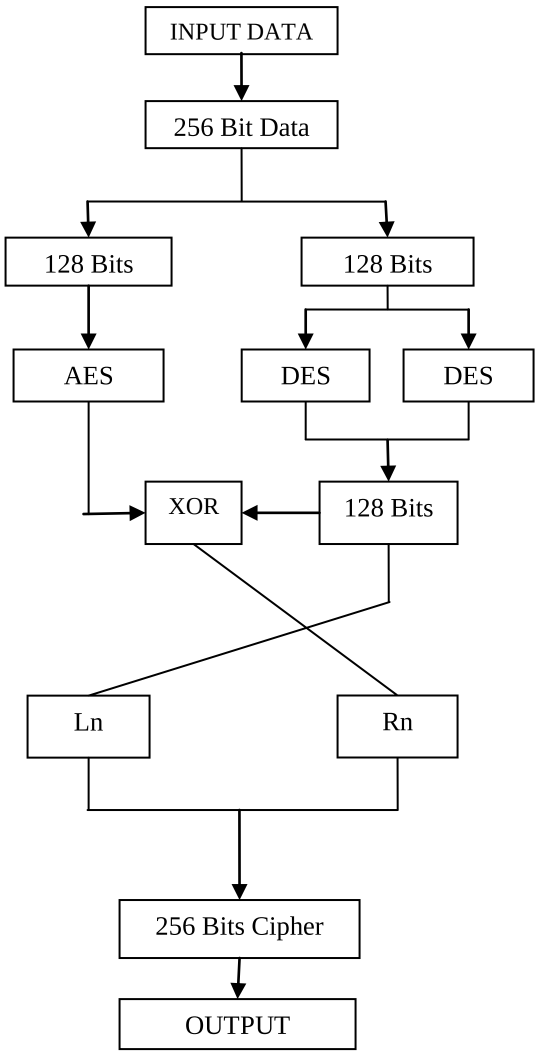

Figure 6.3 Hybrid AES-DES Model

RESULT

The algorithms have been implemented in Matlab[20] R2012a software. The following parameters have been used:

1. Avalanche Effect:A desirable property of any encryptionalgorithm is that a small change in either the plaintext or the key should produce a significant change in the cipher text. In, particular a change in one bit of the plaintext or one bit of the key should produce a change in many bits of the cipher texts.

2.Encryption Time: The time required by the algorithm for processing completely a particular length of data is called the simulation time. It depends on the processor speed, complexity of the algorithm etc. The smallest value of simulation time is desired.

3.CPU Usage: The amount of CPU memory utilization during the execution of algorithms.

4. Throughput: It depicts the number of bits encrypted per unit time. The Formula is as follows:
Throughput = Total no of bits / Total Encryption Time

<u>Configuration Used for Simulation</u>:

Microsoft Windows 7, Intel i5 CPU M480 @ 2.67 GHz, 4GB RAM.

Table 2. Encryption and Decryption Time

Technique	Encryption Time(secs)	Decryption Time(secs)
DES	0.15 sec	0.16 sec
AES	0.12 sec	0.14 sec
DES in Feistal structure	0.91 sec	0.94 sec
AES in Feistal structure	1.78 sec	1.79 sec
Hybrid AES-DES structure	1.91sec	1.94 sec

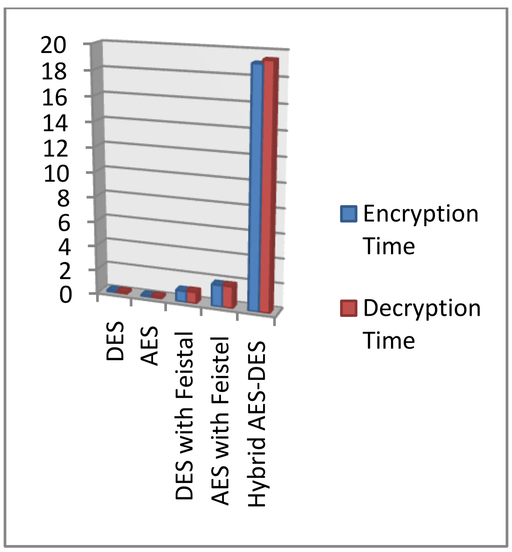

Figure 7

Table 3. Avalanche Effect

Technique	Avalanche Effect	
	Change in 1-bit of Plain Text	Change in 1-bit of Key
DES	34	35
AES	71	64
DES in Feistal structure	69	65
AES in Feistal structure	142	128
Hybrid AES-DES structure	179	174

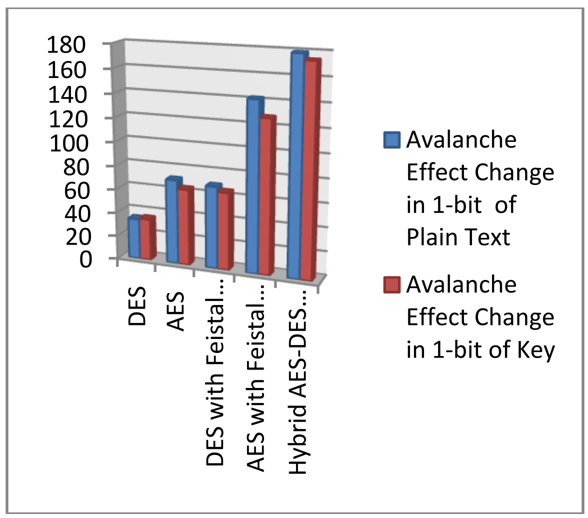

Figure 8

Table 4.CPU Usage and Throughput

Technique	CPU Usage (in %)	Throughput (Bytes/sec)
DES	12%	426.667
AES	22%	1066.67
DES in Feistal structure	25%	140.65
AES in Feistal structure	25%	143.82
Hybrid AES-DES structure	24%	13.40

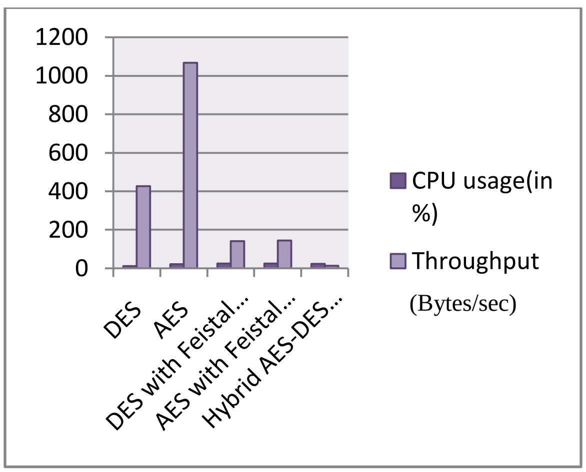

Figure 9

CONCLUSION AND FUTURE WORK

This paper presents a performance evaluation of selected symmetric encryption algorithms. The selected algorithms are AES, DES, and DES in Feistal structure, AES in Feistal structure and Hybrid AES-DES[21] structure. The performance evaluation has been done based on parameters: Avalanche Effect[22], Throughput, CPU Usage, Encryption and Decryption Time.

Till now a single round of the Hybrid structure (Fig 6.3) has been implemented. We intend on implementing up to 10 rounds. Also, we plan to make use of the other algorithms (Fig 4) for our proposed security system which would enable us to enhance the current security standards and adapt to future security demands of various next generation network applications.

REFERENCES

[1] William Stallings, “Cryptography and Network Security”, Pearson Group,4th Edition.

[2] Behrouz. A. Forouzan, “Cryptography and Network Security”, McGraw Hill Group, 5th Edition.

[3] “Cisco Next Generation Encryption Guidelines”, http://www.cisco.com/web/about/security/intelligence/nextgen_crypto.html.

[4] Guillaume Lehembre, “Wi-Fi security – -WEP, WAP and WPA2”.

[5] John Padgette, Karen Scarfone, Lily Chen, “Guide to Bluetooth Security”, NIST Special Publication 800-121 Revision 1.

[6] D. Coppersmith, “The Data Encryption Standard (DES) and its Strength against Attacks”, IBM J. RES. DEVELOP. Vol. 38 No. 3 May 1994.

[7] B. Schneier, “Applied Cryptography: Protocols, Algorithms & Source Code”, C. John Wiley and Sons, 1994.

[8] Mitsuru Matsui, “Linear Cryptanalysis Method for DES Cipher”, In Advances in Cryptology – EUROCRYPT’93, volume 765 of LNCS, pages 386-397.Springer-Verlag, 1993.

[9] Eli Biham, Adi Shamir, “Differential Cryptanalysis of the Data Encryption Standard”, Springer-Verlag, 1993.

[10] William C. Barker, Elaine Barker, “Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher”, NIST, January 2012.

[11] J. Daemen, V. Rijmen, “AES Proposal: Rijndael”, Banksys/Katholieke Universiteit Leuven, Belgium, AES submission, Jun 1998.

[12] NIST, “An Overview of Cryptanalysis Research for Advanced Encryption Standard”, 2001.

[13] “An improved AES algorithm based on chaos” by Yuan Kun, Zhang Han, Li Zhaohui in 2009 at International Conference on Multimedia Information Networking and Security.

[14] H. Nover, “Algebraic Cryptanalysis of AES: Overview”, University of Wisconsin, USA, 2005.

[15] Rashi kohli, Divya Sharma, Manoj Kr.Baliyan “S-Box Design Analysis and Parameter variation in AES Algorithm”, 2012 IJCA.

[16] Aida Janadi and D.Anas Tarah “AES immunity Enhancement against algebraic attacks by using dynamic S-Boxes” in 2008, at IEEE Journal.

[17] Shuo Chen, Rui Wang, Xiao Feng Wang, Kehuan Zhang, “Side-Channel Leaks in Web Applications: a Reality Today, a Challenge Tomorrow”, IEEE Symposium on Security & Privacy, 2010.

[18] David Brumley, Dan Boneh, “Remote Timing Attacks are Practical”, Stanford University, 2003.

[19] Vikas Kaul, S.K.Narayankhedkar, S.Archrekar, S.Agarwal, P.Goyal, "Security Enhancement Algorithm for Data Transmission for Next Generation Networks", IJCA 2012

[20] MATLAB Description, Available: http://www.mathworks.in/help/

[21] M.B.Vishnu, S.K.Tiong, "Security Enhancement using Hybrid AES-DES Algorithm" in 2008 at IEEE Journal.

[22] C. E. SHANNON, "A Mathematical Theory of Communication", The Bell System Technical Journal,Vol. 27, pp. 379–423, 623–656, July, October, 1948.