Hybrid Cryptographic Algorithm for Enhancing Security of Text

Bhavik Rana
P. G. Student, Dept. of Computer Engineering
Rajiv Gandhi Institute of Technology
Mumbai, India
e-mail: ranabhavik25@gmail.com

Sunil Wankhade
Faculty, Dept. of Information Technology
Rajiv Gandhi Institute of Technology
Mumbai, India
e-mail: sunilwankhade9@gmail.com

Abstract—The confidential data that needs to be transmitted over the internet is not safe as that data can be accessible by anyone. Protecting this confidential data over the network is a difficult task and the data security issues become increasingly important. For preventing this confidential data, we use the concept of cryptography. Cryptography is used for securing this confidential data. Cryptography is an art of hiding the data. There are many cryptographic algorithms present for providing security to data, but also same has some drawbacks.

In this paper, we present an approach to develop a hybrid cryptographic algorithm. The hybrid model uses a combination of three symmetric algorithms AES, DES and IDEA. The idea behind creating hybrid algorithm is to provide better security to the data. For our purpose, AES algorithm is restricted to 128-bit key i.e., AES-128 is used in this approach.

Keywords—*AES, DES, IDEA, Hybrid, Cryptography, Security Enhancement.*

*****

I. INTRODUCTION

Transmission of data over the internet is very risky these days as there are many attackers present on the internet. The confidential data that is passed on network is will not be secret if attacker can see this data and hence it is available for all those who are present on network. This means data sent on internet is not at all secure. This means data doesn't remain confidential and is available to all. This means the main security goals are not achieved. For achieving these goals we secure the message using the term cryptography.Cryptography means hidden writing of the data. Cryptography is used to achieve all the security goals as the plaintext is not available to anyone until he/she knows the key. This means data is confidential and only available for those who know the key.

There are many cryptographic algorithms present over the internet to secure the message. Algorithms can be Symmetric-key (Secret key) algorithm or Asymmetric-key Algorithm. Symmetric-key algorithm uses single key for encryption and decryption of the data. Symmetric-key cryptography is also called Private-key cryptography as the key used for encryption and decryption is kept private. Asymmetric-key algorithm used two different keys i.e. private key and public key for encrypting and decrypting data. Asymmetric-key cryptography is also called as Public-key cryptography as the key used for encrypting the data is kept public while the key used for decrypting data is private [1].

There are also some of the hybrid algorithms that combine two Symmetric-key Algorithms like DES and IDEA, DES and AES or combination of one Symmetric-key Algorithm and one Asymmetric-key Algorithm like simple Symmetric-key algorithm and Rivest-Shamir-Adleman (RSA) algorithm. These hybrid algorithms can be used for encryption and decryption of string, a normal file or an image file. Some hybrid algorithms were used for security of digital motion image [2], while some were used for data security [3].

II. METHODOLOGIES

A. Advance Encryption Standard (AES)

AES is a Symmetric-block cipher, which means it uses single key for encryption and decryption purpose. The input block size for AES is 128-bit and the key for AES can be 128-bit, 192-bit or 256-bit. The number of rounds for AES depends on the key size for example, for 128-bit key size the number of rounds are 10, for 192-bit key size the number of rounds are 12 and for 256-bit key size the number of rounds are 14 [4]. The working of overall structure for AES is explained below.

Each round of AES consists of four transformations which include Substitute Bytes, Shift Rows, Mix Column and ADD Round Key. All the four transformation are done in each round except for the last round because in last round Mix Column transformation is not done.

Substitute Bytes is the process in which the bytes are replaced by other bytes which are represented by original bytes from the S-box table. The S-box is not the random value but there is a defined method for creating the S-box. For this round, each byte is mapped with the new byte where the left part of byte represents the row in the S-box table and the right part of the byte represents the column in the S-box table. For example, the byte {25} selects 2^{nd} row and 5^{th} column of the S-box table which will contain the value {3F}.

In Shift Rows transformation, each row is shifted by some bits. This means each row does left-circular shift as per decided by the AES. It is just a simple permutation and it works as the 1^{st} row is not altered, the 2^{nd} row is shifted by 1 byte to the left

in circular manner, 3rd row is shifted by 2 bytes to the left in circular manner and the 4th row is shifted by 3 bytes to the left in circular manner.

In Mix Column Transformation, the output after Shift Rows Transformation is multiplied with the predefine matrix of AES. This stage is basically a substitution. Every element of the product matrix is the sum of products of elements of one row and one column. The Mix Column transformation of a single column j($0 \le j \le 3$) for the output is given in equation (1), (2), (3) and (4).

$$s`_{0,j} = (2 \bullet s_{0,j}) \oplus (3 \bullet s_{1,j}) \oplus s_{2,j} \oplus s_{3,j} \quad 1$$

$$s`_{1,j} = s_{0,j} \oplus (2 \bullet s_{1,j}) \oplus (3 \bullet s_{2,j}) \oplus s_{3,j} \quad 2$$

$$s`_{2,j} = s_{0,j} \oplus s`_{1,j} \oplus (2 \bullet s_{2,j}) \oplus (3 \bullet s_{3,j}) \quad 3$$

$$s`_{3,j} = (3 \bullet s_{0,j}) \oplus s_{1,j} \oplus s_{2,j} \oplus (2 \bullet s_{3,j}) \quad 4$$

Where•indicates multiplicationover the finite field GF (2^8).

In the final transformation, the Round Key is XORed with the output of Mix Column transformation and so it is called Add Round Key Transformation. The operation is column wise operation for 4 bytes of output of Mix Column transformation and 1 row of the round key. This transformation is kept simple but it affects every byte of the output of Mix Column transformation.

B. *Data Encryption Standard (DES)*

DES is a symmetric block cipher which is based on Fiestal network structure which divides the input in two halves. DES uses the same key for encryption and decryption purpose. DES takes input of 64-bit. The key size for DES is 64-bit out of which 8 bits are used for parity checking, which means the key size becomes 56-bit [5]. There are total 16 rounds for Des algorithm. The overall working of DES is explained further.

The working of 16 rounds is done on the basis of equation (5) and (6).

$$L_i = R_{i-1} \quad 5$$

$$R_i = L_{i-1} \oplus \boldsymbol{F}(R_{i-1}, K_i) \quad 6$$

Where L_i indicates left part of round i and $R_i$indicates right part of round i.

The inner working of the single round of DES is based on fiestal network in which first the input of 64-bit plaintext is divided into two halves of 32-bit plaintext. Similarly, the key of 56-bit is divided into two halves of 28-bit. For the value of next round left part is given the value of right part and the key operation is done on right part which includes first the expansion table which converts 32-bit data to 48-bit data. Also, both halves of key do the left circular shift and then both are given to permuted choice box 2 which converts 56-bit key to 48-bit. After that the right part of plaintext is XORed with the key. This output is given to S-box which converts this 48-bit data to 32-bit data. Then, this output is given to the permutation box. Finally, the value for right half is generated by XORing output of permutation box with left half data. This is done for 16 rounds.

C. *International Data Encryption Algorithm (IDEA)*

IDEA is a symmetric block cipher. IDEA is the advance version of DES algorithm. It takes input of 64-bit block. IDEA is stronger than DES. The key size for IDEA block is 128-bit. There are total of 8 rounds in IDEA and 1 output transformation round. The working of IDEA is explained next.

IDEA uses 6 keys for each round uses 4 keys for output transformation round. The working of round is in multiple steps which include multiplications, addition and XOR operations. The input 64-bit block is divided into 4 16-bitblocks and 128-bit key is divided into 8 16-bit blocks. The 8 keys get exhausted in 2nd round, so for generating further keys left circular shift of 25 bits is done. Hence, IDEA uses total of 48 keys for 8 rounds and additional 4 keys for output transformation round i.e., total of 48+4=52 keys are generated for IDEA[6]. Each round has a total of 14 steps and the output transformation round has 4 steps.

III. PROPOSED SYSTEM

The proposed system is a combination of three symmetric-key cryptography algorithms i.e., combination of AES, DES and IDEA to create hybrid cryptography algorithm. The algorithm design here is used for providing better security to the data.

A. *Overall Structure*

The Encryptionprocess for hybrid cryptography algorithm is shown in Fig. 1. The steps for encryption process of hybrid cryptography algorithm are as follows:

Step 1: 64-bit plaintext is taken from user input.

Step 2: This 64-bit plaintext is passed to DES block to generate 64-bit ciphertext.

Step 3: The output of Step 2 is passed to IDEA block which generates 64-bit ciphertext.

Step 4: Finally, the output from Step 3 is given to AES block which generates 128-bit ciphertext.

The hybrid algorithm uses three keys. Key 1 is of 64-bit which is given to DES, key 2 is of 128-bit which is given to IDEA and key 3 is of 128-bit which is given AES.

The Decryption process for the hybrid algorithm is the reverse of the Encryption process.The Decryption process for the hybrid algorithm is shown in Fig 2. The steps for encryption process of hybrid cryptography algorithm are as follows:

Step 1: 128-bit ciphertext is passed to AES block which gives the output of 64-bit deciphertext.

Step2: The output of Step 1 is passed to IDEA block which generates the deciphered 64-bit deciphertext.

Step 3: The output of Step 2 is passed to DES block which generates the 64-bit plaintext.

Step 4: Finally, the 64-bit plaintext is shown to user.

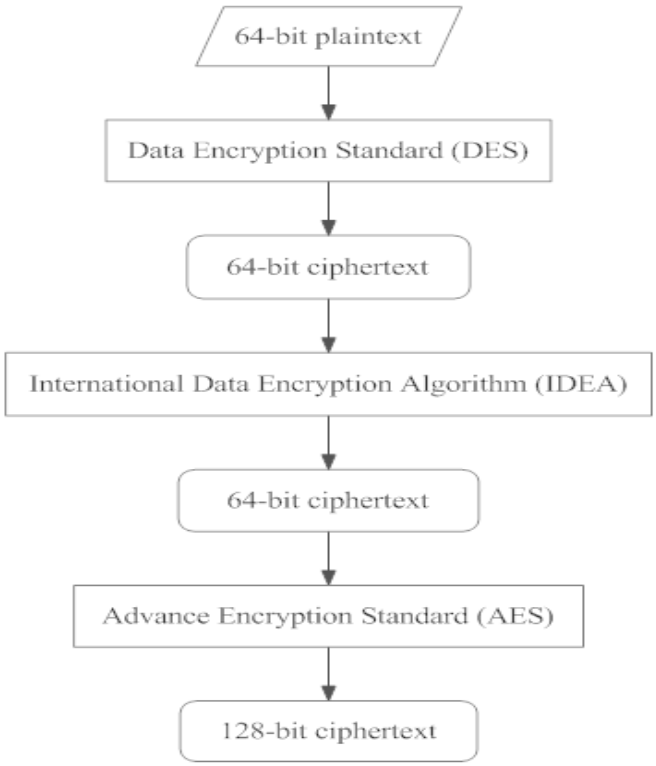

Figure 1: Encryption process of hybrid cryptography algorithm.

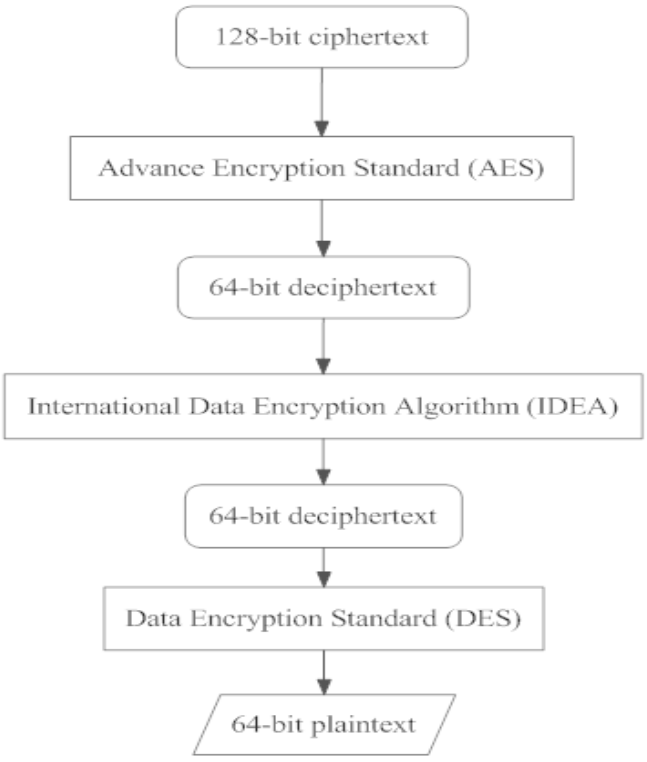

Figure 2: Decryption process of hybrid cryptography algorithm.

IV. Experimental Results

The experimental results for the hybrid algorithm are discussed in this. Starting from the main interface,this is shown in Fig. 3.In which the user has the option for choosing the algorithm from AES, DES, IDEA or Hybrid.

The output of encryption process of the hybrid algorithm is shown in Fig. 3. And the output of the decryption process is shown in Fig. 4.

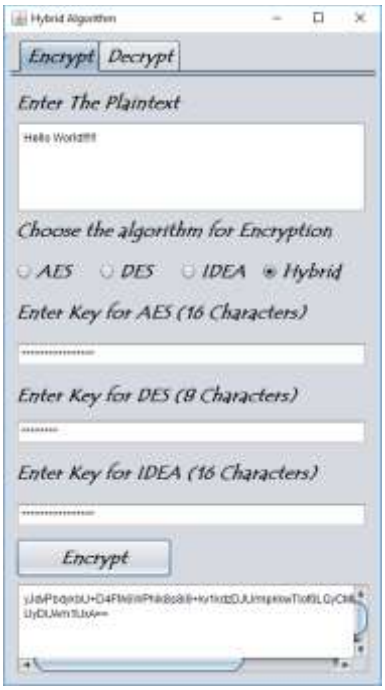

Figure 3: Output of encryption process of hybrid algorithm.

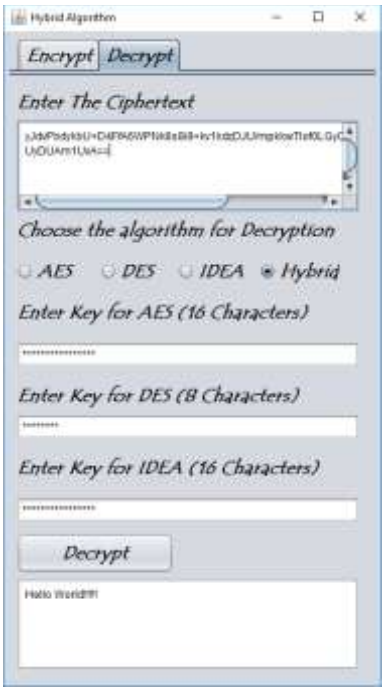

Figure 4: Output of decryption process of hybrid algorithm.

The results and analysis on the output (ciphertext) generated by the different algorithms is shown in Fig. 5(a), Fig. 5(b), Fig. 5(c) and Fig. 5(d). Fig. 5(a) shows the comparison ofEntropy value between AES algorithm and Hybrid algorithm,Fig. 5(b)shows the comparison of Histogram graph between DES algorithm and Hybrid algorithm, Fig. 5(c)shows the comparison of Auto-correlation graph between IDEA algorithm and Hybrid algorithm and Fig. 5(d) shows the result analysis of Floating frequency for Hybrid algorithm. The plaintext given to

all the different algorithms is “Hello World!!!!!” to generate ciphertext.

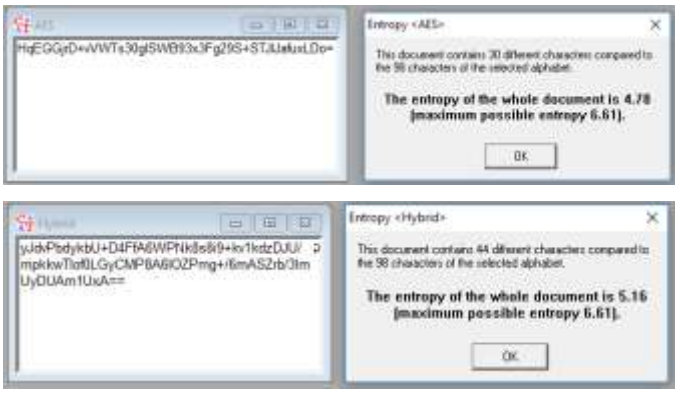

Figure 5(a): Comparison ofEntropy value between AES and Hybrid algorithm.

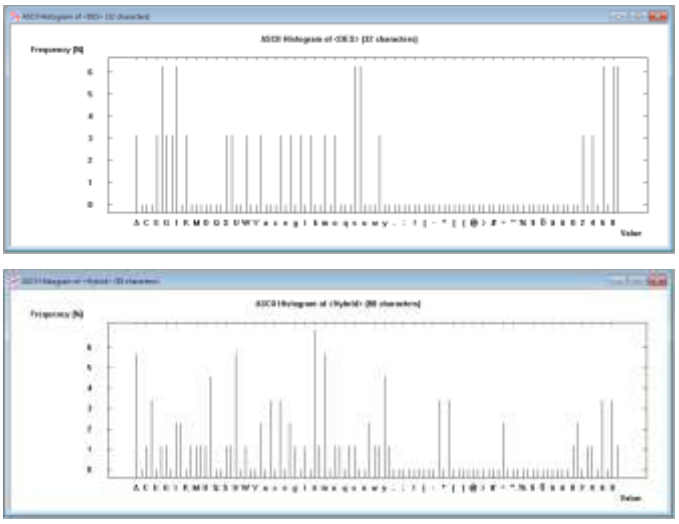

Figure 5(b): Comparison of Histogram graph between DES and Hybrid algorithm.

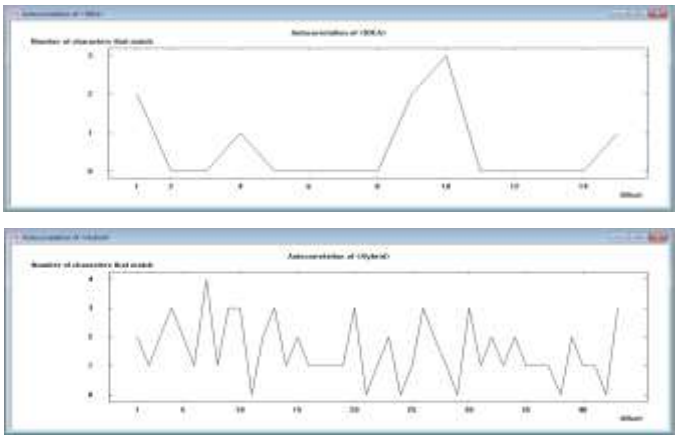

Figure 5(c): Comparison of Auto-correlation graph between IDEA algorithm and Hybrid algorithm

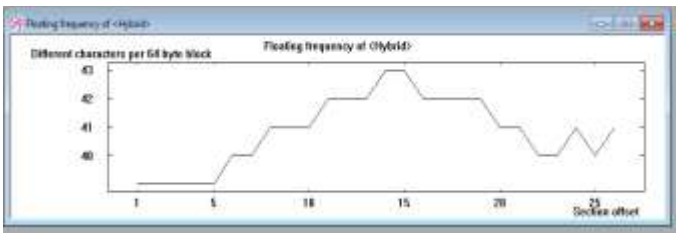

Figure 5(d): Result Analysis of Floating frequency for Hybrid algorithm.

The result analysis of entropy shows the different values for different algorithms. The entropy is used to define the randomness of the calculated ciphertext. The higher the entropy value, the more randomness is included. The lack of entropy can have the negative impact on performance and security. As per the results, the hybrid algorithm described here offers the highest entropy value than the rest all algorithms for the same plaintext.

The other result analysis is the histogram for generated ciphertext. The histogram is the graph for the characters present in the ciphertext and the frequency of a character which means how many times the character appeared in the generated ciphertext. On the X-axis of histogram all the alphabets including upper and lower case, special characters, space, etc. are included. The Y-axis shows the frequency in percentage of the character is present in the ciphertext. The ciphertext generated using hybrid algorithm gives the total value of 88 characters whereas, AES gives the total of 44 characters and DES and IDEA provides the total of 32 characters for same plaintext.

The other result analysis is the auto-correlation for generated ciphertext. The autocorrelation is an index of the similarity of different sections. The similarity between two sets of data is normally measured by their correlation. Correlation C between two sequences of length n is calculated from the number A of agreeing and the number D of non-agreeing sequence members according toequation (7).

$$C: = (A-D) / n \qquad 7$$

On the X-axis the offset value is given and on the Y-axis number of characters that match is given. The ciphertext generated using hybrid algorithm gives the total value of 88 characters whereas, AES gives the total of 44 characters and DES and IDEA provides the total of 32 characters for same plaintext.

The hybrid algorithm also gives the result analysis of floating frequency as the ciphertext generated is greater than 64 characters. The floating frequency is a characteristic of its local information content at individual points in the document. The floating frequency specifies how many different characters are to be found in any given 64-character long segment.

On the X-axis the section offset is given and on the Y-axis different characters per 64-byte block is given. In cryptography, the mechanism is mainly used to locate keys amongst large quantities of data.

The comparison of different parameter used for result analysis for all the algorithms are shown in Table 1.The table shows the different values of entropy, input characters, output characters and either the algorithm can generate Floating Frequency or no. The input taken here was “Hello World!!!!!” which contains 16 characters.

TABLE I. COMPARISION OF DIFFERENT PARAMETERS OF RESULT ANALYSIS FOR DIFFERENT ALGORITHMS

Algorithms / Parameters	AES	DES	IDEA	HYBRID
Entropy (out of 6.61)	4.78 (30/98 different characters)	4.56 (25/98 different characters)	4.41 (24/98 different characters)	5.16 (44/98 different characters)

Input Characters	16	16	16	16
Output Characters	44	32	32	88
Can generate Floating Frequency	No	No	No	Yes

The comparison of encryption and decryption time in milliseconds of AES, DES, IDEA and Hybrid algorithm are given in Table 1.

TABLE II. COMPARISION OF ENCRYPTION AND DECRYPTION TIME OF DIFFERENT ALGORITHMS

Time Taken / Algorithm Used	Average Encryption Time (In ms)	Average Decryption Time (In ms)
AES	101.8	97.4
DES	93.8	90.6
IDEA	330	336
Hybrid	348.6	337

The graph for the encryption and decryption process for the different algorithms is shown in Fig 6.

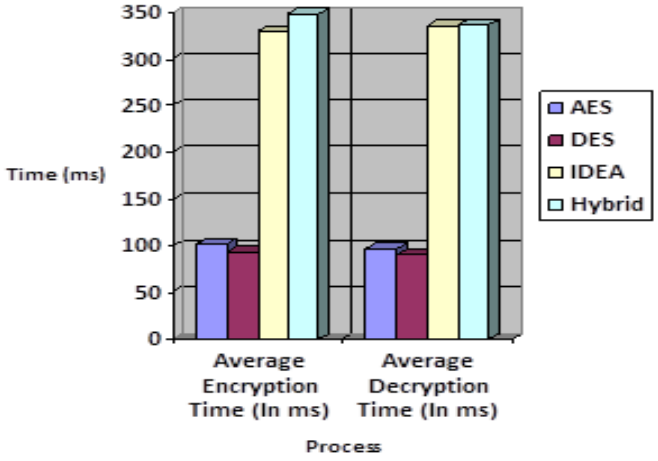

Figure 6: Graph for Encryption and Decryption Process

As per the experimental results shown in table I and in Fig. 6. The average time (in ms) taken for hybrid algorithm is bit higher as compared to AES, DES and IDEA. The DES algorithm uses 64-bit key which makes the processing time faster. The AES algorithm uses 128-bit key which slower the processing time by some margin. The IDEA algorithm also uses 128-bit key but the processing time for IDEA algorithm is higher as compared to AES and DES algorithm. The Hybrid algorithm on the other hand uses three keys out of which one key is of size 64-bit and other two keys are of size 128-bit has little bit higher processing time. From the comparison, the proposed system provides the better security compared to other algorithms at a little cost of time factor.

V. CONCLUSION

The paper shows the combination of AES, DES and IDEA algorithm to obtain the hybrid cryptography algorithm. The purpose of creating this hybrid algorithm is to provide better security to the string. The time that requires to attack the purpose system is the total time of attacking all the three algorithms as we use three key for the encryption and decryption purpose.

The different result analysis for all the different algorithms is shown in the figures. The calculated values for different algorithm and hybrid algorithm are shown. The hybrid algorithm provides more security than individual algorithms for the same plaintext. The algorithm discussed here can provide better security rattan than using individual algorithm at a time. The comparison of different parameters used for result analysis is shown in figure and highlighted in table. The comparison of time taken for encryption and decryption is shown in the tabular as well as graph format for better classification of different algorithms. The time shown here is the average time as the time depends on the processing time taken by processor.

As the algorithm combines three different cryptographic algorithms, the security of the data is improved. The proposed algorithm uses three different keys of different length for encryption and decryption process which maximize the time for the Brute-Force attack.

In the proposed system, the mode of input is string. Converting this string into binary mode and then passed for encryption and decryption purpose.

REFERENCES

[1] Bhavik Rana, Sunil Wankhade "A Comparative Study of Hybrid Cryptographic Algorithms" in International Journal of Modern Engineering Research (IJMER), vol. 6, Issue 10, Ver. 2, pp 71-75, October 2016 (ISSN: 2249-6645).

[2] M.B. Vishnu, S.K. Tiong, Member IEEE, M. Zaini, Member IEEE, S.P. Koh, "Security Enhancement of Digital Motion Image Transmission Using Hybrid AES-DES Algorithm", in *Proceedings of APCC2008 copyright © 2008 IEICE 08 SB 0083.*

[3] Jigar Chauhan, Neekhil Dedhia, Bhagyashri Kulkarni, "Enhancing Data Security by using Hybrid Cryptographic Algorithm", in *International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 2, Issue 3, May 2013.*

[4] AES.pdf [online]. Available: http://www.facweb.iitkgp.ernet.in/~sourav/AES.pdf

[5] DES.pdf [online]. Available: http://www.facweb.iitkgp.ernet.in/~sourav/DES.pdf.

[6] IDEA.pdf [online]. Available FTP: ftp://180.211.120.110/04%20IT%20Department/RNK/SE/International%20Data%20Encryption%20Algorithm.pdf

[7] Mr. Mahavir Jain,Mr. Arpit Agrawal, "Implementation of Hybrid Cryptography Algorithm", in *International Journal of Core Engineering & Management(IJCEM) Volume 1, Issue 3, June 2014.*

[8] Jignesh R Patel, Rajesh S. Bansode, Vikas Kaul, "Hybrid Security Algorithms for Data Transmission using AES-DES", in *International Journal of Applied Information Systems (IJAIS) – ISSN: 2249-0868 Foundation of Computer Science FCS, New York, USA Volume 2– No.2, February 2012.*

[9] P.G. Gopika, N. Hariharan and S. Perumal Sankar, "Hybrid AES Algorithm Using 16 Fiestel Based Network with Distinct Keys", in *Middle-East Journal of Scientific Research 24 (4): 1325-1329, 2016, ISSN 1990-9233 © IDOSI Publications, 2016. DOI: 10.5829/idosi.mejsr.2016.24.04.23301*.

[10] Anurhea Dutta, Prerna Bharti, Swati Agrawal, Surekha K S, "Hybrid AES-DES Block Cipher: Implementation using Xilinx ISE 9.1i", in *UACEE International Journal of Advancements in Electronics and Electrical Engineering Volume 1: Issue 2 [ISSN: 2319 – 7498]*.

[11] Wang Tianfu, K. Ramesh Babu, "Design of a Hybrid Cryptographic Algorithm", in *International Journal of Computer Science & Communication Networks, Vol 2(2), 277-283 277 ISSN:2249-5789*.