International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868
Foundation of Computer Science FCS, New York, USA
Volume 2– No.2, February 2012 – www.ijais.org

Hybrid Security Algorithms for Data Transmission using AES-DES

Jignesh R Patel
PG-scholar,TCET
Kandivali,mumbai
india

Rajesh S. Bansode
Asst.prof, TCET
Kandivali,mumbai
india

Vikas Kaul
Asst.prof, TCET
Kandivali,mumbai
india

ABSTRACT
The fast evolution of digital data exchange has forced the information security to be of much important in data storage and transmission. As large amount of data is transmitted over the network, it is preliminary to secure all types of data before sending them. The problem with AES, most extensively used encryption is that it uses many multi variant equations which are linear in nature. Thus it can be broken using algebraic cryptanalysis. This provides a serious threat as AES was considered to be unbreakable and thus it was used in many encryption systems.

The current paper presents the design and implementation of a hybrid based 128 bit key AES-DES algorithm as a security enhancement.

Keywords
Cipher, DES, AES, Hybrid AES DES, Key matrix.

1. INTRODUCTION
The DES (Data Encryption Standard) is a cryptographic standard. The algorithm is designed to encipher and decipher blocks of data consisting of 64 bits under control of a 64-bit key.
In cryptography, the Advanced Encryption Standard (AES) cipher has a 128-bit block size, with key sizes of 128, 192 and 256 bits, respectively.
The integration of AES with DES is to enhance security for input mode as text ,image, audio and video. The paper outlines the possible weaknesses within the current AES encryption algorithm especially against algebraic based cryptanalysis. To understand the need for minimizing algebraic attacks on AES there by the idea of integrating AES with DES is proposed. Hence the development of the Hybrid AES-DES algorithm.

1.1 Cryptanalysis of AES

AES is based on a design principle known as a Substitution permutation network. It is fast in both software and hardware. Unlike its predecessor DES, AES does not use a Feistel network[12].

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 block and key sizes in any multiple of 32 bits, with a minimum of 128 bits. The block size has a maximum of 256 bits[7].

AES operates on a 4×4 column-major order matrix of bytes, termed the *state* (versions of Rijndael with a larger block size have additional columns in the state). Most AES calculations are done in a special finite field. The AES cipher is specified as a number of repetitions of transformation rounds that convert the input plaintext into the final output of cipher text. Each round consists of several processing steps, including one that depends on the encryption key. A set of reverse rounds are applied to transform cipher text back into the original plaintext using the same encryption key[13].

The key size used for an AES cipher specifies the number of repetitions of transformation rounds that convert the input plain text into the final output, called the cipher text. The number of cycles of repetition are as follows:

- 10 cycles of repetition for 128-bit keys.
- 12 cycles of repetition for 192-bit keys.
- 14 cycles of repetition for 256-bit keys[5].

1 .2 DES
DES is the block cipher algorithm that takes a fixed-length string of plaintext bits and transforms it through a series of complicated operations into another cipher text bit string of the same length. In the case of DES, the block size is 64 bits. DES also uses a key to customize the transformation so that decryption can be performed by authentic user used to encrypt the key. The key ostensibly consists of 64 bits however only 56 of these are actually used by the algorithm. Eight bits are used solely for checking parity, and are thereafter discarded. Hence the effective key length is 56 bits, and it is never quoted as such. Every 8th bit of the selected key is discarded, that is, positions 8, 16, 24, 32, 40, 48, 56, 64 are removed from the 64 bit key leaving behind only the 56 bit key [17].

The F-function, operates on half a block (32 bits) at a time and consists of four stages:

1. Expansion — The 32-bit half-block is expanded to 48 bits using the expansion permutation by duplicating half of the bits. The output consists of eight 6-bit(8*6=48bits) chunk, each containing a copy of 4 corresponding input bits, plus a copy of the immediately adjacent bit from each of the input pieces to either side[17].

2. Key mixing — The result is combined with a sub key using an XOR operation. Sixteen 48-bit sub keys one for each round are derived from the main key using the key schedule[3].

3. Substitution — After mixing in the sub key, the block is divided into eight 6-bit pieces before processing by the S-boxes, or substitution boxes. Each of the eight S-boxes replaces its six input bits with four output bits according to a non-linear transformation, provided in the form of a lookup table. The S-boxes provide the core of the security of DES without them, the cipher would be linear, and trivially breakable[19].

4. Permutation — Finally, the 32 outputs from the S-boxes are rearranged according to a fixed permutation, the P-box. This is designed so that, after expansion, each S-box's output bits are spread across 6 different S boxes in the next round[17].

DES - The 16 Rounds

The basic process in enciphering a 64-bit data block and a 56-bit key using the DES consists of:

- An initial permutation (IP)
- 16 rounds of a complex key dependent calculation f
- A final permutation, being the inverse of IP

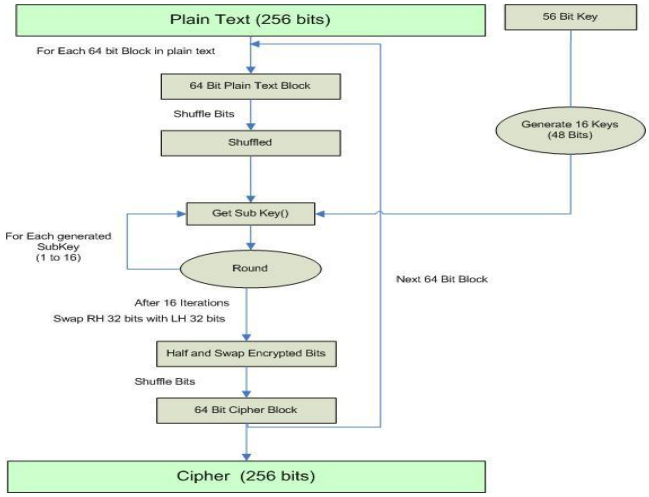

Fig. 1 DES rounds

1.3 AES

A byte in Rijndael is the basic data unit for all cipher operations. Such bytes are interpreted as finite field elements using polynomial representation, where a byte b with bits b0, b1 ,... b7 represents the finite field elements. Finite field operations like addition and multiplication are required for key scheduling and rounding. The addition of two finite field elements is achieved by adding the coefficients for corresponding powers in their polynomial representations, this addition being performed in GF(2), that is, modulo 2, so that 1+ 1 = 0. Addition is nothing but performing XOR between two expressions. Finite field multiplication is more difficult than addition and is achieved by multiplying the polynomials field generator and the remainder is taken as the result. Since there are 256 possible polynomials, a look up table can be created for a specific field generator. So the lookup table contain 256 * 256 entries [16].

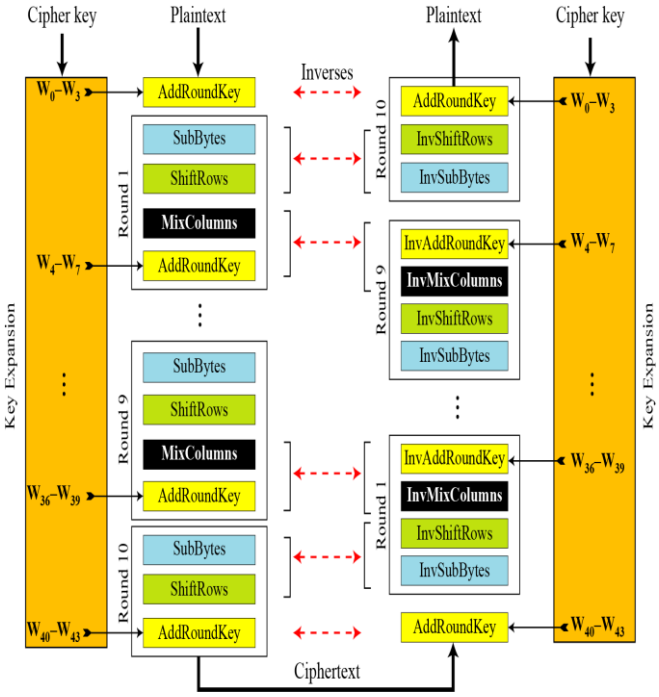

Fig. 2 AES rounds

Scheduling: The round keys are each round requiring Nc words of key data. For 128-bits keys the key scheduling operates intrinsically on blocks of four (4) 32-bits words. calculating one new round key from the previous one, denote the i^{th} word of the actual round key with K[i], where $0_i i_i 4$, and the i^{th} word of the next round key with K[i]. K[0] is computed by an XOR between K[0], a constant r (field generator) and K[3], the latter being pre rotated and transformed. The other three words K[1], K[2] and K[3] are calculated as K[i] = K[i] . K[i - 1][9].

Rounding: At the start of the cipher the cipher input is copied into the internal state using the conventions described before Fig.1. An initial round key is then added and the state is then transformed by iterating a round function in a number of cycles. The steps involved in AES are shown in Illustration 1. It is the algorithm as rinjdael suggested[4].

Round Function: One round is termed as a cycle and each cycle has four steps. Each step of transformation is described below. Add Round Key: This is the first step of transformation. The Xor Round Key function declared in Illustration 1 has to perform a bitwise Xor of the state matrix and the round key matrix[1].

Sub-Bytes : Transformation: Inverse of the state matrix is found here and a fine transformation is performed[6].

Shift Rows: The Shift Rows transformation operates individually on each of the last three rows of the state matrix by cyclically shifting the bytes in the row. The second row is

shift done time to the left, third row shifted two times and fourth rows shifted three times[3].

Mix Columns: The mix columns transformation computes the new state matrix S by left-multiplying the current state matrix S by the polynomial matrix[14].

The Advanced Encryption Standard (AES) is a block cipher which is ratified as a standard by National Institute of Standards and Technology of the United States (NIST), was chosen using a process markedly more open and transparent than its predecessor, the aging Data Encryption Standard (DES). This process won plaudits from the open cryptographic community, and helped to increase confidence in the security of the winning algorithm from those who were suspicious of backdoors in the predecessor, DES[8].

2. Hybrid AES -DES

In proposed algorithm (Hybrid AES-DES) the goal had been achieved by combining two algorithms called DES and AES.

For encryption of data:-

1. The input is consider as Text, image (.jpeg), audio (8 bit low level .wav file) or video (.avi) is being converted to 128 bit plain text.
2. Further 128 bit text is being divided into two sets of 64 bit plain text data.
3. Next this 64 bit plain text is being given as input to DES algorithm, which encrypts to give encrypted 64 bit text.
4. Such two sets of encrypted 64 bit texts are then merged as single 128 bit encrypted data, which further being applied to AES algorithm for further encryption[4].

For decryption of data:-

1. The 128 bit encrypted data is applied to AES algorithm, which provide decrypted set of 128 bit of data.
2. This one set of 128 bit of data is then further divided into two 64 bit data set.
3. These data sets are then further applied to DES algorithm to get the two decrypted set of 64 bit.
4. This two sets of 64 bit decrypted data merge into single 128 bit data.

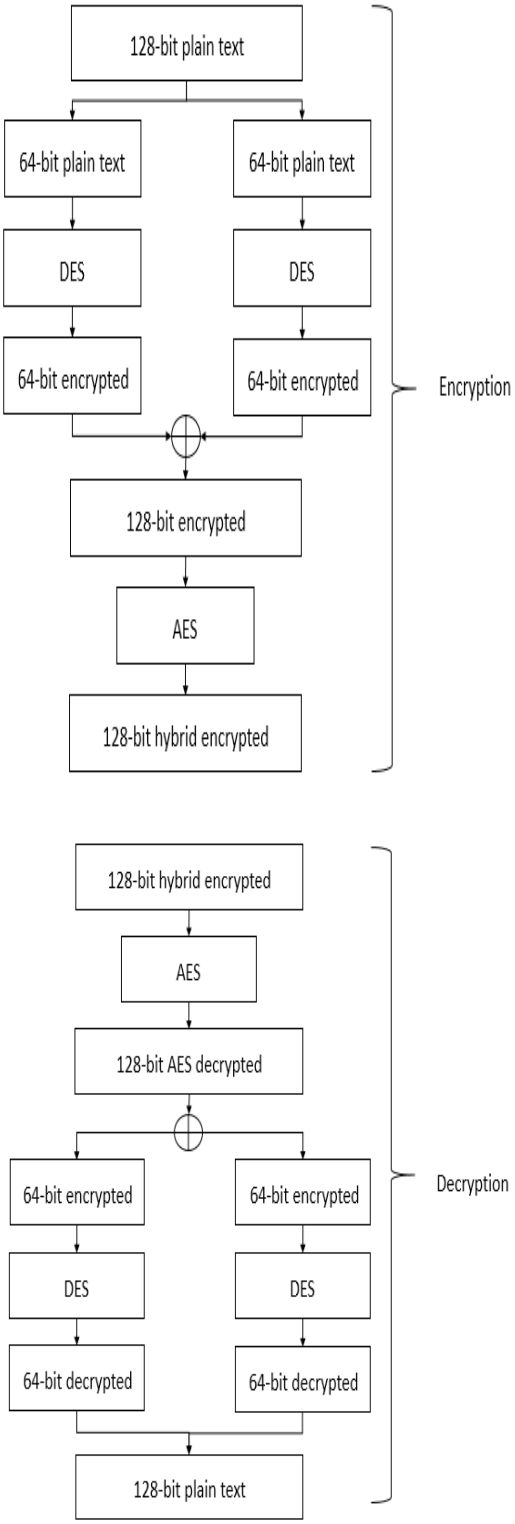

Fig. 3 Hybrid AES-DES flow

3. Implementation

In this system the implementation of DES, AES, and Hybrid AES-DES is done for comparative study so it can be easily understood that time requirement for encryption of Hybrid AES-DES is greater than that of the time requirement of individual AES and DES. The time getting during the experimental result may varies for same input because it depends upon the processor and memory available during the execution of the program. The decryption time is less because the decryption is done continuously with the encryption.

3.1 Hybrid AES-DES algorithm implemented in this snapshot for input mode (image)

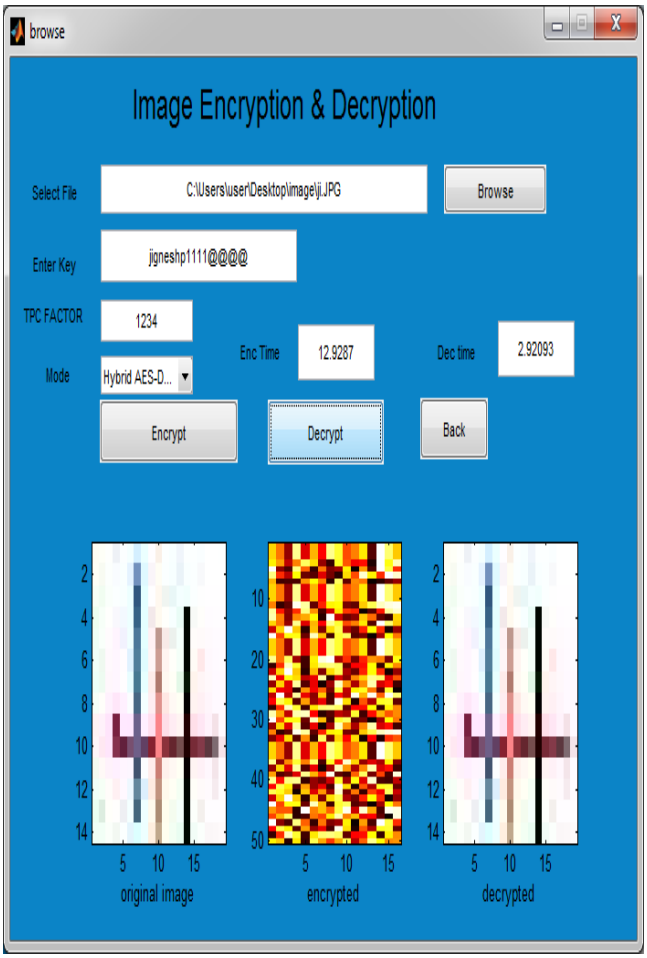

Fig.4 Snapshot for Hybrid AES-DES algorithm for input mode image

In this system the different size of images are taken as a input to the system for encryption such as 328 bits,798 bits ,3600 bits,4692 bits,5700 bits,22500 bits images and same are decrypted also images of (jpeg) format is only done for encryption and decryption.

3.2 Hybrid AES-DES algorithm implemented in this snapshot for input mode (video)

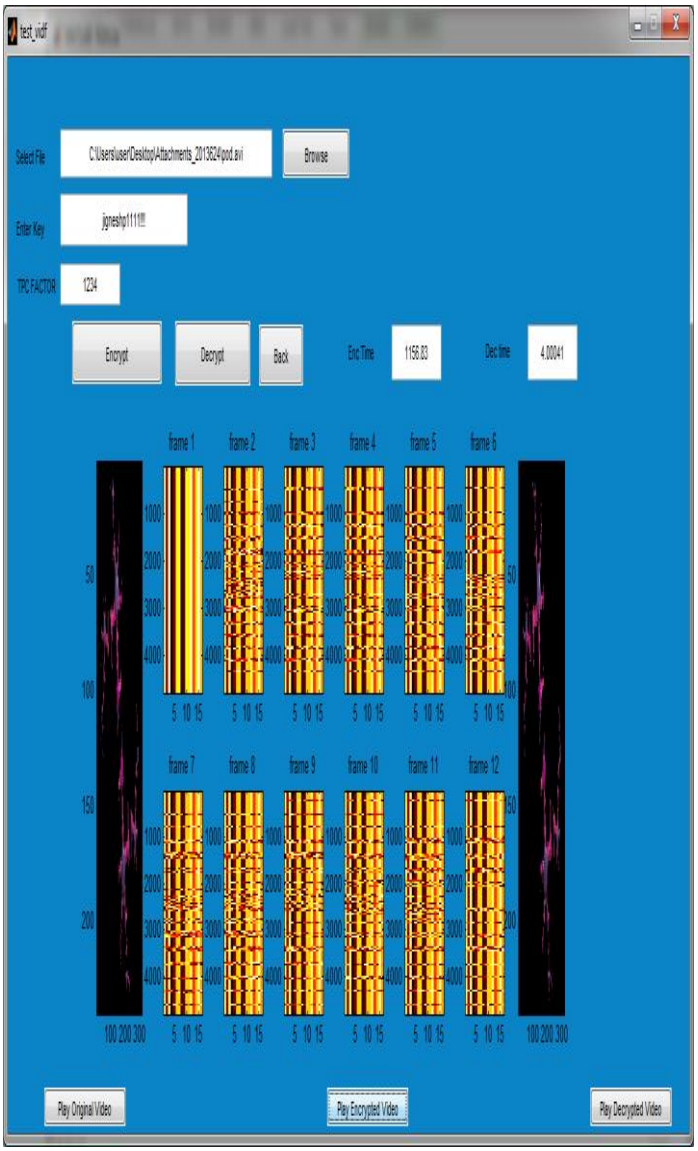

Fig.5 Snapshot for Hybrid AES-DES algorithm for input mode video

In this system only 12 frame video of size 145 Kb taken as a input to the system for encryption and decrypted the same. The decryption time is less because the decryption is done continuously with the encryption also video of (.avi) format is only done for encryption and decryption. The time require for encryption is higher because the encryption is done at bit level so the security for encrypted data is very high that it can't be easily understood by any of the attackers. The video file is divided into 12 frames and encrypted as shown in the figure and after that merging is done after decryption.

3.3 Hybrid AES-DES algorithm implemented in this snapshot for input mode (audio)

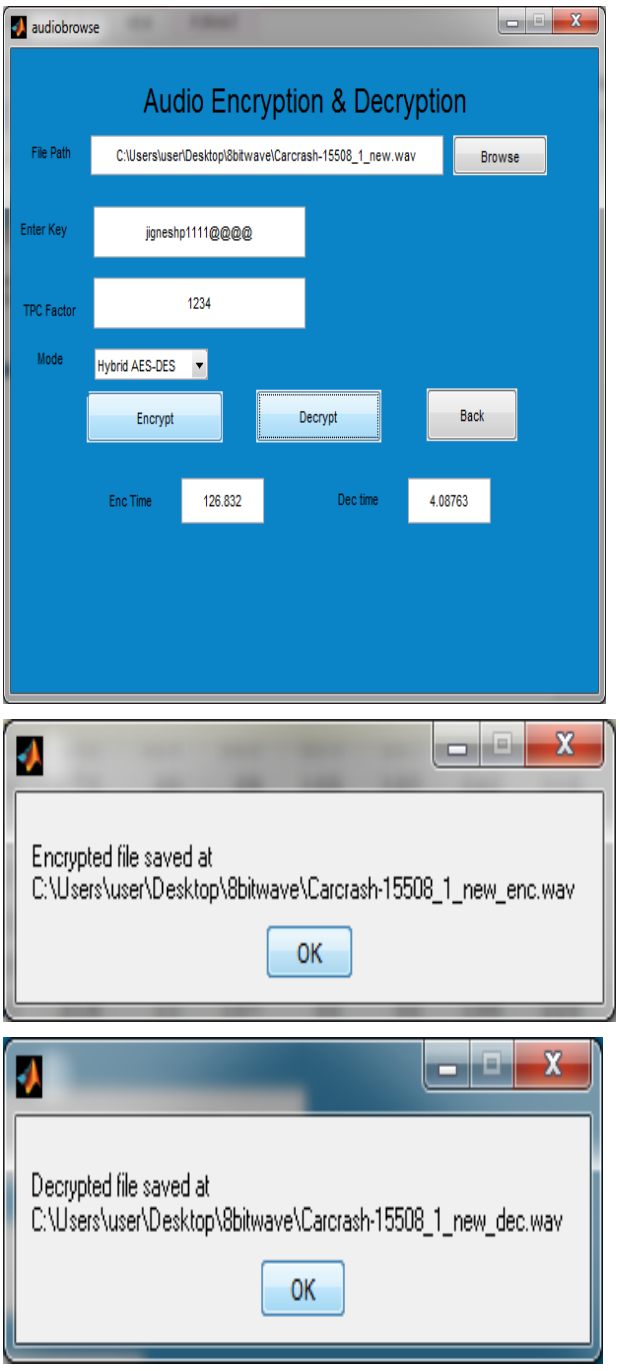

Fig.6 Snapshot for Hybrid AES-DES algorithm for input mode image

In this system the different size of audio files are taken as a input to the system for encryption such as 8.59 Kb, 9.46 Kb, 15.6Kb, 19.2Kb,19.5Kb,22.9Kb,26.7Kb and same are decrypted also audio of (8 bit low level wav file) format is only done for encryption and decryption.

4. Results and Performance Analysis

Table 1. Encryption time (average) in seconds for image (mode of input) for different number of bits

Size(Bits)	324	798	3600
DES	5.24878	14.0182	39.4617
AES	6.12828	16.7967	42.5645
Hybrid	11.1528	17.9159	50.2624

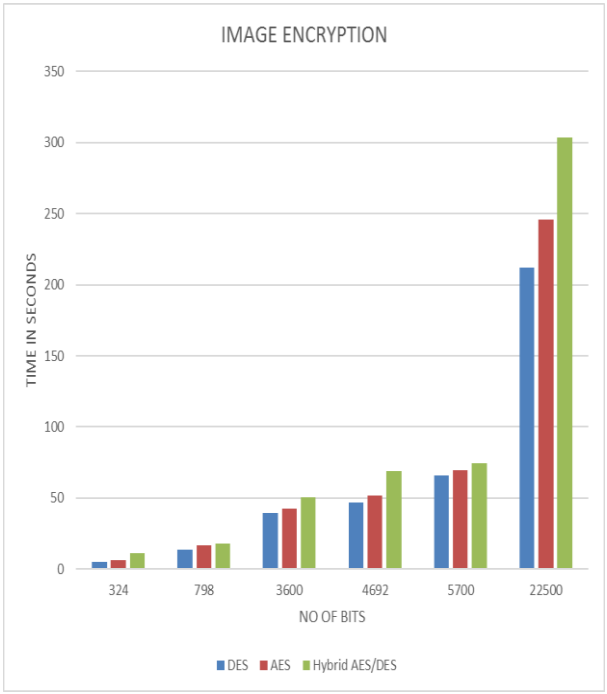

Fig. 7 Encryption time for image mode of input for different number of bits for DES,AES, Hybrid AES-DES algorithm.

Table 2. Decryption time (average) for image (mode of input) for different numbers of bits

Size(Bits)	324	798	3600
DES	2.71026	2.85587	4.84221
AES	2.66177	2.85153	3.91078
Hybrid	2.61099	2.84419	4.42111

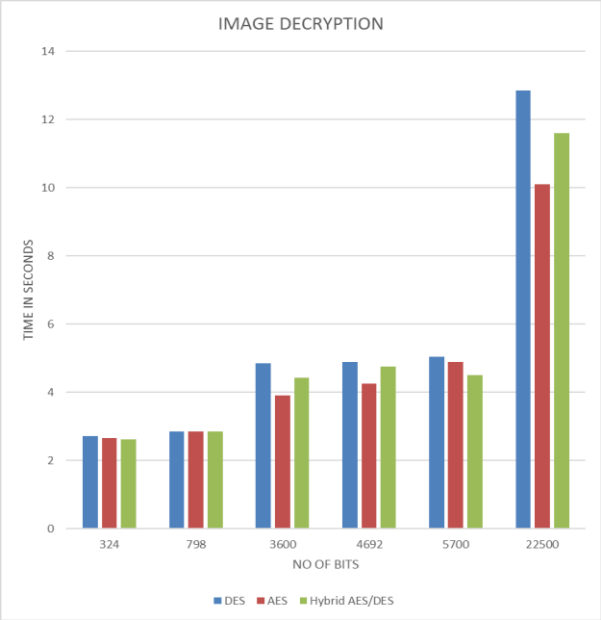

Fig.8 Decryption time for image mode of input for different number of bits for DES, AES, Hybrid AES-DES algorithm

Table 3. Encryption time (average) for audio (mode of input) for different sizes (in KB)

Size(KB)	8.59	9.46	15.6
DES	102.63	144.052	236.211
AES	114.584	150.953	240.747
Hybrid	133.459	155.421	245.3467

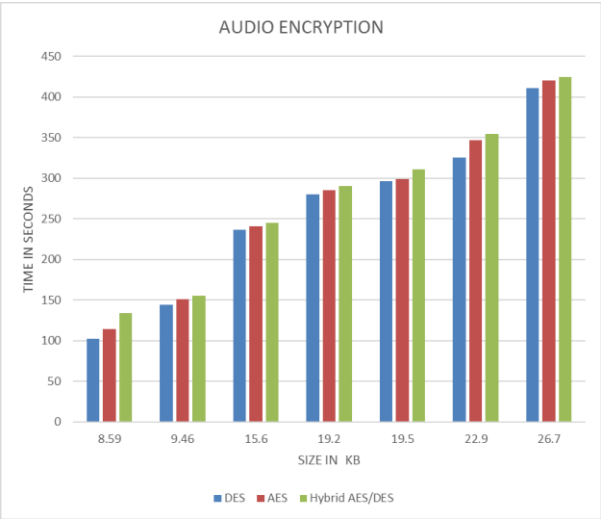

Fig. 9 Encryption time for audio mode of input for different size of wav file for DES, AES , Hybrid AES-DES algorithm

Table 4. Decryption time (average) for audio (mode of input) for different sizes (in KB)

Size(KB)	8.59	9.46	15.6
DES	4.00382	4.00412	4.00451
AES	4.0038	4.00385	4.00485
Hybrid	4.00366	4.00375	4.0045

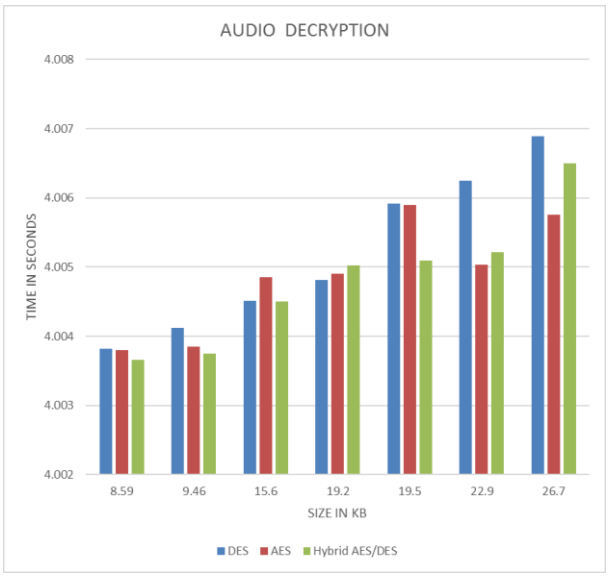

Fig. 10 Decryption time for audio mode of input for different size of wav file for DES, AES , Hybrid AES-DES algorithm

5. Conclusion

An improved Hybrid AES-DES algorithm as means of strengthening the current AES architecture. The hybrid model gives a better non linearity to the plain AES and as it is merged with DES there is better diffusion hence the possibility of an algebraic attack on the hybrid model is reduced.

Also the time shown on the analysis are average time because the time may vary depend upon the processor availability and processor speed. one can't get the different time for same input for encryption as well as decryption because of same.

In this algorithm the image are only for (jpeg) file format is supported and audio file for (8 bit low level wav file) format is supported and video only (avi) format is supported.

In this system applying different algorithm like DES, AES & Hybrid AES-DES for text , image ,audio and only hybrid algorithm for video mode of input.

In this algorithm key is not in valid format then error report is generated. The key format is 16 character key with 8 characters 4 numbers and 4 special characters are there for validation.

Being a hybrid of two powerful encryption standards the algorithm will act as efficient and reliable encryption technique for data. The proposed algorithm can also use a double key approach which makes it resistant to linear attacks. In this case, the safety of encryption algorithm can be further improved Improving DES by adding the irrational number and integrating the AES algorithm into DES structure to further improve its security.

In this system the mode of inputs are different like text, image, audio and video. Converting this mode in binary mode and taken as input to the system and on this apply the encryption and decryption.

6. ACKNOWLEDGMENTS

Our thanks to the experts who have contributed towards development of the template.

7. REFERENCES

[1]Carlos Cid, Sean Murphy and Matthew Robshaw,2004 "Computational and Algebraic aspects of the Advanced Encryption Standard", In Proceedings of the Seventh International Workshop on Computer Algebra in Scientific Computing .

[2] Aida Janadi, 2008 " AES immunity Enhancement against algebraic attacks by using dynamic S-Boxes", Information and Communication Technologies from Theory to Applications, ICTTA2008.

[3] Jing Wang & Guo-ping Jiang, 2008 "Improved DES algorith based on irrational number", IEEE Int. Conference Neural Networks & Signal Processing.

[4] M.B. Vishnu & S.K. Tiong, 2008 "Security Enhancement of Digital Motion Image Transmission Using Hybrid AES-DES Algorithm", IEEE Int.

[5] Tingyuan Nie, 2009 "A Study of DES and Blowfish Encryption Algorithm".

[6] Yuan Kun, Zhang HanLi Zhaohui, 2009 "An Improved AES algorithm based on chaos",Multimedia Information NetworkingandSecurity,INES'09.International Conference.

[7] Tingyuan Nie, Chuanwang Song, Xulong Zhi, 2010 " Performance Evaluation of DES and Blowfish Algorithms", Biomedical Engineering and Computer Science International Conference.

[8] Xiang Li, Junli Chen, Dinghu Qin, Wanggen Wan. 2010 " Research and Realization Based on hybrid encryption algorithm of improved AES and ECC", Audio Language and Image Processing (ICALIP).

[9] M.Zeghid , M.Machhout, L. khriji, A.baganne and R.Tourki, 2007 "A modified AES based algorithm for image encryption ",World Academy of Science ,Engineering and Technology .

[10] Abdinasir hasan Ali, "Analysis and implementation of security algorithms for wireless communication", IEEE, 2010.

[11] Craig Teegarden,Mudit Bhargava,Ken mai, 2010 "Side channel attack Resistant ROM based AES S-Box", IEEE Int.

[12] Manhee Lee, Student Member, IEEE, and Eun Jung Kim, Member, IEEE Computer Society, 2007 "A Comprehensive Framework for Enhancing Security in InfiniBand Architecture",IEEE Int.

[13] H. Nover, 2005 "algebraic cryptanalysis of aes: overview", university of wisconsin, usa,.

[14] S. Murphy, mj.b robshaw, 2002 "essential algebraic structure within the aes", advances in cryptology crypto 2002, lecture notes in computer science, springer-verlag.

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

[16] AES Description, Available: http://people.eku.edu/styere/Encrypt/JS-AES.html

[17] DES Description, Available: http://orlingrabbe.com/des.htm

[18] AES mix column http://www.angelfire.com/biz7/atleast/mix_columns.pdf

[19] Forouzan Behrouz "Cryptography & Network Security",McGraw-Hill Forouzan Networking , 2007.