Encrypted Security Technique by using Cubical Efficient Block Cipher Method

Pooja Singh[1] Sunil Singh[2] Satish Kumar Soni[3] Prof. Anubhav Pandey[4]
[1,2,3]M. Tech Student [4]Professor
[1,2,4]JNCT REWA, India [3]RIT REWA, India

Abstract— Cryptography plays a vital role in information security. during digital exchange of information, this can be necessary technique; data shouldn't be access by an unrecognized user. Cryptography schemes are rely on symmetric and asymmetric encoding. Researchers worked on secure and efficient information transmission and presented numerous crypto graphical techniques. For secure information broadcast over the network, it is needed to use correct encoding technique .Symmetric encryption is extensively used technique .During this article, we are representing an efficient block cipher encoding techniques depend upon cubical technique and improved key. Planned AESD technique is based on block level symmetric encoding. A combine of binary inputs are contains by every cell. The Cube will able to give a numerous variety of combinations, by that system can generate a powerful cipher text. For efficient and powerful cipher, proposed technique uses shuffling of bits in cube. Planned AESD rule, performed a series of bit transformations, by using of S -BOX, operation XOR, and operation AND. The performance analysis of projected encoding technique area unit compared with different existing symmetric encryptions ways, primarily based on block cipher encoding ,such as encoding normal, 3-Data encoding normal, Advance encoding standard, and blowfish fish, supported numerous comparison parameters like encoding and decoding time, Avalanche impact and cipher text size .Simulation results clearly shows that projected technique performs outstanding in terms of encoding and decoding time, Avalanche impact and size, as compared to existing strategies.

Keywords: Encryption, Decryption, Block Cipher, DES, AESD, 3-DES, AES, Blowfish and Encryption

I. INTRODUCTION

Day by day, the importance and the data value of exchanged over the network, Internet or other any media types are constantly increasing. Researchers are the continuously researching, for the best probable data security solution. That offers the best possible security protection against the various data thieves' attacks. Still it is challenging, for researchers to provide such important security services under timely manner. It is one of the most active research areas in the field of data and network security related communities. Along with over the past decades, computer science and information technology has infiltrated more and more areas of our society [6, 3, 4].

II. EXISTING BLOCK CIPHER METHODS

1) DES- (Data Encryption Standard), was the first encryption standard to be recommended by NIST (National Institute of Standards and Technology).DES is (64 bits key size with 64 bits block size) .Since that time, many attacks and methods recorded the weaknesses of DES, which made it an insecure block cipher [7].
2) Triple DES- 3DES is an enhancement of DES; it is 64 bit block size with 192 bits key size. In this standard, the encryption method is similar to the one in the original DES but applied 3 times to increase the encryption level and the average safe time. It is a known fact that 3DES is slower than other block cipher methods[6,7]
3) AES- AES is a variable bit block cipher and uses variable key length of 128, 192 and 256 bits. If both the block length and key length are 128 bits, AES will perform 9 processing rounds. If the block and key are of 192 bits, AES performs 11 processing rounds. If the block and key are of length 256 bits then it performs 13 processing round [2].Encryption is said to occur when data is operated through a series of mathematical operations that produce an alternate form of that data; the sequence of these operations is called an algorithm. To help distinguish between the two forms of data, the unencrypted data is referred to as the plaintext and the encrypted data as ciphertext. The security of encryption lies in the ability of an algorithm to generate ciphertext that is not easily reverted to the original plaintext .In a very simple example, encryption of the word "secret" could result in "terces." Reversing the order of the letters in the plaintext generates the ciphertext. This is a very simple encryption - it is quite easy for an attacker to retrieve the original data. A better method of encrypting this message might be to create an alternate alphabet by shifting each letter by some arbitrary number. Encryption is an important mechanism for modern life as We perform many transactions over internet thus to secure Data it is necessary to convert the data in unreadable Format so no one can read it.
4) BLOW FISH-Blowfish was developed by Bruce schneier in 1993. It is a symmetric block cipher having variable length key from 32 bits to 448 bits. It operates on block size 64 bits[14]

III. DIFFICULTIES

Based on literature survey following, problems are acknowledged [1,2,8]-

1) Higher Encryption and Decryption time-Existing methods have higher encryption and decryption time.
2) Avalanche Effect-Existing methods have less effect.
3) Not support various data formats- Existing methods are not able to convert all types of file formats such as text, image, audio, and video files.

IV. OBJECTIVE OF THE PAPER WORK

The main objective of the work is to generate an efficient encryption and decryption method for various file formats. Proposed encryption scheme will achieves the following-

1) The type of operations used for transforming plain text to cipher text- Achieved efficient selection of substitution and transposition elements, by proposed EES Method.
2) Achieved efficient encryption and decryption time- Perform fast encryption and decryption, as compared to existing block cipher symmetric encryption methods such as DES, AES, 3-DES and Blowfish.
3) Memory used- Use less memory space as compared to existing block cipher symmetric encryption methods
4) Achieved best Avalanche effect-To achieved higher avalanche effect, as compared to existing block cipher symmetric encryption methods such as DES, AES, 3-DES and Blowfish.

V. PROPOSED EES METHOD

KEY GENERATION()- This proposed EES_key_generation function, takes input key string of size up to 64 bit from user, and produces a strong key of size128 bit. It uses following functions-

– Key_add ( ) - This function converts user string in to 64 bit string
– Key_expansion ( ) - This function expand 64 bit input (64 bit output by, Key_add()), in to its equivalent key K128 with size 128 bits.
– Key Mixing(Key_128)- Proposed EES method use two types kinds of key mixing process, called Forword_KM and Backword_KM.

AESD_Substition_function( )- This function performed, bitwise operations are performed on values of sub-blocks to change their properties.

AESD_encryption()-It takes input a block of size 128 bit, and a user private key length up to 128 bit. Private Key, K_128, generated by key_generation (). Send this plain text and keys to substation function. Finally, XORed operation is performed to generate cipher text.

1) Select the plain text PT
2) Divides the input PT in to equal size block of 128-bits, equal to the key length K
3) Call Key Mixing ( )-
   The keys mixer function, mixes the input 128 bit key and generates Key_128_mix, and Send results to AESD Substition function
4) The result of step 3 above will be the key,
5) Call Key Mixing (Key_128)
6) Performed XOR operation-
7) CT= PT_128 XoR Key Mixing(Key_128)

Decryption process is just reverse of encryption process.

VI. RESULT ANALYSIS

In this work various block cipher based encryption methods such as AES, DES, 3-DES, Blowfish and proposed AESD implemented, and following results are calculated.

A. Encryption time for Text File

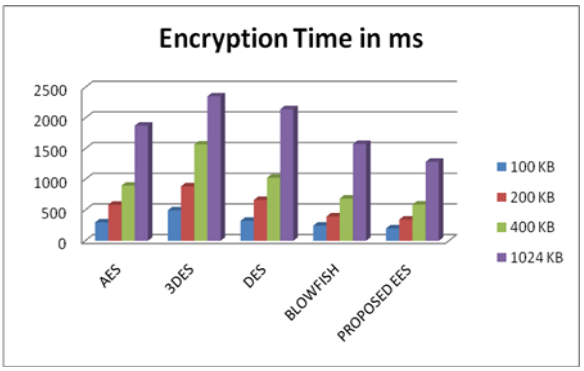

Fig. 6.1 Encryption time for text files

1) Throughput of Encryption for Different Text File Size-

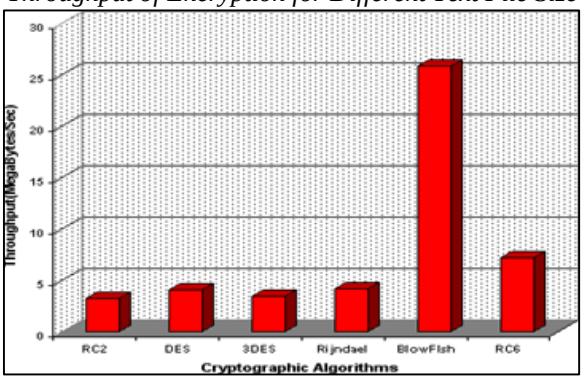

Fig. 6.1: Throughput of Encryption for Different Text File Size

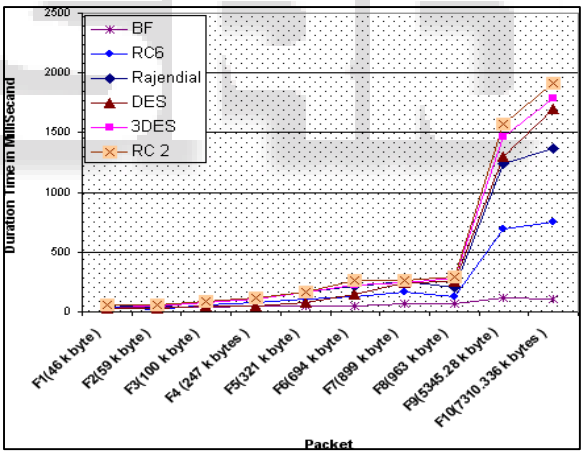

Fig. 6.2: Encryption time for PDF files

2) Decryption of the PDF Files

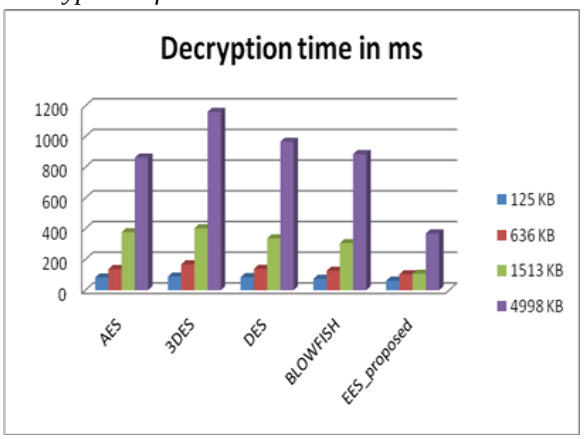

Fig. 6.3: Decryption time for PDF files

3) Encryption of the Audio Files

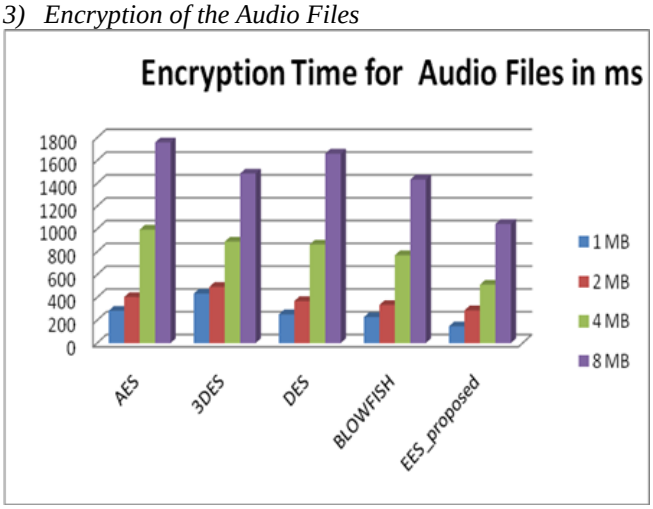

Fig. 6.4: Encryption time for PDF files

4) Encryption of the Video Files

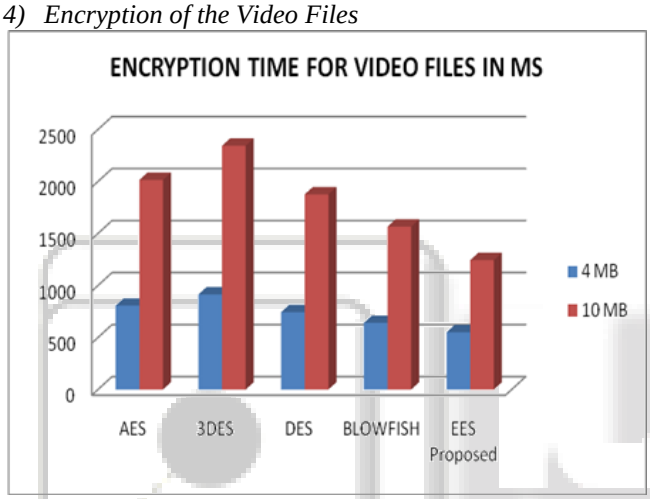

Fig. 6.5: Encryption time for Video files Avalanche Effect %-

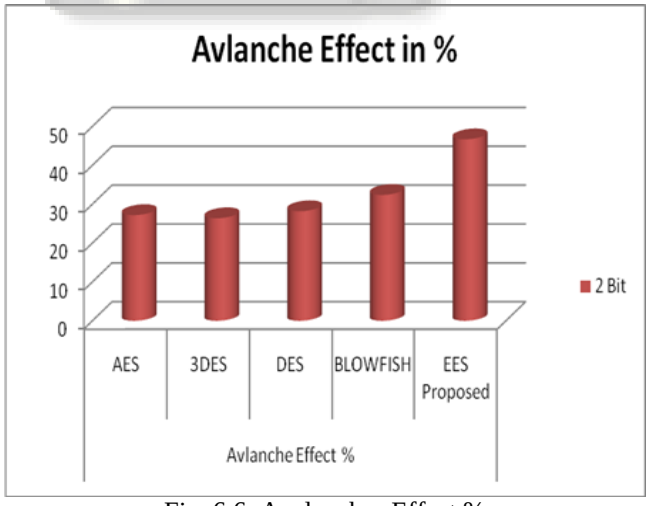

Fig. 6.6: Avalanches Effect %

B. Influence

The above result 6.1 to 6.7 shows performance comparison in between AES, DES, 3- DES, Blowfish and Proposed AESD. Above graphs clearly shows that proposed EES method have better encryption, decryption time for various files formats such as Text, PDF, Audio, Video. Better avalanche effect % as compared to existing methods.

VII. Conclusions & Future Work

By acting algorithms depend upon parameter Avalanche impact AESD scores most, we are able to conclude that AESD are often utilized in applications wherever confidentiality and integrity is of highest priority. Evaluating DES, 3DES, AES, Blowfish and planned EES. The given simulation results showed that our EES algorithmic program features a better performance than alternative common encoding algorithms used. Since it's not any known security weak points up to now, this makes it a superb candidate to be thought-about as a regular encoding algorithm.

In this thesis we've tried to reduce the encoding time which is main target of my work however during this algorithmic program we have a tendency to used only fastened matrices attributable to this the algorithmic program time remains high and in future we'll create identical algorithmic program for the twenty seven X twenty seven matrices for reducing the time and increasing the reliability of encryption.

References

[1] Guy-Armand Yandji, Lui Lian Hao,"Research on a normal file encryption and decryption", IEEE conference, PP 978-982, 2017.

[2] Manju Rani,Dr. Sudesh Kumar,"Analysis on Different Parameters of Encryption Algorithms for Information Security", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 8, PP 104-108,August 2015.

[3] P Verma, Ritu Agarwal, Dhiraj Dafouti, Shobha Tyagi," Peformance Analysis Of Data Encryption Algorithms", IEEE conference, PP 542-547, 2016.

[4] Sharad Boni,Jaimik Bhatt,Santosh Bhat," Improving the Diffie-Hellman Key Exchange Algorithm by Proposing the Multiplicative Key Exchange Algorithm", International Journal of Computer Applications (0975 – 8887)Volume 130, No.15, PP 7-11,November-2015.

[5] Manju Rani,Dr. Sudesh Kumar,"Analysis on Different Parameters of Encryption Algorithms for Information Security", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 8, PP 104-108,August 2015.

[6] Priyadarshini Patil, Prashant Narayankar, Narayan D G , Meena S M, "A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish", Science Direct, Elsevier, International Conference on Information Security & Privacy (ICISP), 11-12 December 2017, Nagpur, INDIA, PP 617-624, 2017.

[7] Swati Kashyap, Er. Neeraj Madan,"A Review on: Network Security and Cryptographic Algorithm", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 4, PP 1414-1419, April 2015.

[8] Prakash Kuppuswamy, Saeed Q. Y. Al-Khalidi," Hybrid Encryption/Decryption Technique Using New Public Key and Symmetric Key Algorithm", MIS Review, Vol. 19, No. 2, pp. 1- 13, March (2014).

[9] Dharitri Talukdar, "Study on symmetric key encryption: An Overview", International Journal of Applied Research, PP 543-546, 2015.
[10] Rajesh R Mane," A Review on Cryptography Algorithms, Attacks and Encryption Tools", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 3, Issue 9, PP 8509-8515, September 2015.
[11] Dharitri Talukdar, Prof (Dr.) Lakshmi P. Saikia," A Review On Different Encryption Techniques: A Comparative Study", International Journal of Engineering Research and General Science Volume 3, Issue 3, PP 1622-1626,May-June, 2015.
[12] Obaida Mohammad Awad Al-Hazaimeh,"A new approach for complex encrypting and decrypting data", International Journal of Computer Networks & Communications (IJCNC) Vol.5, No.2, PP 96-105, March 2013.
[13] Rajdeep Bhanot and Rahul Hans, "A Review and Comparative Analysis of Various Encryption Algorithms", International Journal of Security and Its Applications, Vol. 9, No. 4, pp. 289-306, 2015.
[14] Rashmi A. Gandhi,Atul M. Gosai,"A Study on Current Scenario of Audio Encryption", International Journal of Computer Applications (0975 – 8887) ,Volume 116, No. 7, April 2015.
[15] Dhishan Dhammearatchi," Particlemagic: need for quantum Cryptography research in the south Asian region", International Journal of Artificial Intelligence & Applications (IJAIA) Vol. 6, No. 5, PP 99-109, September 2015.
[16] Harsh Mathur, Prof.Zahid Alam," Analysis In Symmetric And Asymmetric Cryptology Algorithm", International Journal of Emerging Trends & Technology in Computer Science, Volume 4, Issue 1, PP 44-47,January-February 2015.
[17] Pranjala G Kolapwar," An improved geoencryption algorithm in location based services", International Journal of Research in Engineering and Technology, eISSN: 2319-1163, Volume: 04 Issue: 05,547-551, May-2015.
[18] Rupinder Kaur, Dr. Madhu Goel,"Effective Symmetric Key Block Ciphers Technique for Data Security: RIJNDAEL", International Journal of Science, Engineering and Technology Research (IJSETR), Volume 3, Issue 7,PP 224- 228, July 2014.
[19] Soheila Omer AL Faroog Mohammed Koko, Dr.Amin Babiker A/Nabi Mustafa," Comparison of Various Encryption Algorithms and Techniques for improving secured data Communication", IOSR Journal of Computer Engineering, Volume 17, Issue 1, Ver. III, PP 62-69, Feb. 2015.
[20] Neha,Paramjeet Singh, Shaveta Rani, "Optimal Keyless Algorithm for Security", International Journal of Computer Applications (0975 – 8887),Volume 124 - No.10,PP28-33,, August 2015.

