IJCSE International Journal of Computer Sciences and Engineering Open Access
Survey Paper Vol.-7, Special Issue, 6, March 2019 E-ISSN: 2347-2693

# A Brief Study on AES Technique With Double and Triple Block Cipher

**P. Lakshmi Devi[1*], K. Madhusudhan Reddy[2]**

[1,2]Dept. of MCA, Srikalahastiswara Institute of Information and Management Sciences, S.V.University, Tirupati, India

*Corresponding Author: pothapulakshmi096@gmail.com*

DOI: https://doi.org/10.26438/ijcse/v7si6.7376 | Available online at: www.ijcseonline.org

***Abstract***— Cryptography plays an important role in data security. During digital exchange of data, it is important; data should not be access by an unauthorized user. Cryptography methods are based on symmetric and asymmetric encryption. It is challenging researchers to find out advanced encryption security development algorithm. Cryptography techniques are based on, symmetric key or private key and asymmetric key or public key. Researchers worked on secure and efficient data transmission and presented various cryptographic techniques. For secure and efficient data transmission over the network, it is necessary to use correct encryption method. Symmetric encryption is widely used technique. In this research work, we are presenting an efficient block cipher encryption techniques based on triple method and improved key.

Proposed AESD method is based on block level symmetric encryption. The proposed AESD method is based on improve cubes. A pair of binary inputs are contains by each cell. The Cube can able to provide a various number of combinations, by that system will generate a strong cipher text. For efficient and strong cipher, proposed technique uses shuffling of bits in cube. Proposed AESD algorithm, performed a series of bit transformations, by using of S-BOX, operation XOR, and operation AND. The performance analysis of proposed encryption technique are compared with different existing symmetric encryptions methods, based on block cipher encryption, such as Data encryption standard, 3-Data encryption standard, Advance encryption standard, and blowfish fish, based on various comparison parameters such as encryption and decryption time, Avalanche effect and cipher text size. Simulation results clearly shows that proposed method performs outstanding in terms of encryption and decryption time, Avalanche effect and size, as compared to existing methods.

***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 continuously increasing. Researchers are the continuously researching, for the best possible 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

## II. RELATED WORK

**DES- (Data Encryption Standard)**
DES is 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.

**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.

**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.

**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.

 

**PROBLEM SATEMENT**

Based on literature survey following, problems are identified

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

**OBJECTIVES**

1. The main objective of the work is to develop an efficient encryption and decryption method for various file formats. Proposed encryption scheme will achieves the following-
2. The type of operations used for transforming plain text to cipher text- Achieved efficient selection of substitution and transposition elements, by proposed EES Method.
3. 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.
4. Memory used- Use less memory space as compared to existing block cipher symmetric encryption methods
5. 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.

## III. METHODOLOGY

**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.

## IV. ALGORITHM

**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 input128 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.

## V. 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.

Encryption time for Text File-

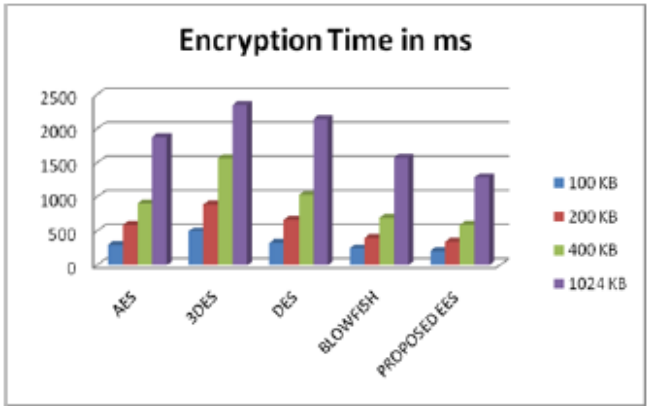


***Figure 1: Encryption time for text files***

Throughput of Encryption for Different Text File Size-

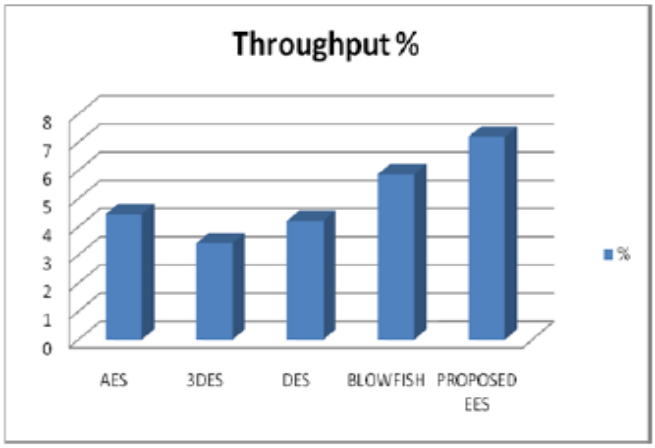


***Figure 2: Encryption time for text files***

 

Encryption of the PDF Files-

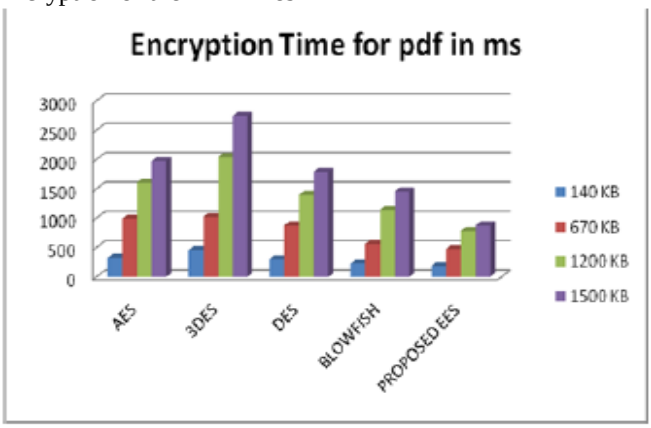


***Figure 3: Encryption time for PDF files***

Decryption of the PDF Files-

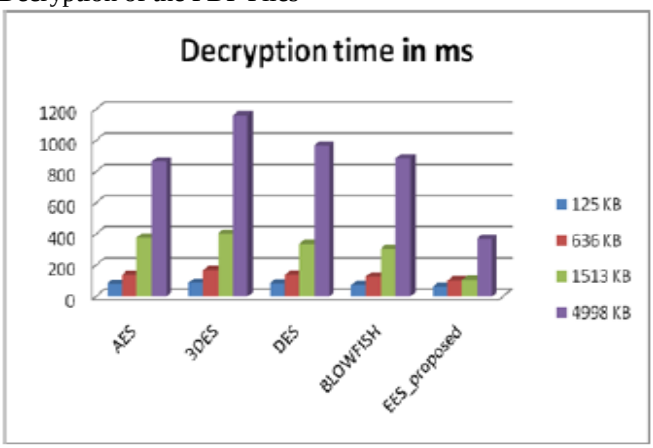


***Figure 4: Decryption time for PDF files***

Encryption of the Audio Files

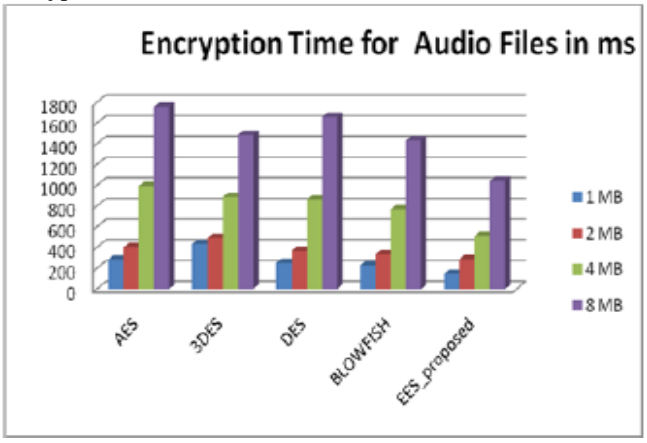


***Figure 5: Encryption time for PDF files***

Encryption of the Video Files-

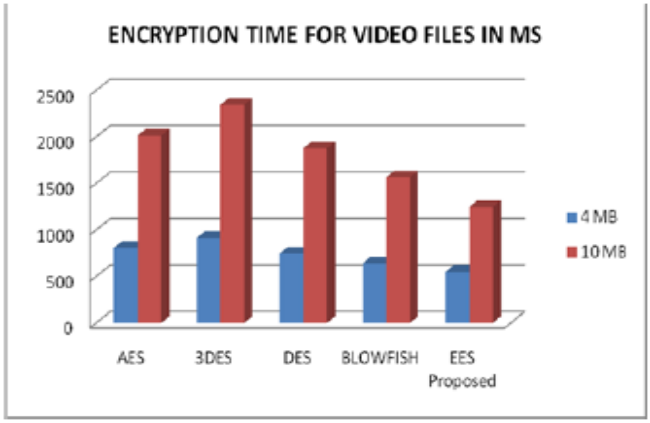


***Figure 6: Encryption time for Video files***

Avalanche Effect %-

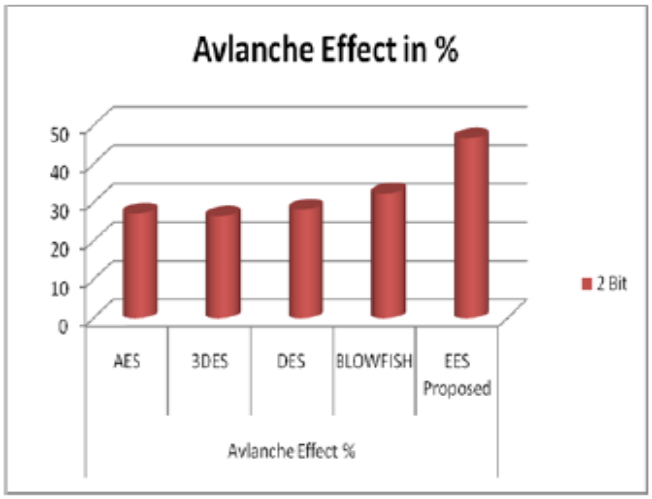


***Figure 7: Avalanches Effect %***

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.

## VI. CONCLUSION AND FUTURE SCOPE

After evaluating algorithms based on parameter Avalanche effect AESD scores highest, we can conclude that AESD can be used in applications where confidentiality and integrity is of highest priority. Evaluating DES, 3DES, AES, Blowfish and proposed EES. The presented simulation results showed that our EES algorithm has a better performance than other common encryption algorithms used. Since it has not any known security weak points so far, this makes it an excellent candidate to be considered as a standard encryption algorithm.

 

In this dissertation we have tried to reduce the encryption time which is main target of my work but in this algorithm we used only fixed matrices because of this the algorithm time is still high and in future we will make the same algorithm for the 27 X 27 matrices for reducing the time and increasing the reliability of encryption.

## REFERENCES


[1] 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.

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

[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] 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.

[7] 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).

[8] Dharitri Talukdar, "Study on symmetric key encryption: An Overview", International Journal of Applied Research, PP 543-546, 2015.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] Pahrul Irfan, Yudi Prayudi,Yogyakarta,Imam Riadi, Image Encryption using Combination of Chaotic System and Rivers Shamir Adleman (RSA)", International Journal of Computer Applications (0975 -8887)Volume 123 ,No.6, August 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 geo-encryption 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.


## Authors Profile

**P. LAKSHMI DEVI** received his Graduate Degree in B.Sc. Computer Science from Sri Venkateswara University, Tirupathi in the year of 2013-2016. Pursuing Master of Computer Applications from Sri Kalahastiswara Institute of Information and Management Sciences, Sri Kalahasti, Affiliated to Sri Venkateswara University, Tirupathi in the year 2016-2019.

**K. MADHU SUDHAN REDDY** received Master of Computer Applications (MCA) from Sri Venkateswara University, Tirupathi. She has over 3 Years of teaching experience in the area of computer Science and she has published papers at various International Conferences and research interests include Internet Technologies, Operating System, Software Engineering. Currently, he has been working as an Assistant Professor in the Department of MCA from Sri Kalahastiswara Institute of Information and Management Sciences, Sri Kalahasti.

 