ISSN No:-2456-2165

Cipher Block Chaining Mode Using AES

Pavan A. C[1], Shweta. S. Magadum[2]
[1, 2]Assistant Professor, Department of Computer Science,
KLE Society's S.Nijalingappa College, Bengaluru.

Abstract:- The main objective of data transfer is providing good security to data and faster data encryption, communication and decryption. In this paper we find out how encryption process and decryption process can be done faster by splitting the original message to bigger block sizes. AES algorithm is designed to provide more security by doing higher value encryption and decryption. By this methodology we can provide more security to the data and the time can be consumed by dividing the block sizes to larger size than 64 bits.

Keywords:- *DES, AES, Cipher Block Chaining, Security.*

I. INTRODUCTION

Data Security for the communication of data is very much necessary resource in the cryptography. For the security purpose hiding of data using encryption algorithms is important. Even though after using encryption algorithms there are many issues related to security and time consumption. So, better encryption algorithms [3] have to be selected while using them.

The technique of converting original readable message to hidden unreadable message is said as encoding and the reverse of it i.e., unreadable text to readable text is said decoding. These algorithms can be divided into 2 types: symmetric and asymmetric algorithms. Symmetric algorithm uses single key to encrypt and decrypt.

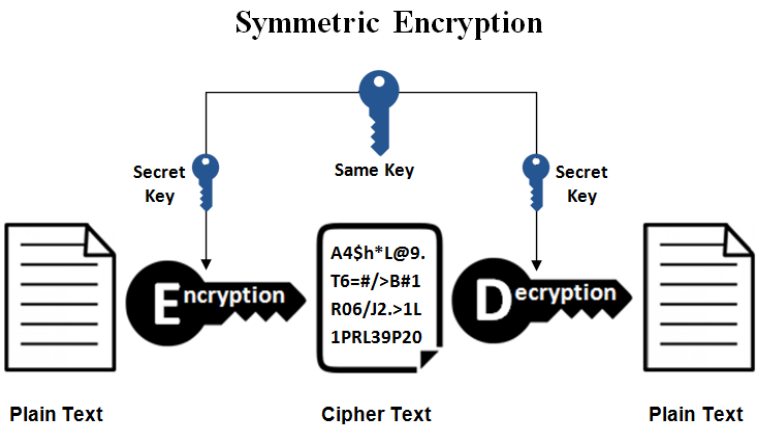

Fig 1

These ciphers can be of stream ciphers and block ciphers. Stream cipher uses 1 byte at one time to encrypt and decrypt. A Block cipher uses different block size of fixed size to encrypt and decrypt.

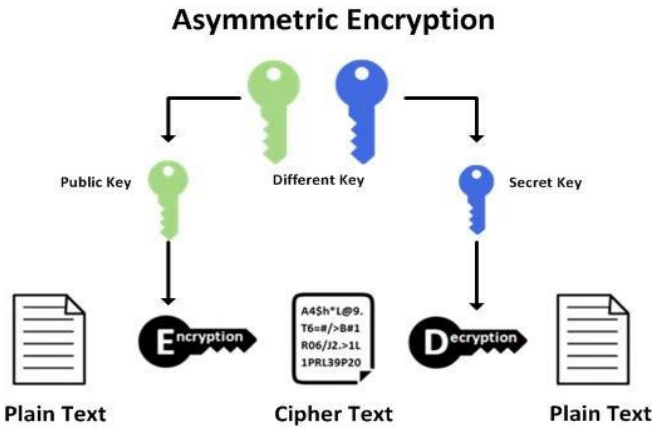

Fig 2

Asymmetric key uses 2 keys, one for encryption and another for decryption. Apart from these algorithms we also have another cryptographic algorithm know as Cipher Block Chaining mode [5-7]. There are multiple types of Cipher Block Chaining mode called as Electronic Code Book (ECB), Cipher Block Chaining (CBC), Cipher Feedback Block (CFB) and Output Feedback Block (OFB). For ECB we should provide a key and for CBC, CFB and OFB we should provide an initialization vector and a key.

II. EXISTING SYSTEM

We have many algorithms for encrypting and decrypting in which cryptographic algorithms are a type. In cryptographic algorithms like Cipher Block Chaining mode, the original message will be divided into multiple blocks of a particular block size. These cryptographic algorithms have an encryption process for each block which can be any algorithm [8]. In the existing system it said that for every block encryption process DES algorithm is used.

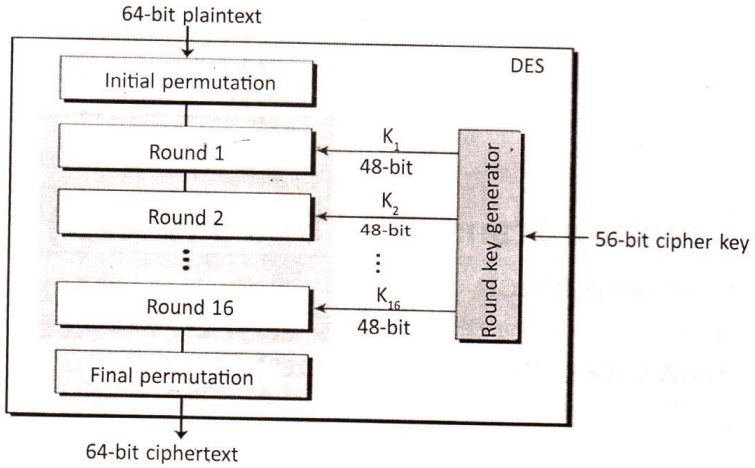

Fig 3:- DES General Structure

The message block size in DES algorithm is 64bits and after encryption the cipher block size will be 64bits. The key used in this algorithm is of the size 56bits. DES algorithm [1-2] is a good algorithm because it used 16 rounds of encryption process. Each round contains mainly 2 operations: Mixing and swapping.

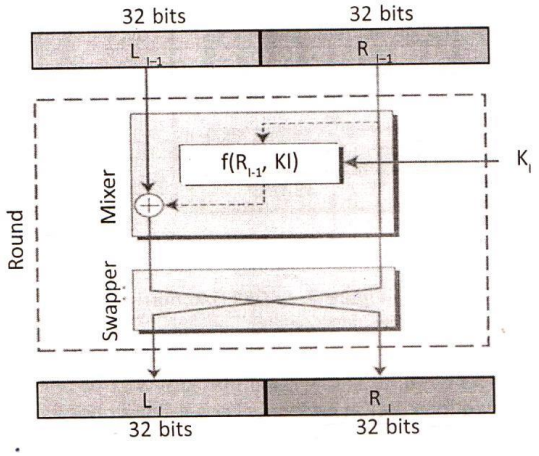

Fig 4:- Rounds in DES

The cipher block chaining [4] mode is a process of encrypting and decrypting the information which is applied on a block of data as shown in Fig 5. The input block of data is separated in to multiple blocks to perform EX-OR operation using Initialization Vector. The result of the EX-OR operation is fed as input to encryption process and encrypted with the given Key value. The result obtained from encryption process is called as Secret/Cipher Text. Thus, the result of the encryption process will be the Initialization Vector to the next block. In this manner, the process is repeated for all the blocks of data to get the cipher text for all the blocks.

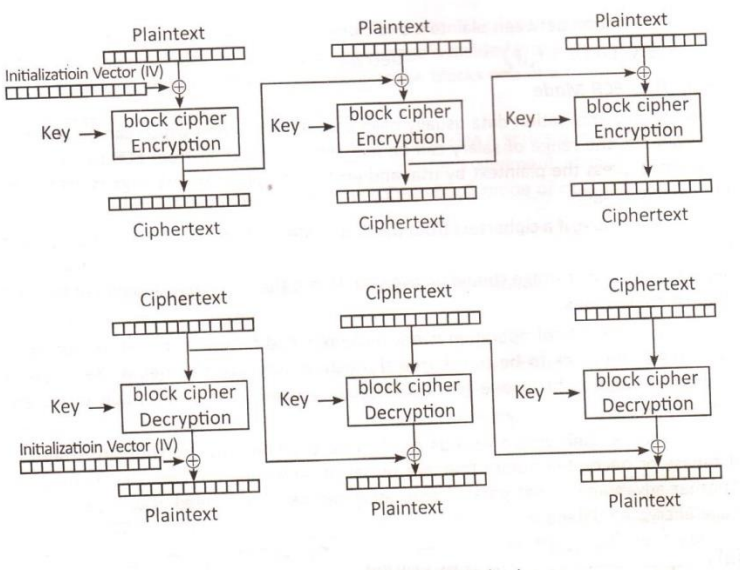

Fig 5:- Cipher Block Chaining

In this process, the original text is converted into ASCII code and each ASCII code of each character will be converted into multiple blocks of data. For example the ASCII code of the 'A' is 65 for which the binary value will be 01000001. In this method the defined block size is 64-bit so first 64-bits will be considered as one block. In the same way, all the bits are converted into multiple blocks. If the last block is not full that is if it is not 64 bits then padding (Adding dummy values) will be done. After converting the data in to blocks the encryption process is performed to convert it in to an secret text or cipher text. But while encoding and decoding the given text as the bit size is only 64bits so it takes more time to for the process if the original message is too big.

III. PROPOSED SYSTEM

In this paper to ensure high security with less time for an original message to encrypt, transfer the encrypted message and decrypt, it is suggested to use AES algorithm. In this process the algorithm uses 128 bits as input message and key. As the block size is double compared to DES algorithm, the process of encryption and decryption will be faster and secure.

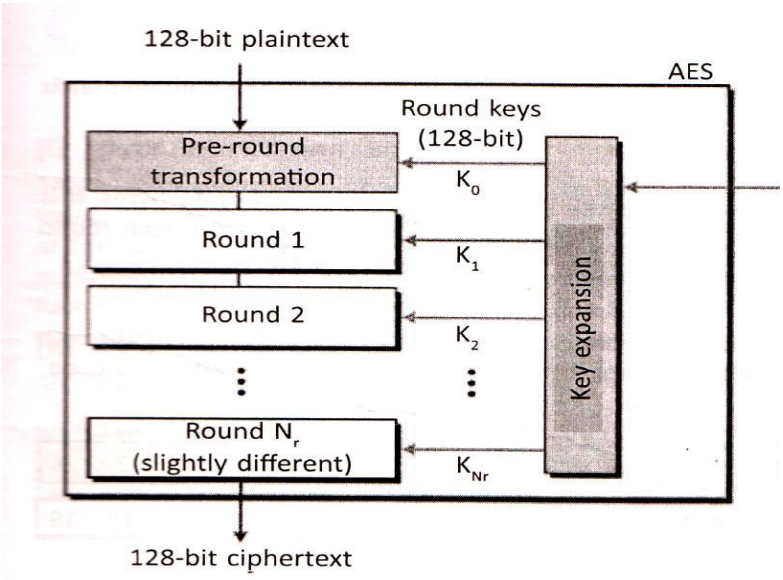

Fig 6:- AES General Structure

➢ *Proposed Encryption Algorithm:*

Step 1: As per the above figure (Fig-4), first we have to find out the no. of blocks and also we should specify the block positions.

Step 2: Main step is to divide the data into multiple and IV should be given for each of the blocks and the data within the block will undergo Ex-OR operation.

Step 3: The output from Ex-OR operation will be used with the key we perform the AES process. The result after AES process will be the Encrypted Text.

Step 4: The output of the first block is sent as the IV for the next block.
Step 5: The same process of Ex-OR operation will be done and the output of next block is send as an input to the further blocks.
Step 6: In this way all the data blocks will be encrypted.

Proposed decryption works reverse of the above explained encryption process.
Let's consider an example where the data is like GOODGIRLCHILDRENSNICKERSDOCUMENT will be converted using ASCII code to binary:

- *Input 2 blocks of data, that is 128 bits each:*

BLOCK 1: 01000111 01001111 01001111 01000100 01000111 01001001 01010010 01001100
010000110 10010000 10010010 10011000 10001000 10100100 1000101 01001110
BLOCK 2: 010100110 10011100 10010010 10000110 10010110 10001010 1010010 01010011
010001000 10011110 10000110 10101010 10011010 10001010 1001110 01010100

- *Encryption Process:*

BLOCK 1: 01000100 01010010 01000001 01000111 01001111 01001110 01000101 01010011
01000011 01000001 01010000 01010011 01001001 01000011 01010101 01001101
BLOCK 2: 01001000 01001111 01010100 01000011 01001000 01001001 01010000 01010011
01000011 01001111 01001110 01000111 01010010 01000001 01010100 01010011

- *Decryption Process:*

BLOCK 1: 01000111 01001111 01001111 01000100 01000111 01001001 01010010 01001100
010000110 10010000 10010010 10011000 10001000 10100100 1000101 01001110
BLOCK 2: 010100110 10011100 10010010 10000110 10010110 10001010 1010010 01010011
010001000 10011110 10000110 10101010 10011010 10001010 1001110 01010100

IV. CONCLUSION

In this paper, we have encrypted and decrypted the data using AES algorithm which is comparatively faster and provides more security because of the larger block size. As the block size is larger the process of encryption will be done with more combinations and it is proven to be more secure than DES algorithm. By this method we can achieve faster method of providing data security while data transfer.

REFERENCES

[1]. "Enhancing the Security of DES algorithm using Transposition Cryptography Techniques" Singh S, Makkar SK, Kumar S. International journal of Advanced Research in Computer Science and Software Engineering. 2013; 3(6):1–8.
[2]. "New Comparative Study between DES, 3DES and AES within Nine Factors" Alanazi HO, Zaidan BB, Zaidan AA, Jalab HA, Shabbir M, Al Nabhani Y. Journal of computing. 2010; 2(3):152–7.
[3]. "Secure user data in cloud computing using encryption algorithms" Arora R, Parashar A. International journal of engineering research and applications. 2013; 3(4):1922–6.
[4]. "A Novel structure with dynamic operation mode for symmetric-key block ciphers" Huang K-T, Chiu J-H, Shen S-S. International Journal of Network Security & Its Applications (IJNSA). 2013; 5(1):15–36.
[5]. "Recommendation for block cipher modes of Operation methods and techniques" Evans DL, Bond PJ, Bement AL, Dworkin M. USA: NIST Special Publication; 2001. pp. 800–83.
[6]. "Block Cipher Chaining Modes of Operation" Knudsen LR. 2000 Oct.
[7]. "Counter Chain: A New Block Cipher Mode of Operation, Journal of Information Processing Systems" El-Semary AM, Azim MMA. Information Journal of Process Systems. 2015; 11(2):266–79.
[8]. "Magnified Cipher Block Chaining Mode using DES to Ensure Data Security in Cloud Computing" D. Aruna kumari, M. Chandrika and B. Surekha Ratnam Bharadwaj Indian Journal of Science and Technology, Vol 9 (17) | May 2016