Indian Journal of Science and Technology, Vol 9(17), DOI: 10.17485/ijst/2016/v9i17/93028, May 2016
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Magnified Cipher Block Chaining Mode using DES to Ensure Data Security in Cloud Computing

D. Aruna kumari*, M. Chandrika and B. Surekha Ratnam Bharadwaj

K L University, Green Fields, Vaddeswaram, Guntur-522008, Andhra Pradesh, India; aruna_d@kluniversity.in, mchandrika555@gmail.com, surekhabethina@gmail.com

Abstract

Background/Objectives: The main objective is to provide security using Magnified Cipher Block Chaining mode-DES to ensure secure data on cloud. **Methods:** In this work we have to find how the data is converted into binary and splits into blocks of particular size. By using Magnified Cipher block chaining mode-DES we encrypt data and store into cloud. We send the key to the receiver then he/she access the data from the cloud and decrypt the data. By this methodology we can ensure high security because even cloud server cannot access data. **Findings:** In this research, many encryption and decryption algorithms like AES, DES, RSA, Cipher Block Chaining modes have been taken into account. By using the DES operation we proposed a magnified Cipher Block Chaining mode –DES to find out how the data is divided into blocks and how the DES operation will perform. In this work we also find out the several algorithms like AES, DES etc. DES algorithm has been designed to provide more secure because the data is to be perform 16 rounds for encryption and decryption. In our work we divide the data into blocks and encrypt the data using DES algorithm and sent to the next block depending on the midvalue+position. Like this all the blocks of the data are encrypted and decrypted. By this methodology we can provide more secure because we are storing the encrypted data in the cloud so that even cloud server cannot access. **Improvement:** In order to provide security we propose a Magnified Cipher Block Chaining mode using DES. On the basis of mid value + positions the data is encrypted and decrypted.

Keywords: Cipher Blocks Chaining, Cloud, Encryption, Decryption, Magnified, Security

1. Introduction

Data Security is one among the confidential resources in the cryptography. The necessary abstraction within the data security is to enhance the encoding algorithms. Presently most of us are storing the data in the cloud because it is reliable, secure etc.[1]But still there are many problems related to security in the cloud. So to provide more security we have many ways like encryption algorithms.

The procedure of changing the original data into encrypted data is termed as encoding or secret writing and converting the cipher text into original text is called decoding or secret writing. There are two sorts of cryptographic algorithms like Symmetric algorithms or One-key algorithms, Asymmetric algorithms or Double key Algorithms. In Single-key algorithm we only one key is used to encode and decode the data. Symmetric key algorithms can use either stream ciphers or block ciphers. A stream cipher is used to encode the original data one byte at a time. We can decrypt a block of data at a time by using the block cipher. A block may be of 64bits or 128 bits. This block ciphers can be applicable only to the symmetric algorithms. This block ciphers provide more secure in several cases and it is more complex. We have symmetric algorithms like DES, AES, BLOWISH etc. and Asymmetric algorithms like RSA, DSA etc. We also have another algorithm cryptographic algorithm called the Cipher block chaining mode. There are four modes of operation in Cipher Block Chaining mode called the ECB (Electronic code block) mode and second mode is Cipher block chaining mode (CBC), we provide an initialization vector and the key. Third mode is cipher feedback mode (CFB) and the fourth mode is Output feedback mode (OFB). Still there are many modes are evaluating to provide the data security like Counter mode, XCB mode etc.

Encryption and decryption process is shown in Figure 1

*Author for correspondence

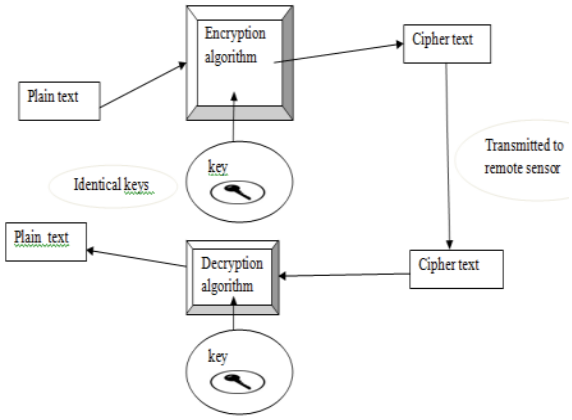

Figure 1. Encryption and Decryption process.

1.1 Symmetric Algorithms

We have already know that symmetric algorithms have one key to encode and decode the data. Several algorithms like Data Encrypted Standard (DES), Advanced Encryption Standard (AES), Blow fish etc.

1.1.1 Data-Encryption Standard (DES)

A whole block of data can encode using Des because it is a block cipher. The block size of DES is 64-bits and after encoding obtain a 64-bit cipher text. The key length is 56 bits. DES is a Symmetric algorithm used to encode and decode the text using a similar and secret key on sender and receiver. Based on transposition and Substitution Des algorithm will perform. DES algorithm has 16 steps called as rounds to encrypt the plain text in to the encrypted text and again 16 rounds are needed to decrypt the cipher or encrypted text in to original plain text. The key size is 56 bits. Originally the key consists of 64 bits. The bits from 8, 16,24,32,40,48,56,64 bits are removed from the key size. Then we will get the key size of 56 bits.

1.1.2 Des Algorithm

DES algorithm is shown in Figure 2

1.1.2.1 Explanation

Firstly the input data must be of 64-bit block size later we perform the initial permutation function. This initial permutation is performed on plain text[1]. After initial permutation the data is divided into two halves of equally shared 32bit. Generally a key size of 56 bits is used in which by using Key Transformation we randomly produce a key of 48 bits. As said before there would be equally shared

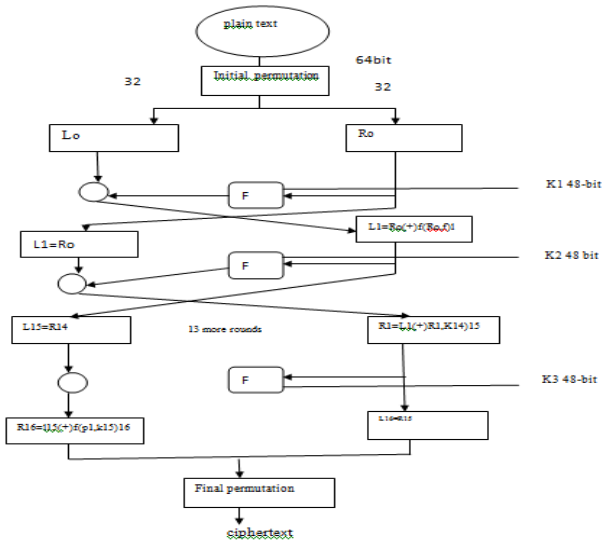

Figure 2. DES algorithm.

data in both the left and right side blocks, now the right block of 32 bits is converted to 48 bit data using Expansion Permutation. Now the resulted 48 bit data on the right block and the key data of 48 bit are EX-OR operated. Now the result of the operation of EX-OR is considered and forwarded to next step. As the next step to be continued with the operations we need a data of 32 bit. Instead we forward a data of 48 bit to the next step, by using S-box substitution we change the 48 bit data to 32 bit data[2]. Now, the 32 bit data is permutated by using P-Box substitution. The output of the P-Box is considered and EX-OR operation is performed with data in the left block (32 bit). The result of this operation is sent to the right block. The previous result of the right block is sent to the left block. This performed technique is known as "Swapping". Now the data present in the right block is presented to the next rounds. In the similar manner we perform the above task for about 15 rounds. To obtain the cipher text result, the data of 16th round is finally permuted which results in Cipher Text.

The above performed process when repeated for 2times gives [3]DOUBLE-DES and when performed for 3 times gives TRIPLE-DES. This TRIPLE-DES has 3 keys in which 2 are independent and the other dependent key. As this being 3 times more efficient than DES algorithm which provides more security when compared with DES.

1.1.3 Advanced-Encryption Standard (AES)

AES algorithm is a symmetric block cipher used to provide the security for the highly confidential information. Block

size of AES algorithm has 128 bits, 192bits or 256 bits. The Key length of AES algorithm is [3]128bits for 128bit-block size. To encode the plain text into the cipher text 10 rounds are need for 128 bit block size and 12 rounds are needed for the 192 bits block size 14 rounds are required for the 256 bit block size.

1.1.3.1 Algorithm-Working

AES Algorithm working is shown in Figure 3

In AES Algorithm, the 128 bit data can be encrypted using 10 different rounds, in which each round includes 4 different steps as shown in Figure 3.

Key Expansion: By Rijindael key schedule the round keys are obtained from the cipher key.

Initial Round: Addition round key: Using EX-OR operation each byte in the state is combined with a block of the round key.

The Steps are stated here:

Sub Bytes: Each byte in this round is replaced with reference to the bytes present in the lookup table.

Shift rows: For certain [3]number of times the last three rows are shifted cyclically.

Mix Columns: In this step the operation is performed on the columns in which 4 bytes in each column are combined.

Now, the addition of the round key is done.

The above stated steps are repeated for 9 times in which the 10th round is different from the above 9 rounds. The 10th round excludes the step named mixed columns.

1.2 Asymmetric Key Algorithm- RSA

RSA algorithm is shown in Figure 4

RSA algorithm is an asymmetric algorithm uses 2 unique keys for encoding and decoding. [4]Public Key Cryptography is also called as Asymmetric key

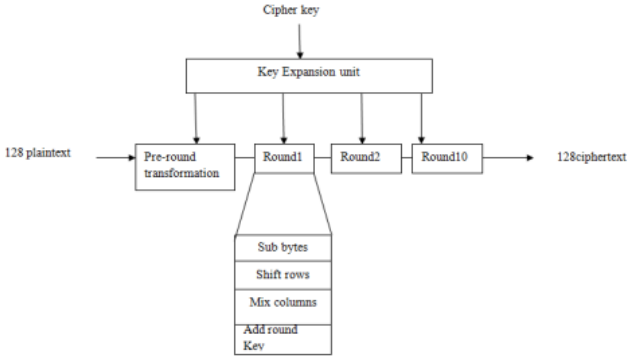

Figure 3. Advanced encryption standard algorithm.

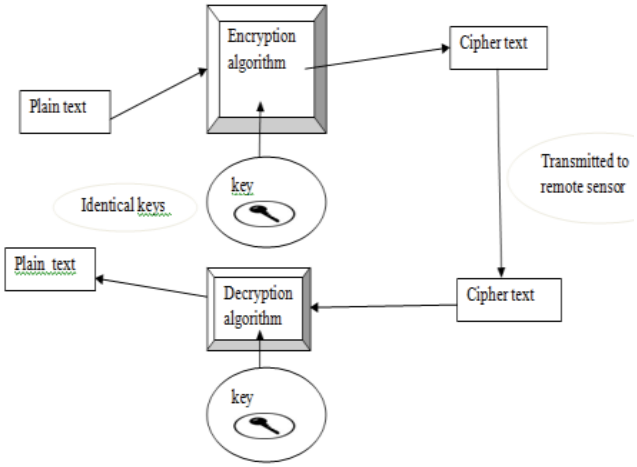

Figure 4. RSA Algorithm.

Cryptography. As stated in Figure 4, in RSA algorithm the public key is distributed to everyone and secret key is kept as personal. In RSA algorithm public and secret keys are needed to encrypt the original text. Key generation in RSA algorithm is very crucial.2prime numbers of larger values a and b are obtained using the Rabin-Miller test algorithm. By multiplying the a and b values a modulus of n is obtained. The result is utilized by the both public and secret keys and provides a link between them. Public Key made up of both modulus, public exponent e. The exponent e can be distributed with everyone. Private key consists of the modulus, secret variable d which is evaluated using Exended Eucledian algorithm. With respect to the value of n, we can find out the multiplication inverse.

2. Problem Definition

Now-a-days many problems are arising corresponding to the data security and data integrity in cloud computing. As we all knowledge security means protecting the information that has been transmitted from a sender to a receiver such that information will never be glorious to the third party and data integrity implies that the information send by the sender ought to stay identical information while it reaches to the receiver so that there mustn't be any sort of alternation throughout transmission. To achieve data security in the cloud we are going to encrypt the data and store in the cloud so that the cloud server also cannot discard the data so that we can achieve the data security and to achieve the data integrity we have be generate a key. To encode and decode the information we use the similar key so that there will be no loss of data and also

we can achieve the data security and integrity. To provide the security we use the modified cipher block chaining (CBC)[5] to encrypt the data and then store in the cloud. To know the data to the receiver has to register and send an request to the sender then sender will send the private or secret key through a mail then the receiver will access the encrypted text and decrypt the text using the decryption algorithm and the key sent by the receiver. By this we can achieve the data security and integrity. In this we have used the Magnified cipher block chaining to encode and decode the information.

3. Existing Algorithms

We have several secret writing algorithms to encode and decode the information like DES, AES, Cipher block chaining mode. In cipher block chaining mode the total message or bits are splitted in to the blocks of a particular block size. Then performs the x-or operation with the Iv value. There are 4 modes of operation in Cipher block chaining mode called Electronic code Block mode (ECB)[5], Cipher block chaining mode (CBC), Cipher feedback mode (CFB), Output feedback mode. The original text is converted in to binary bits of 0's and1's and by using a mode of operation we perform the encoding and decoding of the information.

3.1 Cipher Block Chaining Mode

Cipher block chaining mode is an operation for a block cipher which it can encrypt the data for a block of data. In cipher block chaining there is an Initialization vector of a particular length. When the data is divided into several blocks of a fixed block size then some times the last block cannot have the bits of particular size so padding is done at the last block. After decryption padded bits are removed so then we can get the original plain text.

An[5] IV (Initialization vector) is a block of bits or a binary series used in different modes of operation to obtain different cipher texts. By Iv value we obtain different cipher texts even same plain text is repeated. An formal vector has distinct confidential necessities than a key in order that it does not have to be compelled to be a secret. Therefore, we are able to transmit it publically.

There are [6]four modes of operation in Cipher block chaining mode (CBC):

1. Electronic Code Book mode (ECB)
2. Cipher Block Chaining mode (CBC)
3. Cipher feedback mode (CFB)
4. Output feedback mode (OFB)

3.1.1 Electronic Code Block (ECB) Mode

The [6]ECB is the easiest mode of operation. This mode as stated in Figure 5 works on the fixed block size. Plain text may be of different length. The given message is splitted in to chunks and every chunk is encrypted independently. In this mode, the drawback is similar original data are encrypted in to similar identical cipher text chunks, so in some cases it does not provide the confidential messages secure and it is not mostly used in cryptography protocols at all.

ECB mode is shown in Figure 5

3.1.2 Cipher Block Chaining Mode

Cipher block chaining mode is a technique used to encode and decode the information which is applied on a chunk of data as shown in Figure 6. The input data is segregated in to different number of chunks or blocks and performs EX-OR operation using IV. The result of the above sated step is encrypted with the Key value. The obtained result after encryption step is called as Cipher Text. Thus, the result of the encrypted value is works as an IV to the next chunk of data. In this way the process is repeated for several chunks or blocks of data to get the cipher text of all blocks.

CBC mode is shown in Figure 6

3.1.3 Cipher Feedback Mode

[7]Cipher feedback mode is also one of the techniques applied to encode and decode the information. As stated in Figure 7, CFB is a reverse operational technique of CBC. The operations in the first block are as usual. To obtain the cipher text of 2nd block the result of the previous block

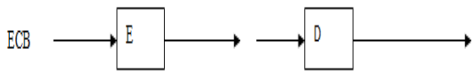

Figure 5. Electronic Code Book mode.

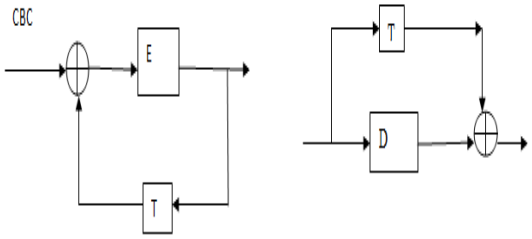

Figure 6. Cipher block chaining mode.

is EX-ORED with the present plain text. In this way all the chunks of data is encrypted and decrypted.

CFB mode is shown in Figure 7

3.1.4 Output Feedback Mode

In Figure 8, [8]Output Feedback Mode the plain text is Ex-Or operated with the IV value. Under the given key the IV value is distinct for every operation. The result of the above step is Ex-or operated with the plain data[7]. The 1st chunk of cipher text is obtained. The cipher text is introduced on the 1st block to produce 2nd output block. In this same way it is repeated several number of chunks of data.

OFB mode is shown in Figure 8

4. Proposed Algorithm

In this paper to provide more security to our data we are encoding the data by using an algorithm which converts the original data in to the encrypted form and then we store in the cloud and if the receiver want to know the data they should access from the cloud and decrypt the data by using the same algorithm.

4.1 Magnified Cipher Block Chaining Mode Encryption

In this mode first the original text like "APPLES ARE IN RED" are converted in to ASCII values and then each ASCII value of a character are converted in to the blocks. For Eg: The ASCII value of the A is 65 then the binary value of 65 is 01000001.Like this we have to convert all the text file into bits. In this mode we have define the block size as 64-bit so first 64-bits belong to one block. Like this, all the bits are separated in to blocks. If the last block has less than the 64 bits then padding will be done. After separation of data in to blocks the encryption algorithm is performed to convert it in to an unknown form or encoded form.

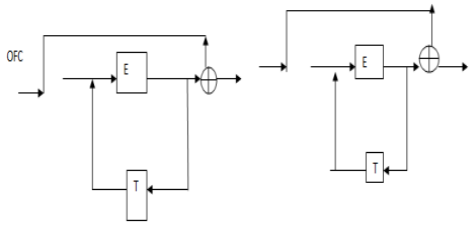

Figure 7. Cipher feedback mode.

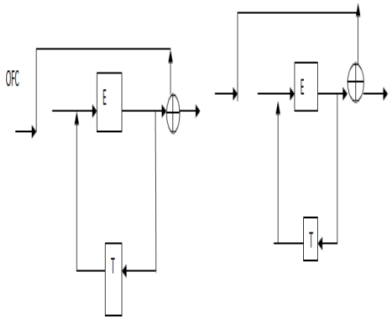

Figure 8. Output feedback mode.

4.1.1 Encryption Algorithm

Proposed Encryption Algorithm is shown in Figure 9

4.1.1.1 Working

Step 1: As shown in Figure 9, first we have to find out the Midvale by dividing the no. of blocks/2 and also give to positions to the blocks.

Step 2: First the data is divided in to blocks of data for each block IV and the data inside the block will perform the X-OR operation.

Step 3: By using the output of the block and the key we perform the DES Encryption algorithm. After working the DES algorithm the result of the block is Encrypted text.

Step 4: The result of the first block is send as a key to the third block because we are sending the output as an input to the block depending on the midvalue+pos is 3

Step 5: The same process of xor operation is done and the output of third block is send as an input to the second block because the position of the block is incremented.

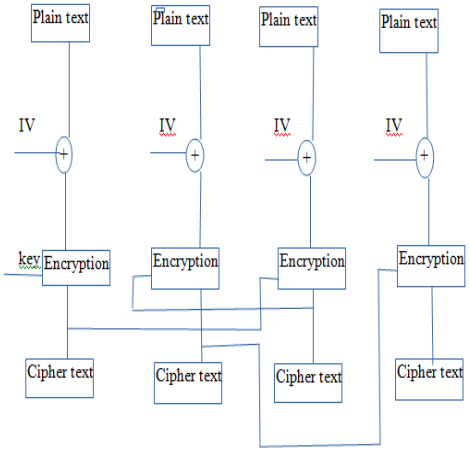

Figure 9. Proposed Encryption algorithm.

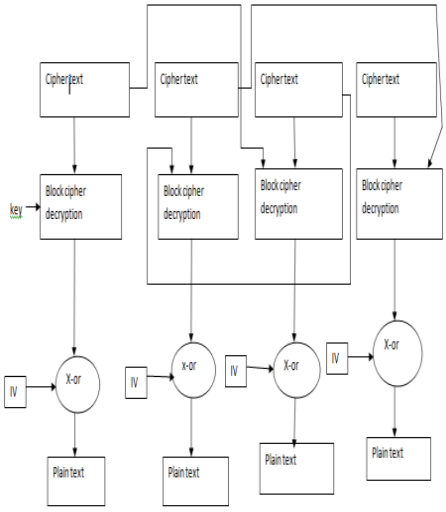

Figure 10. Proposed Decryption algorithm.

Step 6: like this the total blocks of data are encrypted.

Step 7: The same procedure can be repeated to "n" number of blocks.

4.1.2 Enhanced Cipher Block Chaining Mode Decryption

Proposed Decryption Algorithm is shown in Figure 10

4.1.2.1 Working

Step 1: In this decryption process we will perform the reverse of the encryption.

Step 2: As shown in Figure 10, first the cipher text is also divided in to blocks and x-ored with the key by using a DES Decryption algorithm.

Step 3: The output of the block and IV value is X-ORed and the final plain text will be obtained.

Step 4: The output of the block after x-ored with the IV value is send as an input to the third block because the mid value +pos is 3.

Step 5: The output of third block is send as an input to the second block because the position value is incremented.

Step 6: Like this all the blocks of data are decrypted and we will get the original plain text. The same process will be done for "n" number of blocks.

5. Conclusion

In this paper we have encrypted the data using magnified cipher block chaining mode of operation which provides more security rather than the existed cipher block chaining because we have came up with a new idea that in all existing algorithms the output of the first block is send as an input to the next block but we are sending the output of the first block as an input to the another block depending up on the mid values and position of blocks. By using the algorithm we can encode and decode the information and provide more confidentiality. To provide more security we will send the KEY to authorized person only. We will decide it by the UNIQUE ID given to the each person who are registered. Then only the sender can send the private key to the receiver so that he/she can decrypt the data by retrieving from the cloud. By this manner, we can achieve data security in the cloud.

6. Expected Results

6.1 Inputs of the Four Blocks

For example the data like GOODGIRL CHILDRENSNICKERSDOCUMENT will be converted to binary using ASCII values .After encoding it changes to another text. After decryption we get the real data.

BLOCK 1: 01000111 01001111 01001111 01000100 01000111 01001001 01010010 01001100

BLOCK 2: 010000110 10010000 10010010 10011000 10001000 10100100 1000101 01001110

BLOCK 3: 010100110 10011100 10010010 10000110 10010110 10001010 1010010 01010011

BLOCK 4: 010001000 10011110 10000110 10101010 10011010 10001010 1001110 01010100

6.2 After Encryption the Four Blocks of Data is

BLOCK 1: 01000100 01010010 01000001 01000111 01001111 01001110 01000101 01010011

BLOCK 2: 01000011 01000001 01010000 01010011 01001001 01000011 01010101 01001101

BLOCK 3: 01001000 01001111 01010100 01000011 01001000 01001001 01010000 01010011

BLOCK 4: 01000011 01001111 01001110 01000111 01010010 01000001 01010100 01010011

6.3 After Decryption the Blocks of Data is

BLOCK 1: 01000111 01001111 01001111 01000100 01000111 01001001 01010010 01001100

BLOCK 2: 010000110 10010000 10010010 10011000 10001000 10100100 1000101 01001110
BLOCK 3: 010100110 10011100 10010010 10000110 10010110 10001010 1010010 01010011
BLOCK 4: 010001000 10011110 10000110 10101010 10011010 10001010 1001110 01010100

7. Future Scope

In this paper we have define the block size as 64bit and used the DES algorithm to encrypt and decrypt the data. In future we can also increase the block size of data from 64bits to 128 bits then we can use the AES algorithm instead of DES algorithm. By increasing the block size we should use the suitable size of the data of a particular algorithm. So that we can also encrypt for a huge amount of the data and may be time complexity can decrease.

8. References

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