

A TECHNIQUE TO SECURE DATA STORAGE AND SHARING USING AES

G.SAI AKHIL
Student,SCS,Lingaya's University,
Faridabad, Haryana

M.AMARNADH
Student,SCS,Lingaya's University,
Faridabad, Haryana

Mr. Kiran Kumar
Assistant Professor, Dept. of
Computer Science Computer Science
Lingaya's University, Faridabad,
Haryana

Abstract—Storage Security is the group of parameters and settings that make storage resources available to authorized users and trusted networks - and unavailable to other entities. These parameters can apply to hardware, programming, communications protocols, and organizational policy. Several issues are important when considering a security method for a storage area network. The network must be easily accessible to authorized people, corporations, and agencies. It must be difficult for a potential hacker to compromise the system. The network must be reliable and stable under a wide variety of environmental conditions and volumes of usage. Protection must be provided against online threats such as viruses, worms, Trojans, and other malicious code. Sensitive data should be encrypted by using any type of cryptography security algorithm (Such as DES or Triple DES or AES). These algorithms are symmetric key algorithms which uses same key for encryption and decryption. All users should be informed of the principles and policies that have been put in place governing the use of the network.

1. Presentation:-

Type of Encryption:In this project we are using **AES (Advance Encryption System)** algorithm to encrypt the data stored in server, because it is the advance security symmetric key algorithm. Now-a-days many of the government organizations and private organizations are using AES algorithm for data encryption. Before developing AES there are two symmetric key algorithms those are DES and Triple DES. These are having many disadvantages, in DES the is problem in compatibility of hardware and software (DES algorithm) and hacker can easily find the encryption key by using **Brute-Force** attack because it is using small key for encryption. In Triple DES, the disadvantages of DES are been covered and also a new problem is occurred that is slow execution of algorithm. To avoid all these above problems AES was introduced. It uses three variety of key sizes- 128 bit, 192 bit, 256 bit and it

uses substitution and transposition technique instead of feistel network rounds.

DES Algorithm: The Data Encryption Standard (DES) is a symmetric-key block cipher published by the national Institute of Standards and Technology (NIST).DES is an implementation of a Feistel Cipher. It uses 16 round Feistel structure. The block size is 64-bit. Though, key length is 64-bit, DES has an effective key length of 56 bits,since 8 of the 64 bits of the key are not used by the encryption algorithm.

Drawbacks of DES: As it is having many advantages it also contained disadvantages such as **BRUTE-FORCE** attack. This attack can decrypt the cipher text by 2^{55} combinations. If the key size increased it takes long-long time to decrypt the cypher text.

Triple-DES Algorithm:The speed of exhaustive key searches against DES after 1990 began to cause discomfort amongst users of DES. However, users did not want to replace DES as it takes an enormous amount of time and money to change encryption algorithms that are widely adopted and embedded in large security architectures.The pragmatic approach was not to abandon the DES completely, but to change the manner in which DES is used. This led to the modified schemes of Triple DES (sometimes known as 3DES). There are two variants of Triple DES known as 3-key Triple DES (3TDES) and 2-key Triple DES (2TDES).Before using 3TDES, user first generate and distribute a 3TDES key K, which consists of three different DES keys K1, K2 and K3. This means that the actual 3TDES key has length $3 \times 56 = 168$ bits.

Drawbacks of Triple-DES:As we are having many advantages it also containing disadvantages too such as encryption and decryption process will takes long time due to lopping of DES process. This model fails due to its time consumption process.

AES (Advance Security System): The more popular and widely adopted symmetric encryption algorithm which is give by NIST (National Institute Standard and Technology) likely to be encountered now-a-days is the Advanced

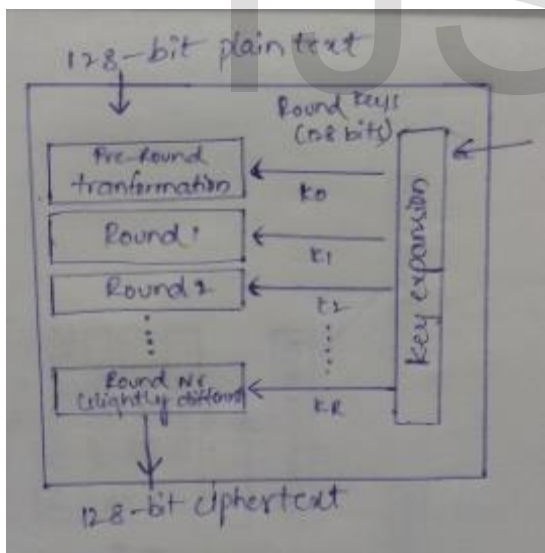
Encryption Standard (AES). It is found at least six time faster than triple DES. A replacement for DES was needed as its key size was too small. With increasing computing power, it was considered vulnerable against exhaustive key search attack. Triple DES was designed to overcome this drawback but it was found slow.

The features of AES are as follows:

- Symmetric key encryption.
- It uses various sizes of keys 128bit, 192bit, 256bit.
- It is better than DES and Triple-DES.
- It is implementable by using C and Java.

2. AES Structure:-

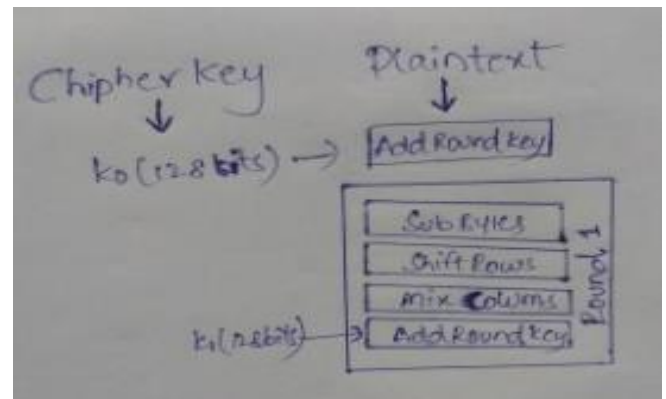
Operation of AES: - AES is an iterative process instead of Feistel cipher. It works like 'substitution-permutation network. It contains a series of operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits among them (Permutations). AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix. Unlike DES, the number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key. The schematic of AES structure is given in the following illustration:



2.1. Encryption Process

Here, we restrict to description of a typical round of AES encryption. Each round comprise of four sub-processes.

The first round process is shown below:



Byte Substitution (SubBytes): - The 16 byte matrix is substituted with substitution box and produces output of 16 bytes.

Shift Rows: - There are four rows in obtained matrix, these rows are shifted to its left according to row number. The shift operations are as following:

- First row is not shifted.
- Second row is shifted one position to the left.
- Third row is shifted two positions to the left.
- Fourth row is shifted three positions to the left.

The result is a new matrix consisting of the same 16 bytes but shifted with respect to each other.

Mix Columns: - Each column of four bytes is now transformed using a special mathematical function. This function takes as input the four bytes of one column and forms output of four bytes, which replace the original column. The result is another new matrix consisting of 16 new bytes. It should be noted that mix column step in now applied in last round.

Add Round key: -The 16 bytes of the matrix are now considered as 128 bits and are XOR with the 128 bits of the round key produced by actual key. After last round the produced output is called cipher text which is fully encrypted. Otherwise, the resulting 128 bits are interpreted as 16 bytes and we begin another similar round.

Usual Round:

Usual rounds will have following operations:

- Sub Bytes
- Shift Rows
- Mix Columns
- Add Round Key , using $K(\text{round})$

Final Round:

Final round will have following operations:

- 1. Sub Bytes
- 2. Shift Rows
- 3. Add Round

2.2. Decryption Process:-

Decryption Process: - The process of decryption of an AES cipher text is similar to the encryption process in the reverse order. It will take input as cipher text and produces output of plain text.

- Add round key
- Mix columns
- Shift rows
- Byte substitution.

Since sub-processes in every round are in reverse manner, unlike for a Feistel Cipher, the encryption and decryption algorithm needs to be separately implemented, although they are very closely related. In present day cryptography, AES is widely adopted and supported in both hardware and software. Till date, no practical cryptanalytic attacks against AES has been discovered. Additionally, AES has built-in flexibility of key length, which allows a degree of ‘future proofing’ against progress in the ability to perform exhaustive key searches. However, just as for DES, the AES security is assured only if it is correctly implemented and good key management is employed.

```

begin
  byte state[4,Nb]

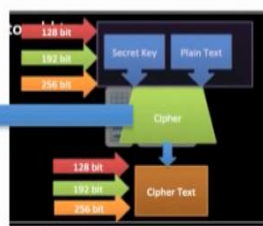
  state = in

  AddRoundKey(state, w[0, Nb-1])

  for round = 1 step 1 to Nr-1
    SubBytes(state)
    ShiftRows(state)
    MixColumns(state)
    AddRoundKey(state, w[round*Nb, (round+1)*Nb-1])
  end for

  SubBytes(state)
  ShiftRows(state)
  AddRoundKey(state, w[Nr*Nb, (Nr+1)*Nb-1])

  out = state
    
```



The diagram illustrates the AES encryption process. It shows a 'Secret Key' (128 bit) and 'Plaintext' (128 bit) entering a 'Cipher' block. The output of the cipher is 'Cipher Text' (128 bit). The cipher block is represented as a green trapezoid with a blue arrow pointing from the plaintext and key to the ciphertext.

2.3. Problem Definition

The main concern of online storage is storing the data in servers which are in far places. So, the main concern is the security of our data. There are two problems that hacker can easily steal our credentials to misuse the data and other problem is that we are storing our data under the control of third-party so that they can misuse our data (data compromise). To avoid this problem we are using cryptography techniques for encrypting data and converting it into cipher text. Cipher is the text which cannot understandable by the human beings. There are many techniques and algorithms to encrypt the data such as DES, Triple DES, AES and so on.

In this project we are using AES algorithm due to its advantages that DES and Triple DES algorithms. Here we will encrypt the uploaded data by using a security key. This key will go through the total process of AES and produce the encrypt form of that data, this data will stored for future purpose. AES is the symmetric key encryption so we will use the same key for both encryption and decryption. We can keep different key passwords for different files which are uploaded, due to this encryption even the hacker or the third party knows our credentials the cannot misuse the data because they are encrypted with a particular key. For the decryption we need the same key used in encryption.

2.4. Solution:-

AES (Advance Encryption System) is the better solution for encrypting the data on internet and saving it from hackers and third parties from misusing it.

The AES Process: The encryption process uses a set of specially derived keys called round keys. These are applied, along with other operations, on an array of data that holds exactly one block of data and the data to be encrypted. This array we call the state array.

You take the following AES steps of encryption for a 128-bit block:

- Derive the set of round keys from the cipher key.
- Initialize the state array with the block data (plaintext).
- Add the initial round key to the starting state array.
- Perform nine rounds of state manipulation.
- Perform the tenth and final round of state manipulation.
- Copy the final state array out as the encrypted data (cipher text).



The reason that the rounds have been listed as "nine followed by a final tenth round" is because the tenth round involves a slightly different manipulation from the others. The block to be encrypted is just a sequence of 128 bits. AES works with byte quantities so we first convert the 128 bits into 16 bytes. We say "convert," but, in reality, it is almost certainly stored this way already. Operations in RSN/AES are performed on a two-dimensional byte array of four rows and four columns. At the start of the encryption, the 16 bytes of data, numbered D0 to D15, are loaded into the array.

Each round of the encryption process requires a series of steps to alter the state array. These steps involve four types of operations called:

- Sub Bytes.
- Shift Rows.
- Mix Column's.
- XOR Round Keys.

Round Keys: - The cipher key used for encryption is 128 bits long. Where this key comes from is not important here; refer to Chapter 10 on key hierarchy and how the temporal encryption keys are produced. The cipher key is already the result of many hashing and cryptographic transformations and, by the time it arrives at the AES block encryption, it is far removed from the secret master key held by the authentication server. Now, finally, it is used to generate a set of eleven 128-bit round keys that will be combined with the data during encryption. Although there are ten rounds, eleven keys are needed because one extra key is added to the initial state array before the rounds start. The best way to

view these keys is an array of eleven 16-byte values, each made up of four 32-bit words. To start with, the first round key Rkey0 is simply initialized to the value of the cipher key (that is the secret key delivered through the key hierarchy).

3. Conclusion

Now-a-days most advanced encryption is AES(Advance Encryption System). It is the advance technology in symmetric key encryption. It overcomes the problems occurs in DES and Triple-DES. It uses variable lengths of encryption keys to keep it more secure so that brute force attack will not possible. The execution of AES process is very fast because it uses substitution and permutation process. Encryption algorithm plays very important role in communication security. Our research work surveyed the performance of existing encryption techniques like AES, DES and RSA algorithms. Based on the text files used and the experimental result it was concluded that AES algorithm consumes least encryption and RSA consume longest encryption time. We also observed that Decryption of AES algorithm is better than other algorithms.

References

- [1] <http://www.facweb.iitkgp.ernet.in/~sourav/AES.pdf>
- [2] <http://www.saylor.org/site/wp-content/uploads/2012/06/Advanced-Encryption-Standard.pdf>
- [3] Cryptography and Network Security – Atul Kahate, Tata McGraw-Hill Education
- [4] <https://www.rosehulman.edu/~holden/Preprints/s-aes.pdf>
- [5] <https://www.rivier.edu/journal/ROAJ-Fall-2010/J455-Selent-AES.pdf>
- [6] <http://www.adamberent.com/documents/AESbyExample.pdf>
- [7] <http://www.cs.columbia.edu/~sedwards/classes/2008/4840/reports/AES.pdf>

[8]http://ip.cadence.com/uploads/126/AES_XTS_onXtensa-pdf

[9]<https://www.cs.utexas.edu/~byoung/cs361/lecture46.pdf>

[10]<http://sandilands.info/sgordon/teaching/reports/simplified-aes-example.pdf>

[11]http://www.sersc.org/journals/IJSIA/vol9_no7_2015/21.pdf

[12]Abdul.Mina, D.S, Kader, H.M. Abdual & Hadhoud, M.M. "Performance Analysis of Symmetric Cryptography"

[13] Kalpana Parsi, Singaraju Sudha. "Data Security in Cloud Computing using RSA Algorithm". International Journal of Research in Computer and Communication technology, IJRCCT, ISSN 2278- 5841, Vol 1, Issue 4, September 2012. pp. 145

IJSER