Enhancing Data Security in Cloud Computing using AES encryption Algorithm

[1]Rajput Snehal, [2] Prof. J S Dhobi
[1]PG student, Government Engineering College, Gandhinagar.
[2] Assistant Professor, Government Engineering College, Gandhinagar.

.

Abstract

Cloud Computing is the upcoming latest technology,it offers computation as per utility of the customer and hence it is known as utility computing. This model is attractive mainly for business oriented people because it reduces total cost of operation, maintainance cost , increases return of investment. But the only thing that is impeding popularity of cloud computing is security issues. In this report we throughly studied and analyse AES encryption algorithm and we found that it is one of the most secure algorithm on cloud. We also discussed AES drawback and tried to overcome it.

Keywords: *AES , BF function, Huffman coding, encryption, decryption.*

---

1. Introduction: When plugging an electric appliance into an outlet, we neither care how electricity is generated nor how it is delivered to the outlets[1]. This is possible because electricity is virtualised and hence it is available from the outlets without any concern where it is produces , how it is delivered to the socket. When extended to information technologies, which means computing is provided to the users hiding other details, such virtualisation of computing it is known as cloud computing. In addition, an important aim of these technologies has been delivering computing as a utility. Utility computing describes a business model for on-demand delivery of computing power; consumers pay for the service as per their usage, similar to the way in which we currently obtain other day to day utility services such as electricity, telephone, water and gas.

Cloud Computing has been coined as an umbrella term to describe a category of sophisticated on-demand computing sevices initially offered by commercial providers, such as Amazon, Google and Microsoft. The main principle behind such model is offering computing, storage, and software " as a service."

Many practitioners in the commercial and the academic spheres have attempted to define exactly what "cloud computing" is and what unique characteristics is presents. Buyya have defined it as follows: "Cloud is a parallel and distributed computing system consisting of a collection of inter-connected and virtualised computers that are dynamically provisioned and presented as one or more unified computing resources based on service-level agreement(SLA) established through negotiation between service provider and consumers."

1.1 Definition of Cloud Computing

Vaquero have stated " Cloud are a large pool of easily usable and accessible virtualised resources(hardware, development platforms and/or services)These resources can be dynamically reconfigured to adjust to a variable load, allowing also for an optimum resource utilisation. This pool of resources is typically exploited by a pay-per-use model in which guarantees are offered by the Infrastructure Provider by means of customised Service Level Agreements."

National Institute of Standards and Technology (NIST) defines Cloud computing as follows:"Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This Cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models."

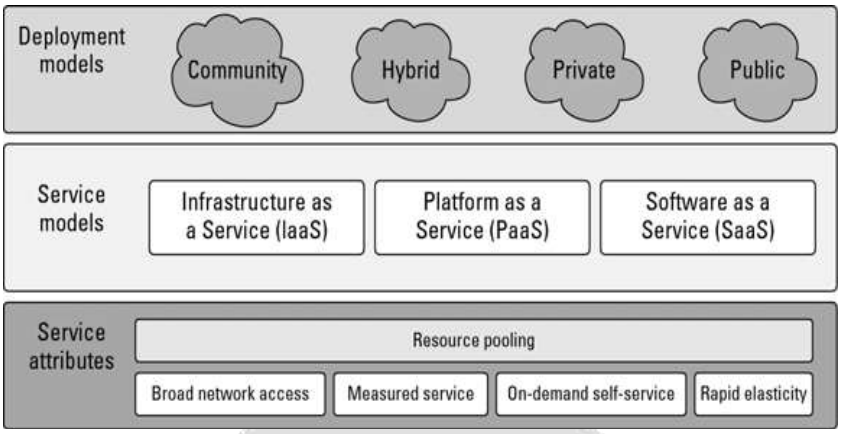


Figure 1.1 The NIST definitions of Cloud Computing

2. Cloud security: One of the crucial challenge of Public cloud computing is Data security.Once data moved onto cloud user himself donot know where his data is located onto with datacenter and in which state or territory. In order to provide security to the user some authentication, some control access should be proposed. Data should be in encrypted form while transferring through the network.

2.1 Cryptography: It is the method of using different algorithms to encrypt and decrypt message and data. Cryptography allows you to secure your crucial data so that it will reach securely to the desirable and authenticate receiver. Data when sent by sender cannot be hacked by hacker in between the transmission.

Cryptography has two parts:

1. Encryption:
   Plain text is converted into the cipher text.

2. Decryption:
   Cipher text is converted again to plain text or original text.

Various level of encryption can be applied to the plaintext to make data more secure.
Even if one level of encryption is cracked by hacker, the text will be again text, which make it difficult to get the plaintext.

Cryptography keys can be classified into asymmetric and symmetric key which is defined below.

Types of cryptographic keys:

1. Asymmetric key:

- In Asymmetric key type, user must have both public key and private key. User will encrypt through its public key and receiver will decrypt Dta through its private key. Here Public keys and private keys are used during encryption and decryption.
- It is more secure than Symmetric key because even if one key is known to hacker, without other key it is difficult to get the plaintext.
- Asymmetric key algorithm is slower than symmetric key algorithm as it require time for to key generation.
- Various examples are RSA, DSA etc.

2. Symmetric key:

- In symmetric key cryptography every user have his own secret key. Only one secret key is used for both encryption and decryption.

- It is less secure than Asymmetric key algorithm because here only one key is used for both encryption and decryption.
- Symmetric key algorithm is faster than Asymmetric key algorithm.
- Various examples are: AES, DES, 3DES etc.

3. Proposed Methodology

3.1 Proposed Scenario:

Let us assume that we have two enterprises say A and B. Both enterprise have their private Cloud storing their records and confidential data onto it.If any enterprise A or B want to sent these data to each other they will use following path showed below.
The following are the step for the Encryption:

Plain Text ---> Brainfuck function ---> Huffman coding ---> AES encryption ---> Cipher Text

The following are the step for the Decryption:

Cipher Text ---> AES decryption ---> Huffman coding ---> Brainfuck function ---> Plain Text

i) Brainfuck function :

Brainfuck is the most popular esoteric programming language, developed by Urban Muller in the year 1993. The language consists of only eight commands and it is fully Turing-complete.

A Brainfuck program has an implicit byte pointer, termed as simply "the pointer", which can freely move within an array of size 30000 bytes, initially each byte is set to zero. The pointer initialized points to the beginning of this array.

The Brainfuck programming language consists of eight simple commands, each is represented as a single character.

ii) Huffman Coding:

Huffman code is for optimal prefix code which is commonly used for lossless data compression. This algorithm was developed by David A. Huffman, who was a Ph.D.student at MIT, and published the paper in 1952 named as "A Method for the Construction of Minimum-Redundancy Codes". Huffman coding is based on the frequency of occurance of any data item .The main motto is to use a lower number of bits to encode the data that occurs more frequently into the data set. Codes are stored in a *Code Book* which may be constructed for each data or a set of data.

iii) AES encryption:

In AES algorithm, intermediate result of any round is called as State. The State can be defined as a array of bytes. It consists of 4 Rows and number of columns (Nc) . Nc is defined as dividing block length by 32. Cipher key is defined similarly.

The ByteSub Transformation function is a non-linear byte substitution where multiplicative inverse is applied, followed by affine function. It operates independently on each state . Here each state is mapped to S-box and required array is obtained.
The ShiftRow transformation function,it shifts each row by some defined offset. Very First row is not shifted, second row is shifted by s1 byte and third row by s2 byte….

For example:

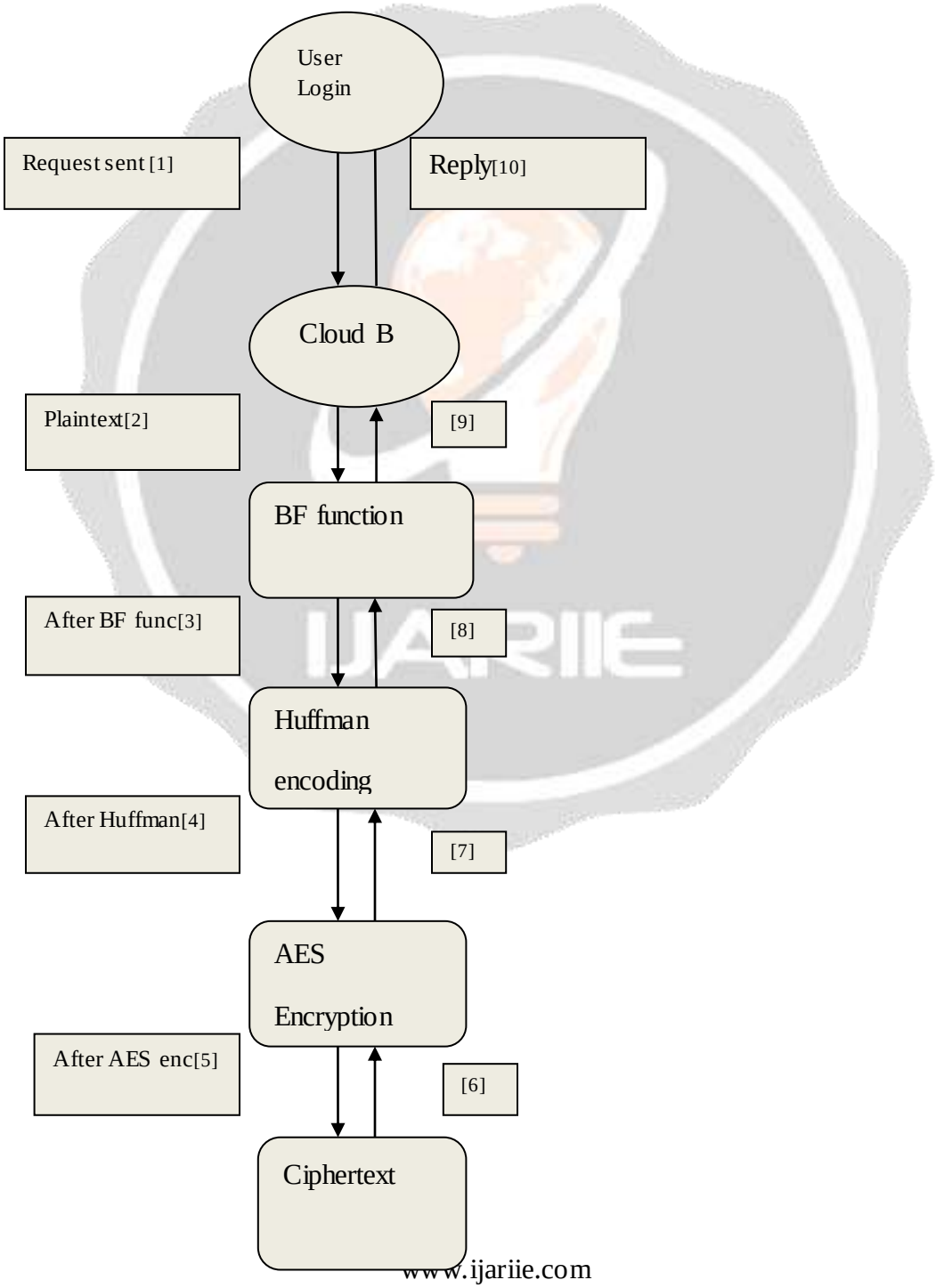
State array	New state array
W 1 Q 4	W 1 Q 4
A B C D	B C D A
0 P Q R	Q R 0 P

The MixColumn transformation : here state as considered as polynomial and multiplied with certain fix polynomial. Let C(x) = B(x) XOR A(x), where B(x) if certain fix matrix.

$$\begin{pmatrix} C0 \\ C1 \\ C2 \\ C4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 2 & 1 \\ 4 & 3 & 1 & 2 \end{pmatrix} \text{XOR} \begin{pmatrix} A1 \\ A2 \\ A3 \\ A4 \end{pmatrix}$$

The Round Key addition: Here XOR operation is performed between state and key blocks.

3.2 Flow Chart



5. IMPLEMENTATION:

Normal AES Encryption:

Key (128): E8E9EA EBEDEE EFF0F2F3F4F5F7F8F9FA

Plaintext: 014BAF2278A69D331D5180103643E99A

Ciphertext: 6743C3D1519AB4F2CD9A78AB09A511BD

Proposed Method:

Plaintext: 014BAF2278A69D331D5180103643E99A

Step 1: Pass the plain text through the brainfuck script:

-+.<]<-<.+>.>.-<.,[-[-.,>[-+-+[-.<[-]--<

Step 2: Further encode it using Huff Man Encoding:

We will get the Huff-Man character count as follow:

[5 00

+ 4 010

> 3 0110

, 2 01110

] 2 01111

- 11 10

< 6 110

. 7 111

And the Huffman binary form will be:

100101111100111111010110111010011011101101111011011101110001000101110111001100010010100100010111110001001111101010110

Step 3: These code need to be converted into hexadecimal form

4be7eb74ddbdbc000000000000000

Step 4: Encrypt this hex value with the AES-128 bit

Key (128): E8E9EA EBEDEE EFF0F2F3F4F5F7F8F9FA

Ciphertext: fbebb049a127d3ff1ba71490ea704829

When following steps are reversely followed it will give the same plaintext.

Even if key is known to any unauthenticate person he may not know what is the plaintext.

6. Conclusion:

In this report, the structure and design of Rijndael cipher (new AES) have been throughly studied and analyzed. We have highlighted its main advantages and limitations, as well as AES performance is also compared with other algorithms. The importance of the Advanced Encryption Standard and the high security of the Rijndael algorithm has been examined and it is learnt that Rijndael AES, currently is an unbreakable algorithm. The only drawback we found in AES algorithm is that, we share key among multiple users which may fall into fake person hand but if we apply multi- level encryption this drawback can be eliminated and hence making it more secure.And our objective of enhancing data security in cloud computing is being achieved.

7. References

1. Mastering Cloud Computing Foundations and Applications Programming by prof. Rajkumar Buyya, Christian Vecchiola, S.Thamarai Selvi.
2. The Rijndael's Algorithm URL: http://www.esat.kuleuven.ac.be/~rijmen/rijndael/
3. E. Biham, "A note on comparing the AES candidates, " Proc. of the 2nd AES candidate conference, March 22- 23 , 1999, Rome, pp . 85-92.
4. Cryptography and network security by Atul kahate
5. The design of Rijndael algorithm by joan daernen and vincent rijrnen.
6. www.muppetlabs.com/breadbox/bf
7. esolang.org/wiki/brainfuck
8. andrew.hedges.name/experiments/brainf_cker/
9. www.cs.cf.ac.uk/huffman_coding
10. rosettacode.org/wiki/huffman_coding
11. www.utdallas.edu/daescu/huffman_coding