SECURITYOF DATA IN CLOUD COMPUTING

Rahul Bisht, MCA Student, Uttaranchal University, Dehradun
Abhishek Kumar Pathak, Assistant Professor – Computer Application, Uttaranchal University, Dehradun

ABSTRACT

Cloud computing is a current running trend all over the world. There are a lot of cloud computing models like PaaS, SaaS, and IaaS. Cloud services growth makes many changes in the computing world. A lot of service providers of the cloud are available in the computer world. Protecting the data or information in the cloud database server is the only area of concerns in the cloud computing. Cryptography method is usually used to protect data in cloud databases. It is a method that transforms the sensitive data into an unreadable form. Cryptography technique offers many asymmetric or symmetric algorithms to protect the data. This paper shows the AES algorithm and AES is based on many permutation, transformation and, substitutions.

Keywords: Cryptography, AES, Security, Cloud Computing.

INTRODUCTION

The word cloud computing is used to provide a set of services, facility, and method for delivering IT services to the client or user, such as it provides data storage over the internet, software development platforms, server, over the internet[1].It is provided "as a service" over the Internet, typically PaaS, IaaS and SaaS, which is the easiest to use [5].In this technique the networking resources, Hard-disk memory, etc. are provided and are charged as per the usage. The companies who provide the services are called as Cloud Service Providers and often these services are provided by big companies [7].

The information can be shared on alarger scale in cloud computing, which is location independent and cost effective.Cloud application is the wider model of organization convergence.There can be three types of cloud-

(A)-Private cloud

(B)-Public cloud

(C)-Hybrid cloud

(A)-Private cloud- It is used by the single institute.

(B)-Public cloud- They are used on a larger scale.

(C)-Hybrid cloud- It is a union of private cloud and public cloud and it is used by most of the industries.

Cloud computing characteristics are-

1-The hardware (back-end application) is entirely handled by a cloud vendor.

2-services are easily scaled up and scale down.

3-clients pay only for services such as bandwidth, memory and processing time, etc.

Using Cloud computing we can store heavy load of data and information. As the central data storage is the main ability of the cloud services it is really importance to offer the security. Protecting the data by converting the data or information in unreadable form is known as cryptography [4].

Cryptography used generally 3 types of algorithm [2]. They are

(A)-Symmetric-key algorithms

(B)-Asymmetric-key algorithms

(C)- Hash function

Symmetric algorithms use the similar key for encryption or decryption.

This is called as the secret key.

So the similar key is used by the sender to encrypt the sensitive data or receiver to decrypt the sensitive data. It contains algorithms such as Ron's Code (RCN), Advanced Encryption Standard, Data Encryption Standard, and Triple DES, Blowfish, etc. Asymmetric techniques works on more than one key, one key to encrypt the data or another key to decrypt the data. One key that encrypts the sensitive data are called as public key and another one that is used to decrypt the sensitive data is called as a private key. Key that is used by the sender to encrypt the data is known to the public and key that is used by the receiver to decrypt the sensitive data are known to the user. It contains various algorithms like Diffi — Hillman, and Adleman (RSA), Shamir, Elliptic Curve (EC), Rivest, Digital Signature Algorithm, El Gamaletc[3].

The Hash functions are used to encrypt the information. It is similar to Message Authentication Code. Takes in variable size letter (information or data) and gives a fixed size result. It is known as Hash code, Hash value, or Message digests.

Symmetric cryptosystem has computational efficiency and speed to handle encryption of big amount of data, so we choose the symmetric cryptography as the solution. Advanced encryption standard is an encryption technique developed by two cryptographers Vincent Rijmen and Joan daemon. Government of United States approved the algorithm in October 2000 [6].

Feature of AES- 1)-Faster and stronger than triple-DES

2)-128 bit data, 128/192/256 bit key.

3)-For 128 bit keys, AES performs 10 rounds, for 192 bit keys AES performs 12 rounds, and for 256 bit keys AES performs 14 rounds.

4)-Software implementable in Java and C.

5) - Provide full design details.

AES Algorithm

AES is a Symmetric encryption algorithm which is stands for Advanced Encryption Standard.Vincent Rijmen and Joan daemon the two cryptographer's designed the AES algorithm.Widely used symmetric algorithm is AES-128, AES-192 and AES-256. United. State government approved theAES algorithm in 2000 and is now used worldwide. Now AES has been adopted by United. State government. In AES single key is used to encrypt or decrypt the sensitive data. AES works on a 4*4 order of the matrix. AES is developed to overcome the drawbacks of DES hence we can also say that AES is an advanced version of DES (Data Encryption Standard).

A- Initial Round

- Add-Round-Key

B-Main Rounds (These phases are periodically repeated)

- Substitute Byte
- Shift Row
- Mix Columns
- Add-Round-Key

C-Final Round

- Substitute Byte
- Shift Rows
- Add-Round-Key

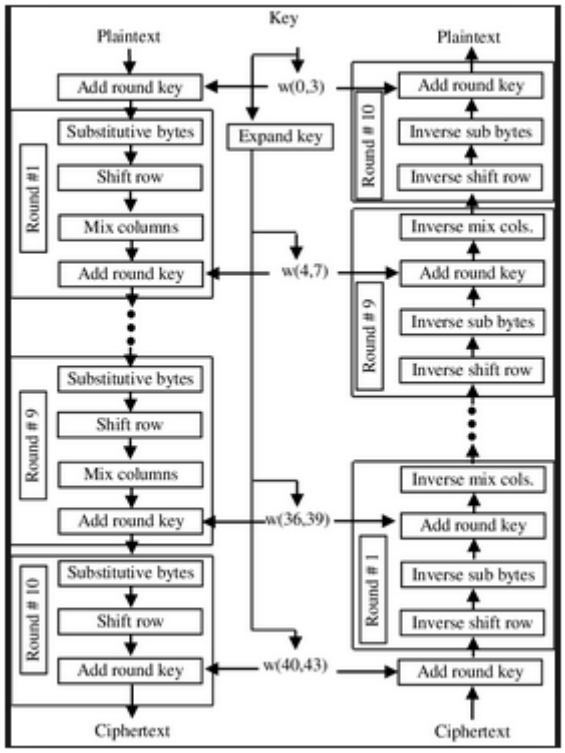

Fig. 1: Encryption process and decryption process [6]

D- Byte Substitution

In this phase involves breaking the input into bytes and passing each bytes by an S-Box.

Every byte is replaced according to a calculated table.

The result is in a 4*4 matrix.

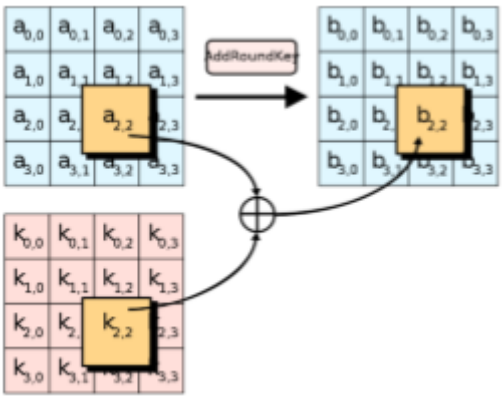

Fig. 2: Byte Substitution

E- Shift Rows

In this step, matrix rows are moved to the left. Any data that are 'left' are re-inserted.

-First row is not moved.

-In Shift Rows Second one is moved by one offset to the left.

-The third row is moved by offsets of two.

-The fourth row is moved by offset of three.

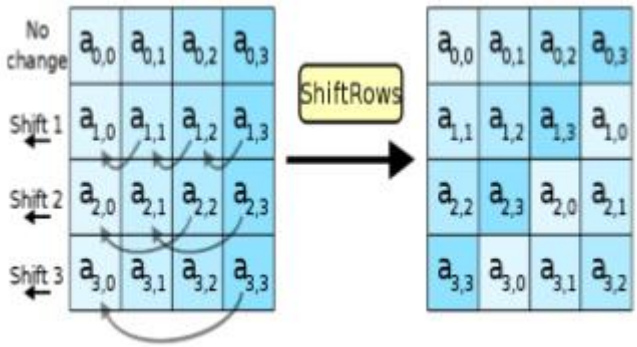

Fig. 3: Shift Rows

F- Mix columns

Each column has a measured calculation applied to it in-order to further diffuse it. Like the Shift Rows phase, the Mix Columns phase mix the input around. This phase provides diffusion of input. Unlike ShiftRows, Mix Columns performs tasks, splitting the matrix by columns rather than rows.

2 3 1 1
1 2 3 1
1 1 2 3
3 1 1 2

G- Add-Round-Key

The matrix of 16 bytes are now considered as 128 bits.

The Add-Round-Key task is the only operation of AES encryption that works on the AES round key.

Decryption process-

The decryption process is just like the encryption process but in the opposite order. In the decryption process cipher text is converted into plain text.

It has 3 rounds-

1) – Final Round

- Add-Round-Key
- Shift-Rows
- Sub Bytes

2) – Main Round

- Add-Round-Key
- Mix Columns
- Shift-Rows
- Substitute Bytes

3) – Starting Round

- Add-Round-Key

Advantage of AES Algorithm-

1) -AES is more secure than DES,

2) -AES is faster in both hardware and software.

3) - AES uses minimum time to execute cloud data.

4) – AES uses a single Substitute-Box for each bytes in all rounds.

CONCLUSION

The paper discuss cloud computing and how AES works in a data. Security is very important for cloud success. AES is a fastest algorithm to secure the cloud data. Multiple attacks tried to break AES like Square attack, differential attack, improved square attack, Key attack, but no one is able to break this algorithm.For 128 bit, hackers need to attempt 2^{128}times to break this algorithm. That's why AES is very secure. Performance of AES is better than other algorithms. And it has least storage space. However, like Data Encryption standard, security of Advance Encryption standard is assured only if it is accurately executed and better key management is used.

REFERENCES

1 - Vishal R. Pancholi, Dr.Bhadresh P. Patel “Enhancement of Cloud Computing Security with Secure Data Storage using AESIJIRST –International Journal for Innovative Research in Science & Technology| Volume 2 | Issue 09 | February 2016.

2- https://www.garykessler.net/library/crypto.html

3-http://www.omnisecu.com/security/public-key-infrastructure/asymmetric-encryption-algorithms.php

4- AmitVerma, Simarpreet Kaur, Bharti Chhabra "Improvement in the Performance and Security of Advanced Encryption Standard Using AES Algorithm and Comparison with Blowfish” International Research Journal of Engineering and Technology (IRJET)Volume: 03 Issue: 10 | Oct -2016.

5- N. Velmurugan, S. Godfrey Winster “Implementation of Enhanced AES for Secure and Efficient Data Storage in Cloud Environment” International Journal of Pure and Applied Mathematics Volume 119 No. 16 2018, 3511-3517

6 - P.V.NITHYABHARATHI, T.KOWSALYA, V.BASKAR “To Enhance Multimedia Security in Cloud Computing Environment Using RSA and AES” International Journal of Science, Engineering and Technology Research (IJSETR), Volume 3, Issue 2, February 2014

7- GurpreetKaur, Dr GagandeepJagdev “Implementation of DES and AES Cryptographic Algorithms in Accordance with Cloud Computing” International Journal of Research Studies in Computer Science and Engineering (IJRSCSE) Volume 4, Issue 4, 2017, PP 1-14