Enhancement of Cloud Computing Security with Secure Data Storage using AES

Vishal R. Pancholi
Research Scholar
Pacific University Udaipur, Rajasthan

Dr. Bhadresh P. Patel
I/C Principal
Matrushri L.J Gandhi (Bakorvala) BCA College Modasa, Gujarat

Abstract

The evolution of Cloud computing makes the major changes in computing world as with the assistance of basic cloud computing service models like SaaS, PaaS, and IaaS an organization achieves their business goal with minimum effort as compared to traditional computing environment. On the other hand security of the data in the cloud database server is the key area of concern in the acceptance of cloud. It requires a very high degree of privacy and authentication. To protect the data in cloud database server cryptography is one of the important methods. Cryptography provides various symmetric and asymmetric algorithms to secure the data. This paper presents the symmetric cryptographic algorithm named as AES (Advanced Encryption Standard). It is based on several substitutions, permutation and transformation.

Keywords: Cloud Computing, Security, Cryptography, AES

I. INTRODUCTION

Cloud Computing is a set of IT Services that are provided to a customer over a network and these services are delivered by third party provider who owns the infrastructure. It is often provided "as a service" over the Internet, typically in the form of infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS) [6]. Cloud computing is the broader concept of infrastructure convergence. This type of data centre environment allows enterprises to get their applications up and running faster, with easier manageability, and less maintenance to meet business demands. For example, we can manage and store all smartphones or tablets apps at one location i.e. cloud. So we do not require any memory space at our end. This also gives the security of data and applications in case device is damaged or lost [1].

As the central data storage is the key facility of the cloud computing it is of prominent importance to provide the security. The art and science of concealing the messages to introduce secrecy in information security is recognized as cryptography.

Security goals of data cover three points namely: Availability, Confidentiality, and Integrity. Cryptography, in modern days is considered grouping of three types of algorithms. They are

1) Symmetric-key algorithms
2) Asymmetric-key algorithms
3) Hash functions

Symmetric algorithms use the same key for encryption and decryption. This is termed as secret key. With the same key messages are encrypted by the sender and decrypted by the receiver. It contains algorithms like Data Encryption Standard (DES), Advanced Encryption Standard (AES), Ron's Code (RCn), and Triple DES, Blowfish etc.

Asymmetric algorithms use different keys. One key (public) is used for encryption and other (private key) is used for decryption. This is named as public key. Public key is known to public and private key is known to the user. It comprises various algorithms like Rivest, Shamir, & Adleman (RSA), Digital Signature Algorithm (DSA), Elliptic Curve(EC), Diffi-Hillman(DH), El Gamal etc.

The Hash functions use a mathematical transformation to irreversibly "encrypt" information. It contains algorithms like Message Digest, Secure Hash Algorithm [10].

We choose symmetric cryptosystem as solution as it has the speed and computational efficiency to handle encryption of large volumes of data. In symmetric cryptosystems, the longer the key length, the stronger the encryption.

AES is most frequently used encryption algorithm today this algorithm is based on several substitutions, permutations and linear transformations, each executed on data blocks of 16 byte. As of today, no practicable attack against AES exists. Therefore, AES remains the preferred encryption standard for governments, banks and high security systems around the world.

II. LITERATURE REVIEW

In [1], it is proposed a simple data protection model where data is encrypted using Advanced Encryption Standard (AES) before it is launched in the cloud, thus ensuring data confidentiality and security.

In [4], a privacy-preserving public auditing system for data storage security in cloud computing is intended, although the computational time is increased but the privacy is preserved where data is stored in the cloud by using the most prominent algorithm AES.

In [8], AES data encryption is more scientifically capable and graceful cryptographic algorithm, but its main force rests in the key length. The time necessary to break an encryption algorithm is straight related to the length of the key used to secure the communication. AES allows choosing a various type of bits like 128-bit, 192-bit or 256-bit key, making it exponentially stronger than the 56-bit key of DES.

In [3], it is described a new architecture for security of data storage in multicloud. Two mechanisms-data encryption and file splitting are used. When user uploads a file, it is encrypted using AES encryption algorithm. Then that encrypted file is divided into equal parts according to the number of clouds and stored into multicloud. This proposed system enhances the data security in multicloud.

In [12], 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. They also observed that Decryption of AES algorithm is better than other algorithms. From the simulation result, they evaluated that AES algorithm is much better than DES and RSA algorithm.

III. AES ALGORITHM

AES acronym of Advanced Encryption Standard is a symmetric encryption algorithm.

The algorithm was developed by two Belgian cryptographers Joan Daemen and Vincent Rijmen. It is useful when we want to encrypt a confidential text into a decryptable format, for example when we need to send sensitive data in e-mail. The decryption of the encrypted text is possible only if we know the right password. AES is an iterative rather than Feistel cipher. It is based on 'substitution–permutation network'. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations).

A. The First Step

– AddRoundKey

B. The Following Four Functions Are Periodically Repeated

– SubByte
– ShiftRow
– MixColumn
– AddRoundKey

C. Final Step

– SubByte
– ShiftRow
– AddRoundKey

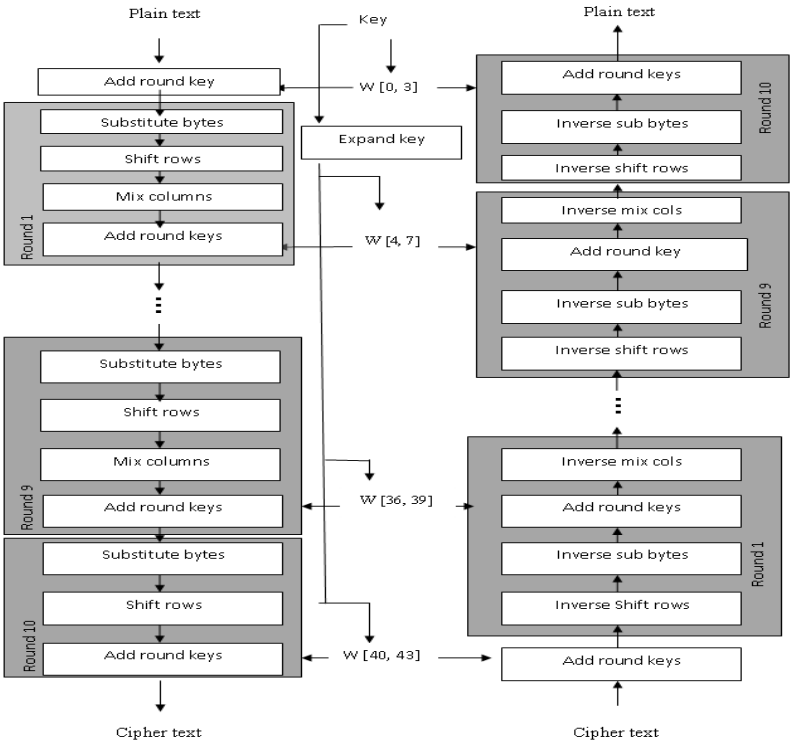

Fig. 1: Encryption and decryption in AES [8]

D. Byte Substitution (SubBytes)

The 16 input bytes are substituted by looking up a fixed table (S-box) given in design. The result is in a matrix of four rows and four columns.

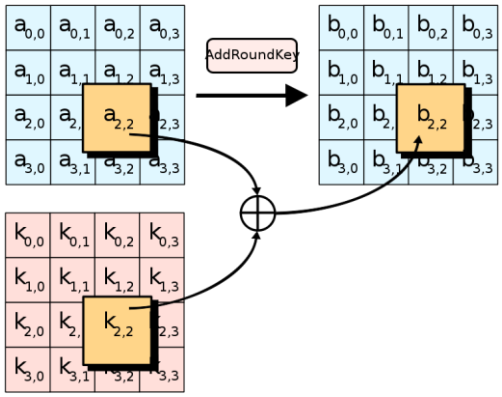

Fig. 2: Byte Substitution (SubBytes)

E. Shift Rows

Each of the four rows of the matrix is shifted to the left. Any entries that 'fall off' are re-inserted on the right side of row. Shift is carried out as follows

- First row is not shifted.
- Second row is shifted one (byte) 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.

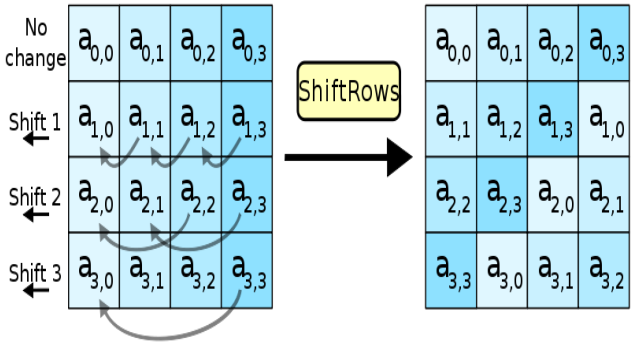

Fig. 3: ShiftRows

F. 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 outputs four completely new bytes, which replace the original column. The result is another new matrix consisting of 16 new bytes. It should be noted that this step is not performed in the last round.

$$\begin{matrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{matrix}$$

G. Addroundkey

The 16 bytes of the matrix are now considered as 128 bits and are XORed to the 128 bits of the round key. If this is the last round then the output is the ciphertext. Otherwise, the resulting 128 bits are interpreted as 16 bytes and we begin another similar round.

IV. CONCLUSION

According to a report, "Worldwide and Regional Public IT Cloud Services 2012-2016 Forecast" released by IDC, cloud services will see as much as 41% growth from 2013 to 2016. Spending on IT cloud services worldwide will edge toward $100 billion by 2016 [13]. And in all this cloud growth, security will play a key role. AES encryption is the fastest method that has the flexibility and scalability and it is easily implemented. On the other hand, the required memory for AES algorithm is less than the Blowfish algorithm. AES algorithm has a very high security level because the 128, 192 or 256-bit key are used in this algorithm. It shows

resistance against a variety of attacks such as square attack, key attack, key recovery attack and differential attack. Therefore, AES algorithm is a highly secure encryption method. Data can also protect against future attacks such as smash attacks. AES encryption algorithm has minimal storage space and high performance without any weaknesses and limitations while other symmetric algorithms have some weaknesses and differences in performance and storage space.

REFERENCES

[1] Abha Sachdev, Mohit Bhansali "Enhancing Cloud Computing Security using AES Algorithm" International Journal of Computer Applications (0975 – 8887) Volume 67– No.9, April 2013
[2] Dr.S.Gunasekaran, M.P.Lavanya " A REVIEW ON ENHANCING DATA SECURITY IN CLOUD COMPUTING USING RSA AND AES ALGORITHMS" (IJAER) 2015, Vol. No. 9, Issue No. IV, April ISSN: 2231-5152
[3] Rashmi S. Ghavghave, Deepali M. Khatwar "Architecture for Data Security In Multicloud Using AES-256 Encryption Algorithm" International Journal on Recent and Innovation Trends in Computing and Communication Volume: 3 Issue: 5 ISSN: 2321-8169
[4] Mr. Santosh P. Jadhav, Prof. B. R. Nandwalkar "Efficient Cloud Computing with Secure Data Storage using AES" International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 6, June 2015 ISSN (Online) 2278-1021
[5] Namita N. Pathak, Prof. Meghana Nagori "Enhanced Security for Multi Cloud Storage using AES Algorithm" International Journal of Computer Science and Information Technologies, Vol. 6 (6), 2015 ISSN:0975-9646
[6] R. H. Sakr, F. Omara, O. Nomir "An Optimized Technique for Secure Data Over Cloud OS" International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) Volume 3, Issue 3, May-June 2014 ISSN 2278-6856
[7] Ranjit Kaur, Raminder Pal Singh "Enhanced Cloud Computing Security and Integrity Verification via Novel Encryption Techniques" SSRG International Journal of Mobile Computing & Application (SSRG-IJMCA) – volume 2 Issue 3 May to June 2015
[8] 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
[9] T. Shobana Maheswari, S. Kanagaraj and Shriram K. Vasudevan "Enhancement of Cloud Security Using AES 512 Bits" Research Journal of Applied Sciences, Engineering and Technology ISSN: 2040-7459; e-ISSN: 2040-7467 November 25, 2014
[10] Disha Shah, "Digital Security Using Cryptographic Message Digest algorithm", International Journal of Advance Research in Computer Science and Management Studies, Volume 3, Issue 10, October 2015.
[11] Dr. Prerna Mahajan & Abhishek Sachdeva "A Study of Encryption Algorithms AES, DES and RSA for Security" Global Journal of Computer Science and Technology Network, Web & Security Volume 13 Issue 15 Version 1.0 Year 2013 Online ISSN: 0975-4172 & Print ISSN: 0975-4350
[12] Rachna Arora, Anshu Parashar " Secure User Data in Cloud Computing Using Encryption Algorithms" International Journal of Engineering Research and Applications (IJERA) Vol. 3, Issue 4, Jul-Aug 2013 ISSN: 2248-9622
[13] Enterprise and Individual Users to fuel Growth in Cloud Computing [Online]. Available: http://www.redorbit.com/news/technology/1112692915/cloud-computing-growth-paas-saas-091212/
[14] Kiruthika.R, Keerthana.S, Jeena.R " Enhancing Cloud Computing Security using AES Algorithm" International Journal of Advanced Research in Computer Science and Software Engineering Volume 5, Issue 3, March 2015 ISSN: 2277 128X