International Journal of Research in Engineering, Science and Management
Volume-3, Issue-1, January-2020
www.ijresm.com | ISSN (Online): 2581-5792


# Enhancement of Cloud Computing Security with Secure Data Storage Using AES

D. N. Mohan[1], V. Hemanth Kumar[2], N. Shashank[3]
[1]*Assistant Professor, Department Information Science & Engineering, Nagarjuna College of Engineering & Technology, Bangalore, India*
[2,3]*Student, Department Information Science & Engineering, Nagarjuna College of Engineering & Technology, Bangalore, India*

***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.**

## 1. 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.

## 2. 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).

The first step: AddRoundKey

The following four functions are periodically repeated

- SubByte
- ShiftRow
- MixColumn
- AddRoundKey

Final step

- SubByte
- ShiftRow
- AddRoundKey

*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.

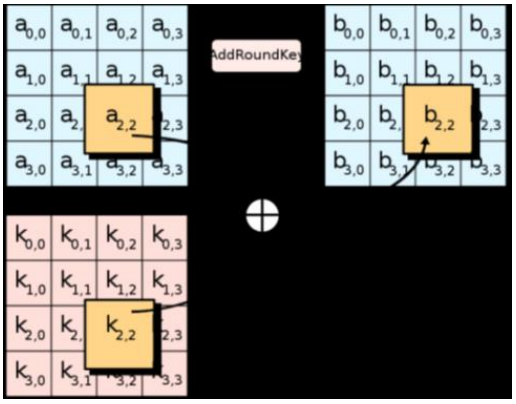


Fig. 1. Byte substitution (sub bytes)

*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.

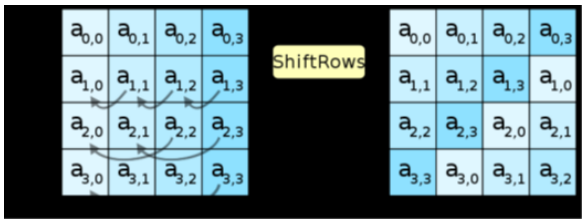


Fig. 2. Shift rows

*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.

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

*Add round key*

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.

## 3. 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 Enhancement of Cloud Computing Security with Secure Data Storage using AES 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, volume 67, no. 9, April 2013.

[2] S. Gunasekaran, M. P. Lavanya "A review on enhancing data security in cloud computing using RSA and AES algorithms," vol. 9, no. 4, April 2015.

[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, vol. 3, no. 5.

[4] Mr. Santosh P. Jadhav, B. R. Nandwalkar "Efficient Cloud Computing with Secure Data Storage using AES" International Journal of Advanced Research in Computer and Communication Engineering, vol. 4, no. 6, June 2015.

[5] Namita N. Pathak, Meghana Nagori, "Enhanced Security for Multi Cloud Storage using AES Algorithm" International Journal of Computer Science and Information Technologies, vol. 6 (6), 2015.