Data Storage Security in Cloud Computing Using AES under AKPA

D. Srinivasulu Reddy[1], M.Tech, ISTE, Associate Professor in Deportment of CSE, PBR Visvodaya Institute of Technology and Science, Kavali, Nellore.

Maramreddy Srihari[2], pursuing Master of Computer Applications (MCA) from PBR Visvodaya Institute of Technology and Science, Kavali, Nellore.

----------ABSTRACT----------

Distributed computing is the novel pattern in everywhere throughout the world. Distributed computing gives the capacity to use assets through Internet. As a great deal of specialist organizations of the cloud are accessible in the aggressive PC world. Security in Cloud registering is an essential and basic perspective, and has various issues and issue identified with it. In this we will talk about how to give security to the information from the unapproved clients and give uprightness to the clients. It requires an extremely high level of security and validation. To secure the information in cloud database server, cryptography is one of the imperative strategies. Cryptography gives different symmetric and topsy-turvy calculations to verify the information. This paper shows the symmetric cryptographic calculation named as AES (Advanced Encryption Standard). It depends on a few substitutions, stage and change.

Keywords - **Cloud Computing, Cryptography, Security, AES**

1. INTRODUCTION

Cloud computing is a set of IT Services evolving as the next generation .This service provided to a customer over a network and these services are delivered by third party provider who owns the infrastructure. The data is stored in remote sector. Cloud Computing is the combination of a technology, platform that provides hosting and storage service on the Internet. Cloud computing is sharing of resources on a larger scale which is cost effective and location independent. There are three types of cloud according to their usage. They are private cloud, public cloud and hybrid cloud. The private cloud is owned by a single organization and public clouds are shared on a larger scale. Hybrid cloud is a combination of Private cloud and Public Cloud which is used by most of the industries. Private cloud provides better control and more flexibility. It is provided three levels of "as a service" over the Internet (i) infrastructure as a service (IaaS)- provides hardware and software and equipment to deliver software application environments with a resource usage, (ii)platform as a service (PaaS)-offers an integrated environment to build test and deploy customer applications.,(iii) software as a service (SaaS)- software development model where applications are remotely hosted by an application or service provider and made available to customer via the Internet. Cloud computing is the broader concept of infrastructure convergence. Cloud computing can manage and store all smart phones or tablets apps at one location. So we do not require any memory space at our end. The advantages of cloud computing may be very appealing but nothing is perfect. Cloud got many issues when it comes to security especially on Data theft, Data loss and Privacy. The parameters that affect the security of the cloud and problems faced by cloud service provider and cloud service consumer such as data, privacy, infected application and security issues. This also gives the security of data and applications in case device is damaged or lost.

Figure 1: General Structure of Cloud Computing

2. CRYPTOGRAPHY

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

SYMMETRIC-KEY ALGORITHMS

Symmetric algorithms used the same (secret key) key for encryption and decryption. The same key messages are used for encrypted by the sender and decrypted by the receiver. It contains algorithms like Data Encryption Standard (DES), Advanced Encryption Standard (AES), IDEA Twofish, Ron's Code (RCn), and Triple DES, Blowfish etc.

ASYMMETRIC-KEY OR PUBLIC KEY ALGORITHMS

Asymmetric algorithms use different keys. One key (public) is used for encryption and other (private key) is used for decryption. It comprises various algorithms like Rivest, Shamir, & Adleman (RSA), Digital

Signature Algorithm (DSA), Elliptic Curve(EC), Diffi-Hillman(DH), El Gamal and Schnoor etc.

HASH FUNCTIONS OR MESSAGE DIGESTS

The Hash functions use a mathematical transformation to irreversibly "encrypt" information. It is handle the two functions are authentication and secrecy. It contains algorithms like Message Digest(MD5), Secure Hash Algorithm.

We choose symmetric cryptosystem as solution as it has the speed and computational efficiency to handle encryption of large volumes of data. It is using the longer key length and good 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. Therefore, AES remains the preferred encryption standard for governments, banks and high security systems around the world.

3. SECURITY

There are numerous security issues for cloud computing as it encompasses many technologies including networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, concurrency control and memory management. The cloud service provider for cloud makes sure that the customer does not face any problem such as loss of data or data theft. There are four types of issues raise while discussing security of a cloud.

DATA ISSUES

Sensitive data in a cloud computing environment emerge as major issues with regard to security in a cloud based system. Firstly, whenever a data is on a cloud, anyone from anywhere anytime can access data from the cloud since data may be common, private and sensitive data in a cloud. Thus there is a need of some data integrity method in cloud computing. Secondly, data stealing is a one of serious issue in a cloud computing environment. Thirdly, Data loss is a common problem in cloud computing. The data can be lost or damage or corrupted due to miss happening, natural disaster, and fire. Fourthly, data location is one of the issues what requires focus in a cloud computing environment. Physical location of data storage is very important and crucial. It should be transparent to user and customer. Vendor does not reveal where all the data's are stored.

SECRECY ISSUES

The cloud computing service provider must make sure that the customer personal information is well secured from other providers, customer and user. As most of the servers are external, the cloud service provider should make sure who is accessing the data and who is maintaining the server so that it enable the provider to protect the customer's personal information.

INFECTED APPLICATION

Cloud computing service provider should have the complete access to the server with all rights for the purpose of monitoring and maintenance of server. So this will prevent any malicious user from uploading any infected application onto the cloud which will severely affect the customer and cloud computing service.

SECURITY ISSUES

Cloud computing security must be done on two levels. One is on provider level and another is on user level. the cloud computing service provider has provided a good security layer for the customer and user and the user should make sure that there should not be any loss of data or stealing or tampering of data for other users who are using the same cloud due to its action.

4. AES ENCRYPTION AND DECRYPTION

AES acronym of Advanced Encryption Standard is a symmetric encryption algorithm published by the National Institute of Standards and Technology (NIST). AES fall into three areas Security, Cost and Implementation. 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 decrypt able format. 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).

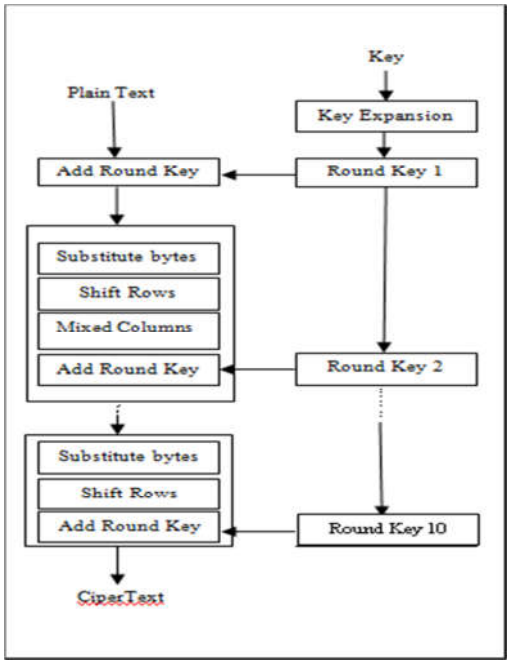

Figure 2: Encryption in AES

AES uses four types of transformations: Byte substitution (SubBytes), permutation (Shift Rows), mixing(Mix columns) and Add round key.

BYTE SUBSTITUTION (SUB BYTES)

Sub Byte does a byte-for-byte substitution on state.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.

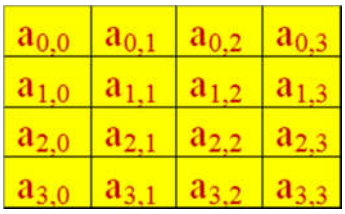

Figure 3: Byte substitution

PERMUTATION (SHIFT ROWS)

Each of the four rows of the matrix is rotated to the left. Any entries that 'fall off' are re-inserted on the right side of row. Shift is carried out as Row1 is not rotated. Row2 is rotated one (byte) position to the left. Row3 is rotated two positions to the left. Row4 is rotated three positions to the left. The result is a new matrix consisting of the same 16 bytes but shifted with respect to each other.

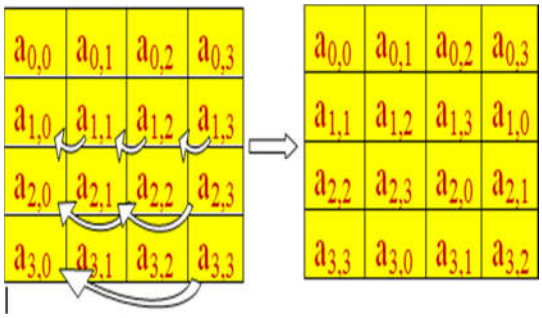

Figure 4: Shift Rows

MIXING (MIX COLUMNS)

Each column of four bytes is now transformed using a matrix multiplication using(finite GaloisField-GF(28)). 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.

ADD ROUND KEY

In the AddRoundKey step, the subkey is combined with the state. For each round, a subkey is derived from the main key using Rijndael's key schedule; each subkey is the same size as the state. The subkey is added by combining each byte of the state with the corresponding byte of the subkey using bitwise XOR.

Decryption

In decryption all encryption step is reversible .Finally we get the original plain text.

5. CONCLUSION

Cloud computing is a promising and emerging technology for the next generation of IT applications. The barrier and hurdles toward the rapid growth of cloud computing are data security and privacy issues. 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. At the same time cloud computing technology is not just a technical problem, it is also involves standardization, supervising mode, laws and regulations, and many other aspects, cloud computing is accompanied by development opportunities and challenges, along with the security problem be solved step by step, cloud computing will grow, the application will also become more and more wide.

REFERENCES

[1] Ch. Chakradhara Rao and A.V.Ramana DATA SECURITY IN CLOUD COMPUTING International Journal of Current Trends in Engineering & Research (IJCTER)

[2] Vishal R. Pancholi Dr. Bhadresh P. Patel Matrushri L.J Gandhi (Bakorvala)and Enhancement of Cloud Computing Security with Secure Data Storage using AES

[3] Sreedhar Acharya B. and Dr. M. Siddappa A Novel Method of Designing and Implementation of Security Challenges in Data Transmission and Storage in Cloud Computing International Journal of Applied Engineering Research

[4]Andrew S.Tanenbaum Computer Network

[5] Monjur Ahmed and Mohammad Ashraf Hossain, "Cloud Computing and Security Issues in the Cloud", International Journal of Network Security (IJNSA), Vol.6, No.1, January 2014.

[6] Rohit Maheshwari, Sunil Pathak, "A Proposed Secure Framework for Safe Data Transmission in Private Cloud", International Journal of Recent Technology and

Engineering (IJRTE) ISSN: 2277- 3878, Volume-1, Issue-1, April 2012.

[7] D. Kanchana, Dr. S. Dhandapani, "A Novel Method for Storage Security in Cloud Computing", International Journal of Engineering Science and Innovative Technology (IJESIT), ISSN: 2319-5967, Volume 2, Issue 2, March 2013.

[8] Arijit Ukil, Debasish Jana and Ajanta De Sarkar, "A Security Framework In Cloud Computing Infrastructure", International Journal of Network Security & Its Applications (IJNSA), Vol.5, No.5, September 2013.

[9] Ahmed E. Youssef and Manal Alageel, "A Framework for Secure Cloud Computing", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 4, No 3, July 2012, ISSN: 1694-0814

[10] Ayesha Malik, Muhammad Mohsin Nazir, "Security Framework for Cloud Computing Environment: A Review", Journal of Emerging Trends in computing and Information Sciences, ISSN 2079-8407, VOL.3, No.3, MARCH 2012.

D. Srinivasulu Reddy[1], M.Tech, ISTE, Associate Professor in Deportment of CSE, PBR Visvodaya Institute of Technology and Science, Kavali, Nellore.

Maramreddy Srihari[2], pursuing Master of Computer Applications (MCA) from PBR Visvodaya Institute of Technology and Science, Kavali, Nellore.