A REVIEW ON ENHANCING DATA SECURITY IN CLOUD COMPUTING USING RSA AND AES ALGORITHMS

Dr.S.Gunasekaran, M.P.Lavanya
Professor, CSE,
Coimbatore Institute of Engineering and Tech,
Coimbatore
PG Scholar,
Coimbatore Institute of Engineering and Tech,
Coimbatore

ABSTRACT

Cloud computing is a new computational paradigm that offers an innovative business model for an organization to adopt IT without upfront investments. It provides enormous storage for data and computing to customers over the internet. Cloud Computing gained great responsiveness from the industry but still there are many issues that are hampering the growth of the cloud. Security of data in cloud is one of the major issue which is more complication in the implementation of cloud computing. These security issues are avoided by various encryption algorithms. This work presents a review on various encryption algorithms to enhance the data security in cloud computing.

***Keywords**: Cloud Computing,Data Security, RSA, AES.*

INTRODUCTION

Cloud computing is a model which allows the user to use the services by the service provider on pay per use basis. Cloud computing is a concept of using remote services through a network using various resources. According to NIST"Cloud computing is a model for enabling, convenient, on demand network access to a shared pool of configurable resources that can be rapidly provisioned and released with minimal management effort or service provider interaction".

The great flexibility and economic saving of cloud computing are monitoring all kinds of users such as customers, enterprise and even government organizations to adopt cloud.The cloud computing model has three functional units. They are: i)Cloud service provider, ii)Client/owner, iii) User

Cloud Service Models:

The major cloud computing service models are known as Software as a service, Platform as a Service and Infrastructure as a Service.

Software as a Service(SaaS): It is a software distribution model in which applications are hosted by vendor.

Platform as a Service (PaaS): It is a program paradigm for delivering operating systems over internet.

Infrastructure as a Service (IaaS): It involves outsourcing the equipment used to support operations, including hardware servers and networking components.

Securing data is always a vital significance, because the cloud computing lugs a large amount of complex data. Therefore data privacy and security are issues that need to be resolved [7]**.**The foremost security issues in cloud computing are, i) Privacy and Confidentiality,ii) Security and Data Integrity.Once the clients farm out the data to the cloud, there must be some declaration that data is reachable to only authorized user. The cloud user guaranteed the data stored on the cloud will be confidential.Data security can be provided using innumerable encryption and decryption techniques. With providing the security of the data, cloud service provider should also implement mechanism to monitors integrity of the data at the cloud.

There are various attacks incloud computing, they are: i) Tampering, ii) Repudiation, iii) Eavesdropping information disclosure, iv) Identity Spoofing. Tampering occurs when an attacker may alter the information either stored in local files or database is showed over public network. Repudiation occurs when sender tries repudiating the validity of a statement which is sent by him/her. Eavesdropping information disclosure occurs when attacker gain access in the data path and gains access to monitor and read the messages Identity spoofing occurs when an attacker impersonates the users as the originator of the message in order to gain access on a network.

LITERATURE REVIEW

A. Ensure Data Communication Using RSA, AES in Cloud Computing:

Nirosha andK.Suma Latha [3] proposed RSA, AES encryption algorithms are used with the erasure coding for secure data forwarding. Constructing a cloud storage system for secure data forwarding using encryption and decryption techniques. For encryption, use the proxy re-encryption scheme integrating with RSA algorithm.

The encryption scheme supports encoding operations over encrypted messages and forwarding operations over encrypted and encoded messages. A secure distributed storage system is formulated by partitioning the data and performing encryption key at user and regenerating it at key servers on demand for partial decryption. In this work, the cryptographic schemes are used; RSA is used for encryption at first time. AES is used for re-encryption, (i.e.) RSA is used for key generation and encryption of data blocks. AES is used for re-encryption of cipher blocks.The goal of proxy re-encryption is to securely enable the re-encryption of cipher texts from one secret key to another without relying on trusted parties.Erasure coding is k blocks of secure data are encoded to n blocks of encoded data, such that the source data can be reconstructed from any subset of k encoded blocks. Each block is operated by arithmetic operations. Fig. 1 shows the data is divided into blocks of user A and encrypts the block and send the cipher blocks to storage servers. User performs re-encryption when data blocks are needed to be forwarded. When user B wants the data queries the key servers. Key servers retrieve the data from storage servers after decoding process is performed and the partial decryption is done by key servers after generating the re-encryption key on demand for partial decryption.

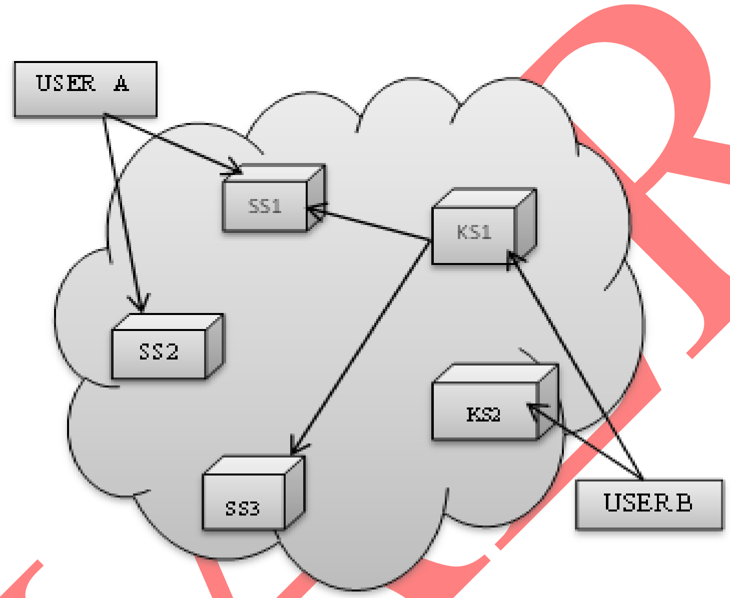

Fig.1 A General Architecture For Secure Data Forwarding.

B.An Improved RSA Encryption Algorithm for Two Key Generation Algorithm (2KGA):

Shubhra saagar and Datta [5] proposed the cryptography concepts to upturn the security of encrypted cloud data in cloud servers with minimum consumption of cost and time at both encryption and decryption processes. Dual encryption processes has been applied to avoid common attacks against RSA algorithms.Two Key Generation Algorithm is used based on the strengths of efficient RSA and RSA small-e. In this algorithm, the number of exponents will be increased to three. The Two Key Generation Encryption Algorithm has the following steps:

A. Key Generation Algorithm:

a. Randomly and secretly choose two large primes: **p, q** and compute n=p.q
b. Compute α n=p-1 q-1.
c. Compute β n, h=ph-p0 ph-p1….ph-ph-1+qh-q0 qh-q1….qh-qh-1.
d. Select Random Integer: r such as 1<r<n and gcd r,α=1 and gcd r,β=1(r should be small integer)
e. Compute e such as r.e ≡ mod α n and 1<e<α n.

f. Compute d such as r.d ≡ mod β n and 1<d<β n.

g. Public Key: e, n

h. Private Key: r,d,n

B. Encryption Processes:

a. Entity A needs to send message m to Entity B

b. Entity B should send his public key to Entity A

c. Entity A will encrypt m as: c= ((m^{e} mod n)e mod n)

d.After that Entity A will send c to Entity B

C. Decryption Processes:

a.Entity B will decrypt the message as m= ((cr mod n)d mod **n).**In this algorithm r is used as a third exponent defined according to RSA small-e.In proposed algorithm, dual encryption process is applied to increase the security level of the algorithm comparison of original RSA.

C. Enhance Data Security Using RSA and MD5:

Sudhansu and Biswaranjan [6] proposed a work for increase the confidentiality and authentication of data by using RSA and MD5 algorithms. Two algorithms are implemented; one is for encryption and decryption. The other algorithm is for authentication purpose. For the secure communication, user send the request to provider that requests are encrypted by using system's public key by RSA. When the user gets the file, after that the user's browser decrypts using the system's private key. After gets connected with the system the user can upload or download files from the server. When the user wants to upload a file, encrypts using system's public key. For each request of user the system randomly generated different keys for both encryption and decryption. After receiving the encryption key, user encrypts the file.MD5 algorithm is used for preventing from unauthorized access for the key. For authentication, using MD5 algorithm user generates the message digest. After receiving the digital signature, from the user, the same MD5 algorithm used for verification. Once the verification is done, the encrypted file is stored on the storage server in the user name. In this model, intruders cannot easily access or upload the file because the algorithms are executed in different servers at different locations.

Let's assume two organizations A and B. Organization B wants a secure data from A's cloud. So send the secure data by using digital signature along with RSA encryption algorithm diagrammatically described in fig 2. Using the RSA encryption algorithm Organization A will encrypt the message by using B's public key. Then the file will be processed large volume of data into fixed few lines by using MD5 algorithm to generate message digest.

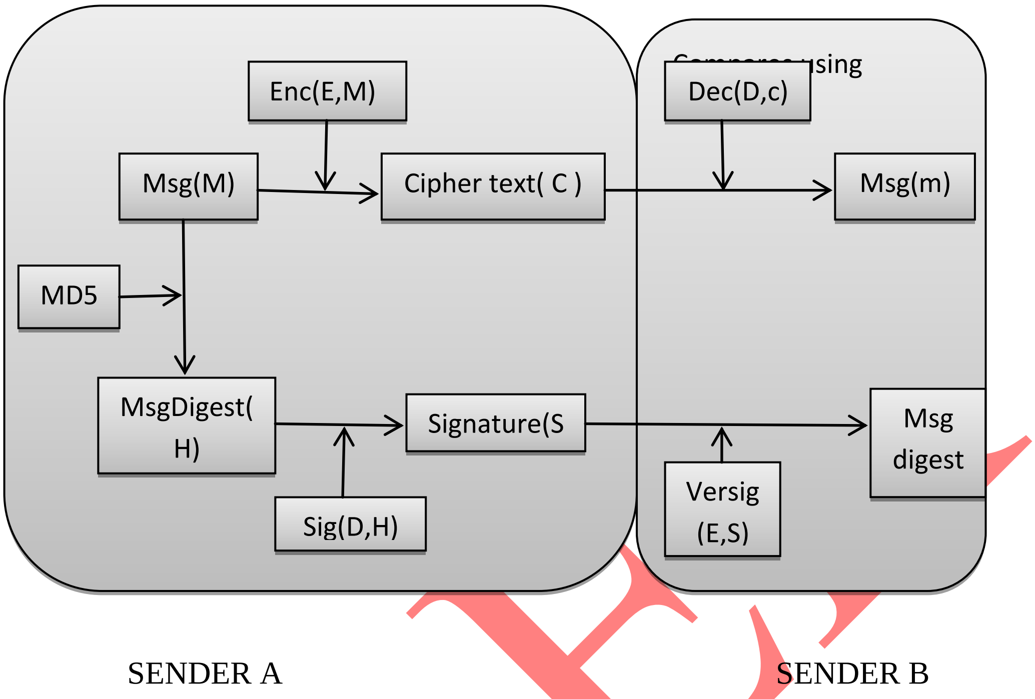

Fig.2 Working of Digital Signature with RSA Encryption Algorithm

A then encrypt the message digest using its own private key to digital signature. B will decrypt the message using his own private key and finally the signature is verified using A’s public key.

D.Enhancing Data Security Using AES:

Abha and Mohit [1] proposed a work for simple data protection model to encrypt the data using Advanced Encryption Standard(AES), that ensuring the data confidentiality and security. CSP cannot provide encryption granularity to each user at each level. So need encryption solution between user applications and database servers in the cloud initiated by the user. Choose symmetric cryptosystem as solution as it has the speed and computational efficiency to handle large volume of data.

In this model the user decides to use the cloud services and transfer the data on cloud. User submits service requirements with CSP’s and chooses provider offering best specified services. Whenever an application uploads any data on cloud, the data is encrypted and then sent. The encryption process is done using AES algorithm. Once the data is encrypted, then it can upload on to the cloud. Any requests to read the data will happen after it is decrypted on the user end. And then the plain text can be read by the requesting application. AES provides greater security to cloud users as encrypted data and prevents the cloud users from many attacks. Thus AES provides security to cloud users as encrypted data in the cloud is safe from several attacks.

COMPARISON

In the below table a comparative study of RSA, AES encryption algorithms in cloud computing founded on the reviews based on the various parameters.[4].

Table1: Comparison between RSA, AES algorithms

Name of Title	Algorithm Used	Parameters					
		Block Size	Key Size	Algorithm	Security	Ciphering and Deciphering Key	Ciphering and Deciphering Algorithm
Ensure Data Communication Using RSA, AES in Cloud Computing	AES, RSA	128bits,Min 512 bits	128,192,256 bits,>1024 bits	Symmetric algorithm, Asymmetric algorithm	Secured	Different, Same	Different ,Same
An Improved RSA Encryption Algorithm for Two Key Generation Algorithm (2KGA)	RSA	128 bits	2048 bits	Asymmetric algorithm	Secured	Same	Same
Enhance Data Security Using RSA and MD5	RSA,MD5	128 bits,512 bits	>1024 bits,	Asymmetric algorithm, Hash algorithm	Secured	Same	Same
Enhancing Data Security Using AES	AES	128 bits	128 bits	Symmetric algorithm	Secured	Different	Different

CONCLUSION

Cloud computing allows user to store their data in cloud storage when user required. So cloud is on internet, various security issues are encountered like confidentiality, privacy, authentication. Various cryptographic algorithms used for both encryption and decryption of cloud data to improve the security. Security of cloud depends on trusted computing and cryptography. This paper presents a review on RSA, AES encryption algorithms and using the cryptographic techniques to enhancing a data security in cloud computing.

REFERENCES

[1] Abha Sachdev, Mohit Bhansali, "Enhancing Cloud Computing Security Using AES" International Journal of Computer Applications, April 2013.

[2] Dhaval Patel, M.B. Chaudhari "Data Security in Cloud Computing using Digital Signature", International Journal for Technological Research in Engineering.

[3] Nirosha, K. Suma Latha, "A Comprehensive Approach to Ensure Secure Data Communication in Cloud Environment", International Journal of Advanced Research in Computer Science and Software Engineering, July 2013.

[4] 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.

[5]Shubhra Saggar, R.K.Datta, "An Improved RSA Encryption Algorithm for Cloud Environments: Two Key Generation Encryption(2KGEA)" International Journal of Software and Web Services, Aug 2013.

[6] Sudhansu Ranjan Lenka, Biswaranjan Nayak,"Enhancing a Data Security in Cloud Computing Using RSA Encryption and MD5", International Journal of Computer Science Trends and Technology, June 2014.

[7] Sanjoli single, Tasmeet Singh in "Cloud Data Security using Authentication and Encryption Techniques", International Journal of Advance Research in Computer Engineering & Technology.