International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868
Foundation of Computer Science FCS, New York, USA
Volume 7– No.8, September 2014 – www.ijais.org

Use of Digital Signature Standard with Station to Station Key Exchange Agreement and Cloud Manager to Enhance Security in Cloud Computing

Manoj Kumar
Associate Professor
Delhi Technological University
New Delhi-110042, India

Kranti Asiwal
M.Tech Student
Delhi Technological University
New Delhi-110042, India

ABSTRACT

Cloud computing provides IT as service. Cloud computing is a budding paradigm having high availability, performance, least cost and many others. Cloud is an IT environment based on which it remotely provides IT resources to users. As cloud computing is an internet based computing solution, there are lots of security breaches and vulnerabilities like authenticity, data security, confidentiality and privacy which should be dealt properly to get high performance. Different combinations are used by different researchers to tackle these security breaches and vulnerabilities, same way we have chosen a combination of authentication technique and key exchange with cloud manager. In this paper we have proposed a model to enhance security of cloud by using Station to Station key agreement for generating session key with a fixed timestamp between User and Cloud Server and then send request for any service by using Digital Signature Standard, the request message would be encrypted by using that session key which was shared earlier and once a session key is used then that session key would not be used again. So the user requires a new key for each session. All of these issues related to authentication and authorization are handled by a cloud manager present between cloud server and user.

General Terms

Cloud Security

Keywords

Cloud Computing, Digital Signature Standard, Station to Station key exchange.

1. INTRODUCTION

Cloud Computing is virtual pool of resources and it provides these resources over the internet on pay per usage basis to users. Companies can reduce cost by providing service over internet.

Services provided by cloud are-

1) Platform as a service
2) Software as a service
3) Infrastructure as a service

Since cloud computing is a utility available on internet so security is main concern. So for Security problems we have used authentication technique, verification technique and a manager which will manage everything to enhance security.

As for secure connection between user and server one to one connection is preferable for security purpose that's why session key is generated by Station To Station (STS) key exchange agreement. Station To Station key exchange agreement will establish session keys between user and server for a fixed timestamp and only for single use that means once a session key is used by user for any service then again it won't be used again. After establishment of session key it is used in Digital Signature Standard so as intruders will be unable to decrypt the message sent by user; this message is the request from user to server for a service. All request-response management, session key generation and management are handled by Cloud Manager.

2. PROBLEM STATEMENT

Cloud computing technology provides services over internet so privacy and security is main concern that's why security issues like authentication, confidentiality, privacy should be handled properly. To deal with these problems a scheme where one to one medium is generated by Station To Station for privacy, encryption algorithm are used by cloud manager for data encryption and thus it provides confidentiality and Digital Signature Standard is used as an authentication technique.

3. RELATED WORK

Prashant Rewagad and Yogita Pawar [1]: They have proposed three way architecture to make use of digital signature and diffie hellman key exchange with advance AES to protect confidentiality of data stored in cloud.

Uma Somani, Kanika Lakhani and Manish Mundra [2]: A scheme has been proposed by them in which Digital Signature with RSA algorithm is used to encrypt data while transferring over network.

Siani Pearson, Yun Shen and Miranda Mowbray [5]: They have described Privacy Manager in Cloud Computing for increasing privacy and privacy management.

Siani Pearson [6]: He has described privacy challenges that engineers face while working on cloud computing.

Mandeep Kaur and Manish Mahajan [8]: They have proposed a plan to use different encryption algorithms like – AES, DES, RSA & BLOWFISH to ensure security of data in cloud for the perspective of different users.

4. PROPOSED MODEL

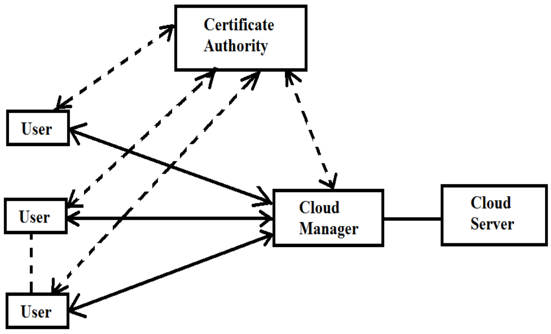

Figure 1: Proposed Model Entities layout

4.1 Parts of model

We are enhancing security of cloud by using Station to Station key agreement with Digital Signature Standard and Cloud Manager.

This model is working on 3 important parts:-

1. Cloud Manager
2. Station to Station key exchange agreement
3. Digital Signature Standard

4.1.1 Cloud Manager:

As its name suggests cloud manager manages everything of cloud server or things related to cloud server.

Cloud manager reduces risk for cloud computing users of their private data being stolen or being misused, and also assists the cloud provider to conform to privacy law.

Cloud Manager acts as a third party to issue session key between user and cloud server, cloud manager will verify user credentials signed by user and then send with request message for using any service from cloud.

After providing any of service to a user from the cloud server cloud manager will remove that session key on which that service was used from session key allocated list managed by cloud manager.

Every time a user requests a file from cloud the cloud manager will decrypt that file where all information regarding all files are present and will check from there that which algorithm has been used on user's required file so as to de-obfuscate i.e. decrypt that file and provide to user.

4.1.1.1 Services provided by Cloud Manager

4.1.1.1.1 Random Obfuscation

When any user stores its file/data on cloud, cloud manager will randomly choose one of the available asymmetric Encryption/Decryption methods to encrypt data provided by user and store it in data storage of cloud. Randomly chosen encryption method information is stored in one file where all of the information of all files is stored and that is encrypted with cloud manager public key.

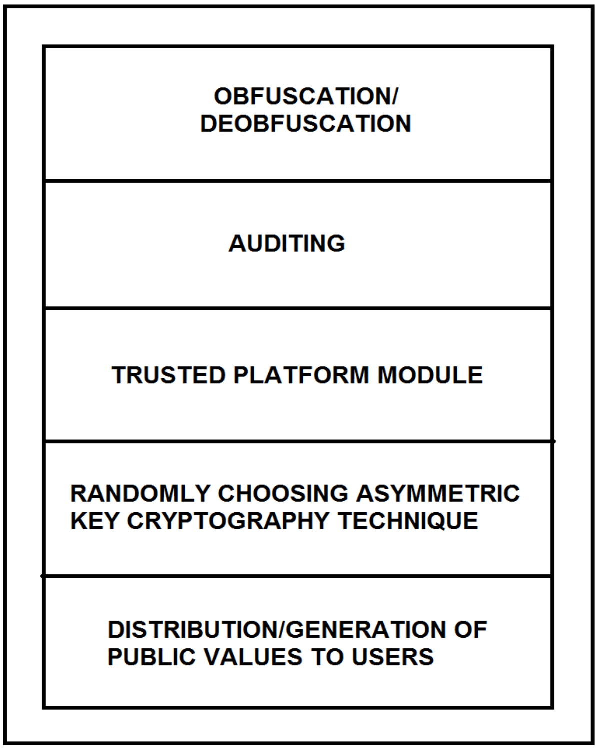
OBFUSCATION/ DEOBFUSCATION
AUDITING
TRUSTED PLATFORM MODULE
RANDOMLY CHOOSING ASYMMETRIC KEY CRYPTOGRAPHY TECHNIQUE
DISTRIBUTION/GENERATION OF PUBLIC VALUES TO USERS

Figure 2: Services Provided by Cloud Manager

After every de-obfuscation, again cloud manager will randomly choose encryption algorithm to obfuscate and store it.

With respect to the privilege of user cloud manager will provide data to him/her i.e. if user is owner then read/write only file is provided and if user is normal user then read only data is provided so that no unwanted changes can be done.

4.1.1.1.2 Auditing

It also act as an auditor by keeping all information regarding what service is provided to users and when, what users did with that service? All information is audited.

4.1.1.1.3 Trusted Platform Module

It is a hardware that checks integrity of cloud manager. It decreases the risk of unsecured access, so increases confidentiality by providing a tamper resistant hardware based security. Protected data cannot be used by other platforms. So trusted computing can be done and it yields trust in integrity of the privacy management and of involved platforms.

4.1.1.1.4 Random Encryption Method

This method is used for obfuscation and de-obfuscation. Cloud manager have a list of asymmetric encryption methods from which it will randomly choose for encryption and save that information in a file which is maintained by it.

4.1.1.1.5 Public Value Generation and Broadcast

Cloud Manager provide values of g, P, q and B to users at the time of registration and broadcast new g, P, q and B values after timestamp is reached. So new public key values and private key values are regenerated by users and their new certificates are created by certificate authority (digital certificates are renewed). g, P, q and B are used in Digital Signature Standard as well as in Station to Station key exchange agreement.

- ($2^{L-1}< P<2^{L}$). L is a multiple of 64.
- q is prime divisor of P-1.
- A random number h is chosen. 0<h<P-1, $g=h^{(P-1)/q}$ modB.
- A value B is also chosen pseudo-randomly or randomly so as to be used in Station to Station Key Exchange Agreement.

A timestamp is set for all these values and when this time expires then these values are regenerated and broadcasted to all users.

4.1.1.2 Files maintained by Cloud Manager

4.1.1.2.1 Audit File

This contains all auditing information.

4.1.1.2.2 Session key allocation file

This file maintains the information about session keys provided to users and their timestamps.

4.1.1.2.3 Data Files obfuscation information

This file has information of files for obfuscation and corresponding encryption methods used.

4.1.1.2.4 Public values File

This file has all values which are public and their timestamps. From this file values are broadcasted to users (Here g, P, q and B are public values, which are broadcasted time to time).

4.1.2 Station To Station Key Exchange Agreement

Station To Station (STS) key exchange agreement is commonly known as Station To Station (STS) protocol. Digital signatures with public key certificates are used to establish session key. It is based on diffie hellman algorithm, as in diffie hellman algorithm man in middle attack can take place but Station To Station key exchange agreement prevents man in middle attack problem. As session keys are created for a fixed timestamp it will increase security level.

4.1.3 Digital Signature Standard

Digital Signature Algorithm is used in Digital Signature Standard (DSS) based on Elgamal scheme with some ideas from Schnorr scheme. DSS signatures are faster than RSA Signatures. DSS signatures are smaller than other Signatures. Message send by user to cloud manager is encrypted by using session key already created by Station To Station key agreement.

4.2 Steps for getting a service from cloud

4.2.1 Registration

- User can register to cloud by providing required information and user name and password.
- After successful registration g, P, q and B values and hashing technique used for creating digests are provided by cloud manager to user.
- Then a random number x is chosen by user and that would be its private key and from that $z = g^{x}$modB is generated, that is its public key (x and z values are renewed time to time when new values of g, P, q and B are received from Cloud Manager).

4.2.2 Station to Station Key Exchange Agreement

Algorithm:

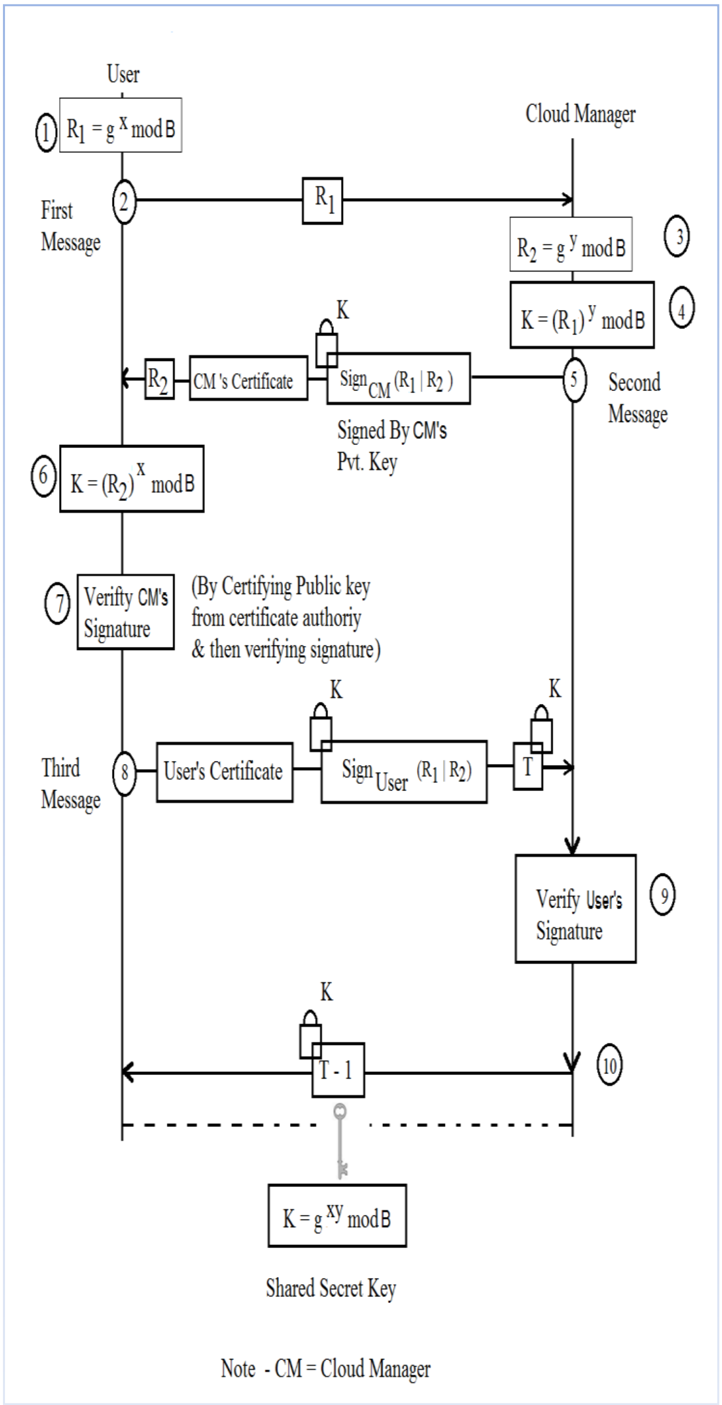

Figure 3: Station to Station Key Exchange Agreement

a) A random number x that is user's private key is already been chosen at the time of registration with a time stamp and will renew it time to time when new g, P, q and B values are received then x is also renewed.

b) New user will calculate $R_1 = g^x$modB & send this R_1 to cloud manager.

c) After getting R_1, cloud manager will choose a random number y & find out R_2.

d) Now cloud manager will find out key (session key) K = $(R_1)^y$modB.

e) After calculating R_2 & the session key, cloud manager concatenates R_1 and R_2 and then signs the result with the private key. Cloud manager now sends R_2, the signature & his own public key certificate to user. Signature is encrypted with session key.

f) Now after getting R_2 user will calculate session key & verify cloud manager signature by the certificate authority

g) After that user will create a signature by concatenate $R_1|R_2$ and encrypt that signature by K & send user's certificate also & send an encrypted timestamp value to cloud manager.

h) Cloud manager will verify Digital signature of user & if it is verified then it will send the encrypted T-1. That means key K is been set for T-1 time.

4.2.3 Digital Signature Standard

Algorithm:

Signing:-

a) User chooses a random number n ($1 \le n \le q$).

b) User calculates the first signature

r = (g^nmodP)modq.

c) User will create digest of Message h(M) by already shared hashing technique with users.

d) Now user will calculate 2nd signature

S = (((h(M)+xr)n^{-1})modq)

e) Now user will send r, s , session key encrypted M & session key encrypted z(public key of user) to cloud manager.

(Cloud manager won't store value of z.)

Verifying:

a) Cloud manager checks whether r or s is less than or greater than zero or not because if any of value will be equal to zero then n must be chosen again.

b) Calculates digest using same hash algorithm as used by user because that's already been discussed.

c) Cloud manager calculates V = $\left(\left(g^{h(M)s^{-1}} z^{rs^{-1}} mod\, P\right) modq\right)$.

d) If r is congruent to V then message request is accepted.

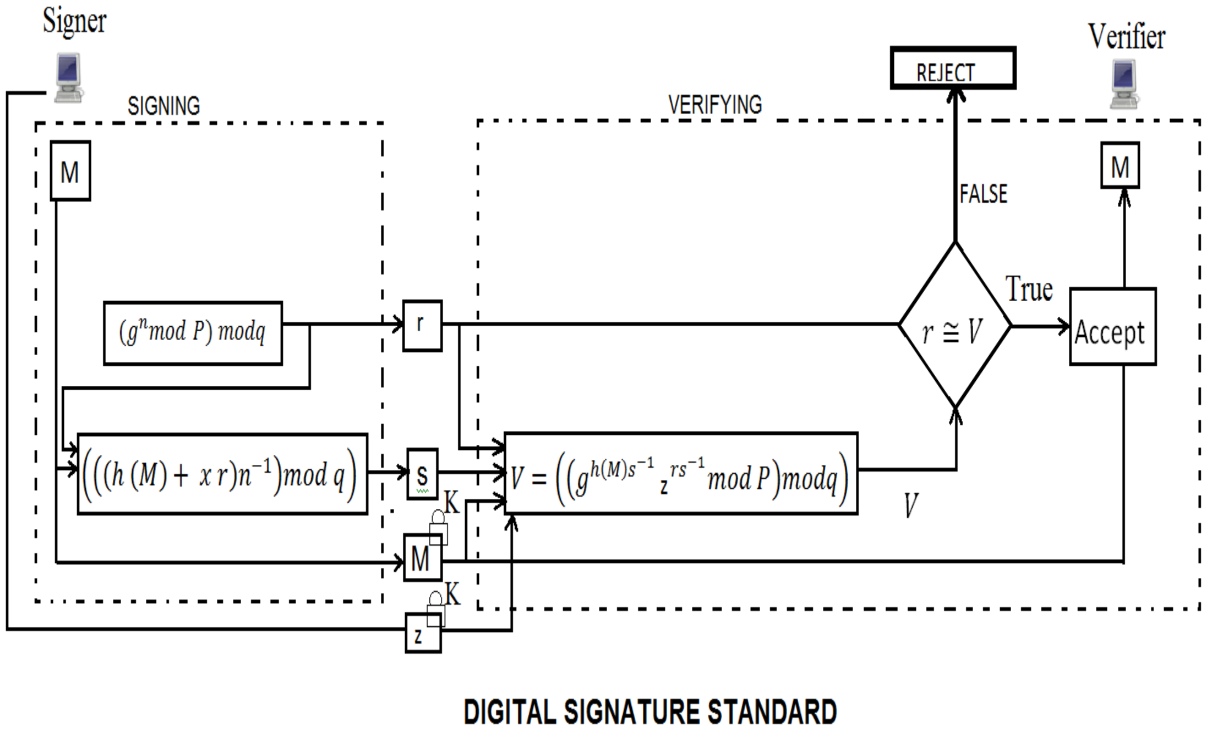
Signer
Verifier
SIGNING
VERIFYING
REJECT
M
FALSE
M
$(g^n mod\ P)\ modq$
r
True
$r \cong V$
Accept
$\left(\left((h(M) + x\,r)n^{-1}\right)mod\ q\right)$
s
K
$V = \left(\left(g^{h(M)s^{-1}} z^{rs^{-1}} mod\ P\right)modq\right)$
V
M
K
z
DIGITAL SIGNATURE STANDARD

Figure 4: Digital Signature Standard

4.2.4 Providing services from cloud to user

- After verification from cloud manager cloud manager will directly provide service to user (except case of data uploading and downloading from data storage of server because in these case cloud manager will be involved for providing service).
- In case of uploading a File on cloud-

After getting this request cloud manager will randomly choose one of Asymmetric algorithm for file and store by using its Public/Private key for encryption.

Cloud manager will maintain a file in which it will have information about user data and corresponding encryption used on them and it has been locked by public key of cloud manager.

Every time if a user/owner requests for that file, cloud manager will decrypt it then provide a copy to user and after that again encrypt that file by randomly choosing an encryption algorithm. Only owner have the privilege to overwrite a file.

- In case of downloading a File-

Cloud manager will first de-obfuscate that file first and then provide it to user according to its users.

5. CONCLUSION

There are lots of security vulnerabilities and breaches in cloud computing, to deal with these breaches and vulnerabilities we have proposed a model in which by Station to Station Key Exchange Agreement a one to one medium is created between cloud server and user so as man in middle attack is completely eliminated by this, as session key is generated for fixed time interval, each session key is generated for one time use and a file is maintained that contains information of all users and corresponding session key provided to them, so by all this replay attack is eliminated and intruders can’t use any users session key because for that a file has been maintained by cloud manager. Digital Signature Standard is used for authentication purpose. Cloud Manager will audit all users work on cloud and it will make files tamper resistant by using tamper resistant module. Cloud Manager performs lots of other functions also like encrypt files by using different encryption algorithm. So Cloud Manager improves privacy and security. Therefore we have used three different parts to enhance security of Cloud Computing.

6. ACKNOWLEDGMENTS

We would like to express our deepest gratitude to all the people who have supported and encouraged us during the course of this work without which, this work could not have been accomplished. We are deeply indebted to Dr. O. P. Verma, HOD, Computer Science, DTU for his immense support. We are grateful to Delhi Technological University for providing the right resources and environment for this work to be carried out.

7. REFERENCES

[1] Mr. Prashant Rewagad and Ms.Yogita Pawar “Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing” 2013 IEEE International Conference on Communication Systems and Network Technologies.

[2] Uma Somani, Kanika Lakhani, Manish Mundra “Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing” 2010 IEEE 1st International Conference on Parallel, Distributed and Grid Computing (PDGC - 2010).

[3] Volker Fusenig and Ayush Sharma “Security Architecture for Cloud Networking” 2012 IEEE International Conference on Computing, Networking and Communications, Cloud Computing and Networking Symposium.

[4] Siani Pearson, Yun Shen and Miranda Mowbray “A Privacy Manager for Cloud Computing” HP Labs, Long Down Avenue, Stoke Gifford, Bristol BS34 8QZ, UK.

[5] Siani Pearson “Taking Account of Privacy when Designing Cloud Computing Services” HP Labs, Bristol, UK.

[6] Mandeep Kaur and Manish Mahajan “Using Encryption Algorithms to enhance the data security in Cloud Computing” 2013 International Journal of Communication and Computer Technologies Vol 1,issue 3,January 2013.

[7] Shabnam Sharma & Usha Mittal “Comparative analysis of various authentication techniques in Cloud Computing” International Journal of Innovative Research in Science, Engineering and Technology Vol. 2, Issue 4, April 2013.

[8] Jian Wang, Yan Zhou, Shuo Ziang & Jiajin Le “Providing Privacy Preserving in Cloud Computing” 2010 IEEE.

[9] Dave Shackleford “Cloud Security and Compliance: A Primer” SANS Whitepaper-August 2010.

[10] Joshua Browser “The Security Onion Cloud” SANS Whitepaper-2013.