Cloud Computing Security Review Paper

[1]Diksha sharma, [2]Bhawna Mallick
[1]Student, [2]Head Of The Department Of CSE
Department of Computer Science and Engineering,
Galgotia's college, Greater Noida, Uttar Pradesh, India

***Abstract* - Now a day's cloud computing has covered wide range of computing and storage online. This technology is growing fastly because of its features like flexibility scalability and low price services etc. the more organisations are connected by cloud, so it becomes a large data on server to handle and what data is stored in cloud is sensitive so security is main issue There are many research that have already developed on cloud .The security methods are applied on different service layer like IaaS (infrastructure as a service), PaaS (platform as a service), SaaS (software as a service). I will summarise the some best security methods which are widely in used.**

***Keywords* - Cloud Computing, ECC Cryptography, RSA Cryptography and Kerberos Authentication.**

I. INTRODUCTION

Cloud computing as the name suggests cloud + computing. Cloud means the storage and computing means the access. Here storage of data is on the server which some organization takes on rent according to their need. The number of server can be increased or decreased as per need of the organization, who is taking the cloud on rent. And to increase the number of server is very easy just add the number of server in cloud providers software.

Cloud computing can be understood by taking an simple example the party organisers: - all the management of function is performed by them just the person who wants to arrange the party that person should pay money for this .so here organiser is third party who manage or arrange all the things like decoration, the infrastructure etc. so burden is reduced and all the work is performed in easy manner. So same with cloud computing. There are some clouds providers like: - Google and Amazon, Microsoft. In cloud computing there are basically three kinds of services performed .IaaS, PaaS and SaaS.

II. SERVICES OF CLOUD

In IaaS is infrastructure as a service, it is all about the hardware the networking management .it provides the hardware , firewalls, load balancer etc on demand from their equipment data center. Which organization takes only the infrastructure on rent they have need a programmer to develop a platform, a data manager a computer analyst etc. so it is expensive and it makes profitable only for big organisations. This does not provide a low cost solution for small organisations.

PaaS: - It offers an environment to develop the application. An organisation who buy the pass services they have infrastructure, only they need to develop a platform like: - operating system windows and Linux according to their choice.

SaaS: - It is used by the end user .It is used only to select customize purpose. It is good for the small kind of business .for example:- some application like Google play store ,the all data is stored in cloud not user's device. The end user can use it as software.

III. METHDOLOGY USED WIDELY

The main aim of security methods that are used in cloud ,data should be in encrypted or decrypted from when it pass through a network by which the attacker and hacker could not identify the sensitive information. Here I will describe the some main and good technologies that are used in security.

a) ECC(ELLEPTIC CURVE CRYPTOGRAPHY)

We used this method with Diffie Hellman Key exchange. There are four steps by which architectures identify the authenticity of user. In first step data connection is established and in second method account is created . in third step authentication and in last one is data exchanged.

In this algorithm we have to select a number'd' and 'n'. Sender use the public key to encrypt the message and private key to decrypt the message

- To generate public key q = d*p…… (1) Here d should be in range of 1 to (n-1). Where d= private key.
- P is the point on curve.

Encryption

- M = message, this should be point on the curve. select k randomly from 1 – (n-1)
- C1= k*p……..(2)
- C2 = M+ k*Q…… (3) Where c1 and c2 = cipher text.

Decryption

- M= C2 - d*c1…….(4)

Advantages

- Attacker need to crack sub exponential time complexity which is really difficult to crack.
- And ECC speed is really good as compared to linear algorithm.

DRAWBACK

- ECC method is more difficult to implement than RSA algorithm and its size of encrypted message is also larger than RSA.

b) RSA METHODOLOGY

This method is invented by Rivest, Shamir and Adelman. RSA is also based on asymmetric key cryptography which consist basically three steps.

- Generations of keys
- Encryption process.
- Decryption process

1. Generation of keys

This is very first phase to generate keys between cloud provider and user.

- Compute n= p*q. p and q should be prime no.
- Compute Ø (n) = (p-1)*(q-1). Where Ø (n) is totient function.
- Select exponent e such that 1<e< Ø(n). where (e, Ø(n) = 1).

- Now compute $d = e^{-1} \pmod{Ø(n)}$, where d is private key .
- Now the public key exponent is (e, n) and the private key is (d, n).

2. Encryption process - This process is performed to convert the readable data (plaintext) in to un readable data (cipher text).

- Public key (n, e) is provided by the cloud provided to cloud user.
- Compute the cipher text by $C = m^e \bmod n$. this cipher text is stored with cloud provider.

3. Decryption process

This scheme is used to convert the data unreadable format (cipher text) to readable format(plaintext).

- In this phase when the user requests to the data, the cloud service provider verify the user's authenticity and provide the cipher text that is C.
- Computed $m = C^d \bmod n$.

4. APPLICATION

- Widely used in digital signature.

5. Drawback-

- In RSA numbers of keys are overhead. It requires more computing power because of large key.

c) Kerberos Authentication

Because of the drawback of RSA, Kerberos authentication comes. It is based on the 'ticket'. In this we use Shamir's secret key sharing procedure in which encryption key is shared on multiple servers. In this case if any attack is performed by attacker on key and that part is losted so we can reconstruct it by using Shamir's threshold scheme. The secret key is reconstructed by combining the sufficient share holders' secret. It works like a group where all the members (m) of group (g) together made the secret key but not less than m members can do this. This scheme works on two bases.

i. Authentication server (AS) - In this client requests for a "Ticket" from AS then AS generate a session key which provide a satisfactory "TGT".

ii. Ticket Granting Ticket (TGT) - In this client send this TGT to TGS (Ticket Granting Server) and TGS provide multiple of tickets from some of them keys are used in decryption. In this way clients get a master key for using the services.

Advantage

- It is more robust than other technologies and it reduces the no. of key exchange problem.
- This is best technology from above both RSA and Elliptic Curve Cryptography.

IV. CONCLUSION

We have discussed here some main methodology that is used in cloud computing to provide security. Besides these technologies some security methods that is based on symmetric and asymmetric key have been already developed, like – Diffie Hellman key exchange but still loop holes arise. By comparing all methods Kerberos is best suitable approach which provides more confidentiality, availability, robustness of data.

V. REFRENCES

[1] N.Padmaja Department of Information Technology and PRIYANKA KODURU "Providing Data Security in Cloud Computing using public key cryptography" Issue 01, 2013 *International Journal of Engineering Sciences Research-IJESR* Vol 04.

[2] Dr. M. Gobi and Karthik Sundararaj "A Secured Cloud Security Using Elliptic Curve cryptography" issue 27th march 2015 *international journal of advanced networking and application*.

[3] Dr. Santosh Lomte and Shraddha Dudhani "Secure Key for Authentication and Secret Sharing in Cloud Computing" Volume 5, Issue 6, June 2015 *International Journal of Advanced Research in Computer Science and Software Engineering* pp. 1008-1010.