IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 12, Issue 5 (Jul. - Aug. 2013), PP 62-64
www.iosrjournals.org

Enhancing Privacy in Cloud Service Provider Using Cryptographic Algorithm

K. Sunitha[1] S.K Prashanth[2]
[1]*M.Tech (C.S.E), VCE, Hyderabad, India,*
[2]*Associate Professor in CSE, VCE, Hyderabad, India,*

Abstract: *Cloud Computing provides the way to share the distributed resources and services that belong to different organizations and sites. Even though it having benefits, but it posses security problems. All types of users who require the secure transmission or storage of data in network. While, the data transmission on the internet or over any networks are vulnerable to the hacker attacks. We are in great need of encrypting the owner data. Our paper aims to give the cloud data storage models and data security in cloud computing system. Here we propose a efficient method for providing data storage security in cloud computing using RSA algorithm. In this algorithm some important security services included such as key generation, encryption and decryption that are provided in cloud computing system.*
Key words: *Data storage security, RSA algorithm, Encryption, Decryption*

I. Introduction

Just a few years ago, people used disk to store their documents. In recent times, many people moved to memory sticks. Cloud computing refers to the ability to access and manipulate the information which was stored on remote servers, using any Internet-enabled platform. Computing facilities and applications will rapidly increased and delivered as a service over the Internet. Cloud computing provides Internet-based services and storage for users in all markets including financial, healthcare, education and government. This new approach to computing allows users to without requirement of hardware and software management, more flexibility, collaborate with others, and take advantage of the sophisticated services that cloud providers offers. Eventhough, security is a huge concern for cloud users.

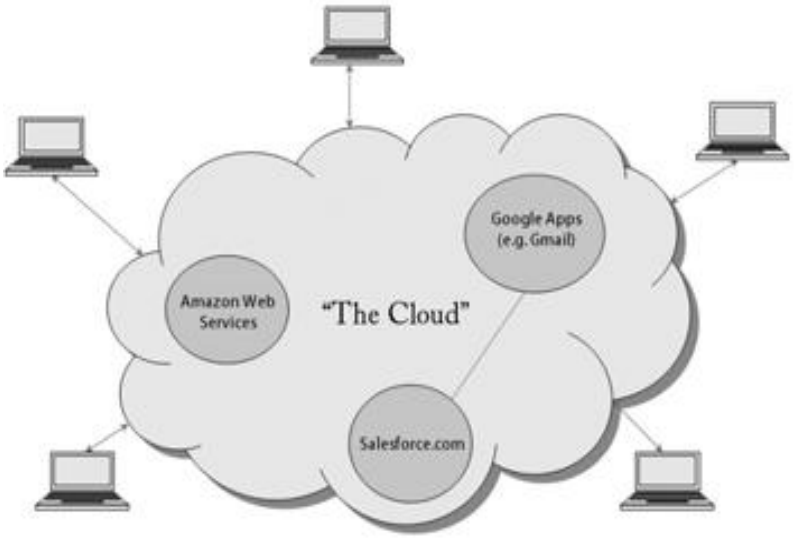

Fig 1: Structure of cloud

The concept of cloud computing provides three services i.e Information as a service (IaaS), Platform as a service (PaaS), Software as a service (SaaS) all of which means a service-oriented architecture.

There are four types of cloud models listed by NIST (2009): private cloud, public cloud, hybrid cloud and community cloud.

A. Public Cloud: The cloud computing resource is shared outer, someone can use it and a few payments maybe calculate. Public organizations assist in providing the infrastructure to carry out the public cloud.

B. Private Cloud: Private cloud resource is limited range to a collection of people, like a employees of a organization. The organization itself supports Infrastructure of private cloud, controlled and corporate data.

C. Hybrid Cloud: This is the combination of both public as well as private cloud. It can also be explained as multiple cloud systems that are related in a way that permits programs and data to be moved easily from one system to another.

D. Community Cloud: This cloud is basically the combination of one or more public, private or hybrid clouds, which is shared by many organizations for a single cause. Infrastructure is to be shared by several organizations within specific community with common security, conformity objectives. The cloud is managed by third party or managed itself. Its cost is less then public cloud but more than the private cloud.

II. Data Storage Security

Cloud storage is a service of cloud computing which allows data owner to move data from their local systems to the cloud. By moving their data in the cloud, data owners can avoid the initial investment of infrastructure setup, large equipments and maintenance cost. The data owners pay only how much they actually use. Another reason is that data owners rely on cloud to provide more reliable services, so we can access data from anywhere and at any time. Cloud storage moves the owner data to large remote data centers, on which data owner does not have any control over it. However, this unique feature of the cloud poses many security concerns like data security, privacy, data availability and integrity. Computer based security measures mostly capitalizes on user authentication.

A. Confidentiality: Confidentiality refers to only authorized persons or systems having the ability to access the protected data.

B. Integrity: Data Integrity refers to the protection of data from unauthorized deletion or modification i.e the data should not be modified**.** Further, detects if any modifications to data stored in cloud.

C. Availability: The availability means that an organization has its full set of computing resources accessible and usable at any time. Availability can be affected either temporarily or permanently, and a loss can be either partial or complete. Denial of service attacks, equipment outages, and natural disasters are all threats to availability in cloud data.

The benifit of cloud is cost savings. The major disadvantage is security, since it is not provided in cloud, many companies have their own unique security structure. For example, Amazon has its own security structure. The data placed in the cloud is accessible to everyone, even though the security is not guarantee. We proposed a method for Cloud Computing system by providing data storage and securing Cloud Computing system using RSA algorithm technique. This method include security services like key generation, encryption and decryption.

III. Security In Cloud Computing Using Rsa

Public key encryption algorithm has been developed by Rivest, Shamir and Adleman in MIT as pioneers work. By taking their initial name, this algorithm is called as RSA encryption algorithm. The RSA encryption algorithm is widely used such as for emails and files encryption system called PGP(Pretty Good Privacy). The wide usage of RSA requires a lot of time for encryption and decryption of plane text. Due to its computational complexity, since it makes use of prime factorization with respect to two prime numbers product.

The RSA algorithm is used to encrypt the data that provides security, so that only the concerned user can access it. By securing the data, we are not allowing unauthorized parties to access data.

Initially, the user encrypts the data and stores it in cloud. When required, user places a request the Cloud provider for the data, cloud provider authenticates the user, if it is valid then delivers the data to the user.

Every message in block cipher (RSA is block cipher) is mapped to an integer. RSA consists of both public key and private key. In our cloud environment pubic key is known to everyone, whereas private key is known only to the user who originally owns the data. Thus encryption is done by the Cloud service provider and decryption is done by the user. Once the data is encrypted with the public key then it can be decrypted with the corresponding private key only.

RSA algorithm has three steps:

1. Key Generation
2. Encryption
3. Decryption

1. Key Generation

The key generation should be done initially. This process is done in between the cloud service provider and the user.

Steps:

1. Select two distinct prime numbers x and y.
2. Compute n = x * y.
3. Compute Euler's cotient function,

a. Ø(n) = (x-1) * (y-1).

4. Chose an integer e, such that 1 < e < Ø(n) and GCD of e , Ø(n) is 1. Now e is come out as public key exponent.
5. Now determine d as follows: d = e-1(mod Ø(n)) i.e., d is multiplicate inverse of e mod Ø(n).
6. Now d is kept as private-Key component, so that d * e = 1 mod Ø(n).
7. The public key is (e, n), where e is public key exponent and n is modulus n.
8. The private key is (d, n), where d is private key exponent and n is modulus n and which must be kept secret.

2. Encryption

Encryption is the process of converting original plain text into cipher text.

Steps:

1. Cloud service provider should give the public key (e, n) to the user who wants to store the data with him or her.
2. Now user data is mapped to an integer by using an agreed upon reversible protocol it is known as padding scheme.
3. Now the data is encrypted and the resultant cipher text (data) C is C = me (mod n).
4. Now the encrypted data is store in the cloud service provider.

3. Decryption

Decryption is the process of converting the cipher text into the original plain text.

Steps:

1. The cloud user now requests the cloud service provider for the data.
2. Now the cloud service provider verifies the authenticity of the user and gives the encrypted data i.e, Cipher text C.
3. Then Cloud user decrypts the data by computing, m = Cd (mod n).
4. After computing m, the user can obtain the original data by reversing the padding scheme.

IV. Conclusion

Cloud Computing is a new and evolving paradigm where computing is regarded as on-demand service. Cloud storage is a service of cloud computing which allows data owner to move data from their local systems to the cloud. By moving their data in the cloud then the organization loses control over the data. Then the amount of protection is needed, for this pupose we suggest the efficient algorithm for cloud security using RSA algorithm. In this method some important security services offered as key generation, encryption and decryption are provided in Cloud Computing system. The main goal is to securely store and manage the data. The RSA gives security for the data, which was stored in Cloud. Only authorized user can retrieve the encrypted data and decrypt it.

References

[1] Cong Wang, Qian Wang, Kui Ren, Wenjing Lou, *"Privacy Preserving Public Auditing for Data Storage Security in cloud Computing",* 2010.

[2] Jianfeng Yang and Zhibin Chen , "Cloud Computing Research and Security Issues", IEEE 2010.

[3] Parsi Kalpana, Sudha Singaraju,*"Data Security in Cloud Computing using RSA".*

[4] P.Kalpana, *"Cloud Computing – Wave of the Future", International Journal of Electronics Communication and Computer Engineering, Vol 3, Issue 3,* ISSN 2249–071X, June 2012.

[5] Subedari Mithila, P. Pradeep Kumar, *"Data Security through Confidentiality in Cloud Computing Environment".*

[6] Uma Somani, Kanika Lakhani and Manish Mundra, *"Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing",* 2010.

[7] Kresimir Popovic and Zeljko Hocenski, *"Cloud computing security issues and challenges",* MIPRO 2010, May 24-28, 2010, Opatija, Croatia.

[8] Qian Wang, Cong Wang, Kui Ren, Wenjing Lou, Jin Li, *"Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing*", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, *Vol. No. 22, Issue 5,* MAY 2011.

[9] Cong Wang and Kui Ren, Wenjing Lou, Jin Li,, *"Toward Publicly Auditable Secure Cloud Data Storage Services*", IEEE Network July/August 2010.

[10] Subashini S, Kavitha V., *"A survey on security issues in service delivery models of cloud computing,"* Journal of Network and Computer Applications (2011), *vol. 34 Issue 1,* January 2011 pp. 1-11.