International Journal of Advanced Technology in Engineering and Science
Vol. No.4, Issue No. 10, October 2016
www.ijates.com
ijates
ISSN 2348 - 7550

SECURITY AND DATA TRANSMISSION TECHNIQUES IN CLOUD ENVIRONMENT

Bhavya Deep[1], Parveen Kumar[2], Palak Bansal[3]

[1, 2]Department of Computer Science, [3]Department of Electronics

Bhaskaracharya College of Applied sciences, University of Delhi, (India)

ABSTRACT

Cloud computing is an emerging technology in the field of information technology. It has plethora of advantages over conventional ways of computing ranging from low economic expenditure, and flexibility of scaling up and down the cloud capacity to reduced hardware infrastructure. Data on the cloud can be accessed from anywhere at any point of time.Despite being a powerful tool, cloud computing security has been a constant source of concern. Its elastic characteristics and the diversity in the services provided by the cloud makes it more vulnerable and prone to malicious activities.Secure upload of data on cloud, secure downloading of data from cloud, proper usage and sharing of data is maintained by using encryption and decryption techniques. Use of keys is employed for encryption and decryption of data.

Keywords*: *Cloud Computing, Security, Private Key, Public Key, Encryption, Decryption

I. INTRODUCTION

Cloud is a wide network over which large amount of data can be stored, shared and accessed. The backbone of a cloud is 'internet'. Cloud model has many benefits and is cost effective. It reduces the infrastructure cost. The resources can be scaled up or down according to the need of the user. The resources could be storage, computing and any other service.It has the advantage of on demand scalability of resources. The cloud provides services to the user and the data and applications can be accessed by the user from anywhere.Security is one of the major challenges in the implementation of a cloud. Failure to ensure a secured cloud model discourages many organizations from adopting the cloud model. The main concern is about data security and privacy protection. Risk factor is due to the multi-tenancy, lack of access control and elasticity. Confidentiality and privacy are the key parameters that a cloud structure must fulfill in order to gain more popularity.

There are three types of cloud models -Public, Private and Hybrid.

a) PRIVATE CLOUD The private cloud is deployed within a company or institution and faces no issues of data security as the whole control of the cloud is in the hands of the administration within a company or institution. The company that has full access over the private cloud can control the applications run on the infrastructure, the place where they can be run and the people or organization accessing it- over every aspect of infrastructure. When sensitive data is involved, private cloud is used. Deployment of private cloud is better for an organization as it gives a better insight and authority over security. An organization can ensure privacy by limiting the number of tenants that can utilize the resources of public cloud. Considering

private cloud to be an internal network, therefore, being secure is not right. Viruses are still there. Perimeter security needs to be deployed to have proper control over the stacks.

b) PUBLIC CLOUD Public cloud services are available to the consumers on the public internet and are free to access to all the people worldwide. The services like applications or storage may be free or available as pay per use. A third party (e.g.- Google, Amazon) is responsible for deployment of services over the public cloud. They expose their service to the users via internet.

c) HYBRID CLOUD a hybrid cloud is an integrated model that provides service of both public and private cloud. This allows an enterprise to store and process sensitive data on private cloud whereas less sensitive data on public cloud. This type of models enjoys the advantage of both private and public clouds[1].

There are three basic service models of the cloud-

a) SAAS (Software as a service) consumers use the applications hosted by the cloud provider on cloud. Examples are Google drive, siri, dropbox.

b) PAAS (Platform as a service)cloud provider provides platform for the consumer to host their applications on cloud and manage them. Examples of PAAS providers are Google App Engine, and Red Hat's OpenShift.

c) IAAS-(Infrastructure as a service) it provides infrastructure for network, computation and network resources. Amazon elastic compute cloud(EC2) is an example of IAAS [2].

II. DATA TRANSFER

Data transfer over cloud has two major steps-

2.1 Uploading data

2.1.1. User is required to authenticate him to the cloud by entering his unique username and password.

2.1.2. After that user is permitted to upload his data for sharing, uploaded data is encrypted.

2.1.3. A key is generated based on system timing.

2.1.4. Data is encrypted by using the key of the user and data is stored in the encrypted form.

2.2 Downloading Data

2.1.5. When another user wants to access the shared secured data, he is required to enter the appropriate key in order to access the data. Cloud decrypts the data on entering the key.

2.1.6. Decrypted data can be downloaded from cloud [3].

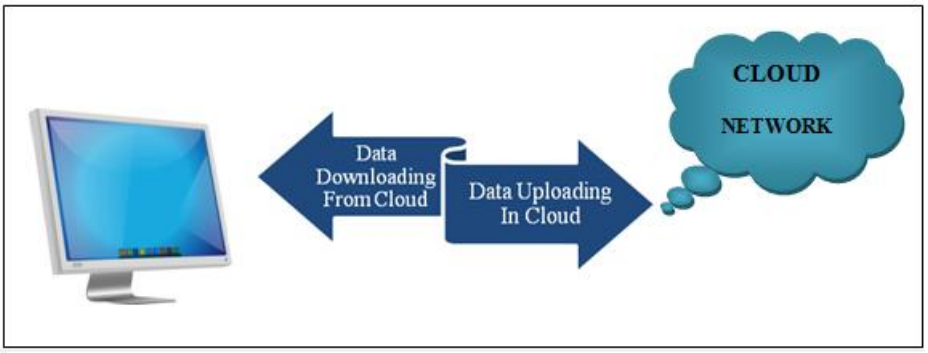

Fig.1 uploading and downloading of data

III. SECURITY PROBLEMS

Data on the cloud can face the problem of theft and unlawful access. Data before sharing on the cloud can be encrypted. However, if there is a large amount of data that needs to be shared or stored on the cloud then it would require more time for data to encrypt. To overcome security issues in the cloud some strategies needs to be implemented. The generations of various public and private keys, their proper sharing with trusted clients and encryption and decryption of data by using these keys are explained in this paper. As the user tries to upload and share the data on the cloud it is encrypted and then decrypted at the receiver end require the user to enter their respective private and each other's public keys.This paper focuses with the various cryptographic techniques in order to make the data sharing a secured method. It focuses on the following key points-

- Secure sending of data over a cloud so that even administrator cannot decode the data.
- Secure receiving of the data over the cloud network.
- Proper usage and sharing of private and public keys for encryption and decryption of data.

3.1 Solution Using Private and Public Keys

There are different ways stated below in order to describe the proper usage and combining of public and private keys to enhance the security of important and confidential data over the cloud.

If a data or message on a network is to be shared among one or more clients on a network by using a single shared public key. The single shared key is common to all the clients and all the clients have the access to that key. In this, the message that is to be shared is first encoded by using the shared key and then is send over the network, after which it is decrypted by using the same shared key by the clients.

In this way, the message can be shared only among the trusted people only.

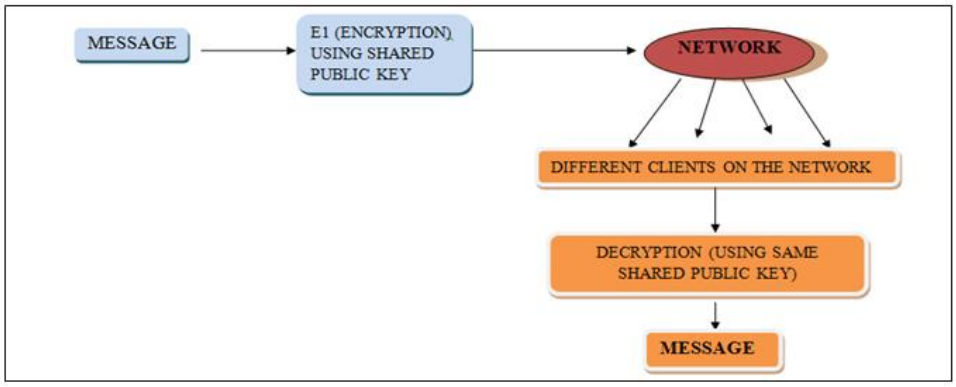

Fig2. Data sharing among many clients

2.2. If data is to be shared only between the two trusted people on an insecure network by using a private and a public key. In this public key is also used along with the private key.

For instance, consider two people 'A' and 'B' on a network between which message or data is needed to be shared. Each has his own private and public key.A's and B's public key are shared between each other and their private keys are personal to them and the data has to be transmitted from A to B.

2.2.1. A and B chooses a random rational point integer say S that acts as a public key and is common to both the clients.

2.2.2. A and B also selects random integers P_A and P_B respectively which acts as their private keys.

2.2.3. A computes P_A*S and B computes P_B*S and these two values are exchanged by them over a network.

2.2.4. Now, on receiving this information from each other and by using their private keys both A and B compute P_A* (P_B*S) = P_B*(P_A*S) = (P_A* P_B)*S.

2.2.5. The value so obtained is the shared secret key that only A and B know. Thus, their private keys and the shared secret key are difficult to decode by anyone. In this way, A and B does not compromise with the security of their keys, now they can use them for securely communicating over a network.

In this the message is to be transmitted between 'A' and 'B' by using their private and public keys. A's private key and B's public key is used to make a single key say X and A's public and B's private key is used to make a single key say Y [4]

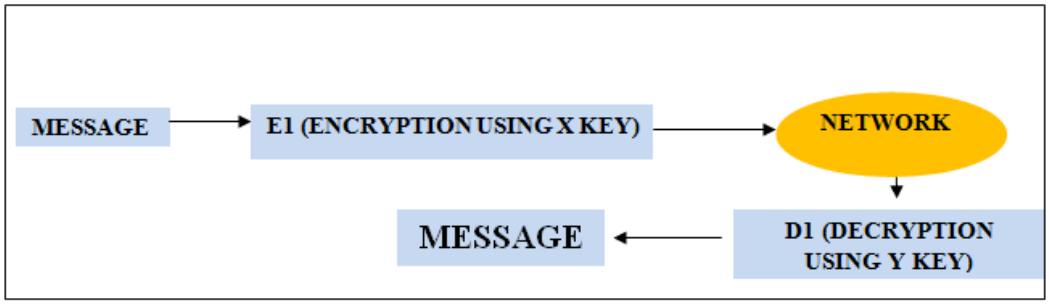

Fig3. Data sharing between 2 clients by combining the keys

III. CONCLUSION

Cloud's pay per use model, dynamic resource provisioning and reduced infrastructure cost makes it an emerging technology in today's world. To provide the user a holistic secured environment, it is important to strictly enforce the security parameters on the cloud. The continuous monitoring of various new policies in this field is essential. The proposed methods in this paper will surely ensure a favorable cloud environment for both the user and the cloud provider. There are many encrypting and decrypting techniques to secure the data. Private and public keys are only known to the user and even the provider has no hint about these. Therefore, it's main advantage is that the data is very secure on the cloud.

IV. ACKNOWLEDGEMENT

We acknowledge University of Delhi for providing funds under DU innovation project scheme to carry out this paper.

REFERENCES

[1] https//en.m.wikipedia.org

[2] A. Behl, K. Behl, An analysis of cloud computing security issues. 2012 IEEE

[3] V.S Mhalle, A.K Shahade, Enhancing the data security in cloud by implementing hybrid encryption algorithm. 2014 IEEE

[4] A. Kumar, B.G. Lee, H.J. Lee, A. Kumari, Secure Storage and Access of Data in Cloud Computing