IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 11, November 2016

Safe and Secure Transfer Framework for Data on Cloud

Vivek Manukonda[1], B Vamsi Krishna[2]

CSE Department, MVGR College of Engineering, Vizianagaram, India [1]

Asst. Professor, CSE Department, MVGR College of Engineering, Vizianagaram, India [2]

Abstract: Cloud computing offers a new way of resources and services like storage, computing and application get access on the demand of customer. Where rapidly increase of using cloud computing in society drew the attention of security and privacy of data. Therefore the sharing of resources and data over the unauthorized public network will be more unsecure to transfer from user to cloud and vice versa on the unauthorized public network because of malicious attacks like man in middle, reply attacks etc. Other one we cannot trust every Cloud service provider (CSP) and keep our data in there cloud. So in this paper we proposed a method that Kerberos and identity based encryption used for secure data transfer over the untrusted public network and provide confidentiality to data which is uploaded in cloud. This maintain a superior security with the combined approach of Kerberos and IBE in cloud computing because no such a method exists and this method provides features of authentication, confidentiality, integrity, privacy and security to Cloud Service Providers and cloud users. [1]

Keywords: Cloud computing, security, Kerberos authentication, private key generator, identity based encryption.

I. INTRODUCTION

Cloud is large-scale computing, where it made the computing to high range. [2]The cloud giving the customers the best services on on-demand, the customer can get access the cloud services remotely anywhere with connection of internet. It maintaining security at the every level of service. [3]The cloud computing provide services in cost effective with the features of scalability, robust, simplified, storage, platform, network, security and services are deliver by on demand Cloud computing provide different services on base of type of resources. [4]The cloud computing provides three different services are 1. SaaS 2. PaaS and 3. IaaS

- Software as a service (SaaS):

It provides software applications remotely on demand over the network to user for low cost. It reduces the burden on customer by providing these services for leased period instead of buying full software application which is used for limited period. Example google apps, google docs, Salesforce, basecamp, quick base, Workday, Concur, Citrix GoToMeeting, Cisco WebEx and etc.

- Platform as a service (PaaS):

It provides a virtual platform for customer allowing him to run, develop, manage and network applications by maintaining and build the infrastructure for good quality experience by lunching an application on demand over the network. Example Microsoft's Azure, Google's Application Engine (app engine), Yahoo Pig.

- Infrastructure as a service (IaaS):

It offers an online services for user from the details of infrastructure like physical computing resources, data partitioning, location, scaling, security, backup etc. It often offers additional resources such as a disk-image library, block storage, file objective storage, firewalls and load balancing, network equipment's etc. Example Amazon Web Services (AWS), Cisco Metapod, Microsoft Azure, Google Compute Engine (GCE), Joyent, Amazon S3, Amazon EC2.

II. RELATED WORK

Symmetric key management [5] in this dedicated key management architecture uses the same data encryption technology to manage key and scramble data, these system called asymmetric key systems, because the same key is used for encrypting and decrypting information, the key manager generates new key for every message on the sender's request. [6]The key is stored in a data base along with the list of recipients. The recipient authenticates, retrieve the key from database and verify the recipient name is matched against the list of authorized recipient. After all verification completed the decryption key sent to recipient. This algorithm has drawbacks: -

Connection to the key server is required for every unique encryption, since a unique key is required for each operation and it must be shared with the server. This also means that offline operation is not possible and connections is quite high.

Encryption, decryption requires that a connection to the key server be made for each of every transaction. This makes impossible offline operation and has the potential to negatively impact scalability.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 11, November 2016

Symmetric key systems can recover keys as long as the key database can be recovered. If the symmetric key database is damaged or lost, ability to recover keys similarly impaired.
Public key infrastructure [7]the use of different key to one for encrypting data and other one use to decrypting data this technology is known as public key or asymmetric key system. For example the famous algorithm are RSA and Diffie-Hellman algorithm public key algorithm to manage encryption keys is that a recipient generates a pair of keys one public key and one private key. The sender encrypt the data with recipient public key, sends to the recipient and recipient get the data, decrypt with his private key. Certificate authority act as a third party which provides service of authenticate the identity of the recipient by issuing a digital certificate by verifying the identity and signs the certificate using its private key. The drawbacks are: -

The inherent problem of locating a public key for a specific user. Users of certificate-based systems often find they cannot locate a certificate for a specific user, making them unable to encrypt the data.
Large deployments has shown that the user interface issues with respect to managing, revoking certificates and keys make wide-scale use of PKI very expensive. The existing defects of the current protocol & shortage of current improvement we have to focus on new methods. To propose the Diffie Hellman algorithm, we have to put the password. And we also use the method of EIQ algorithm. We have to use random number to associate the public key which increase the ability of preventing replay attack. The result shows the improved Kerberos protocol can give information & password.
[8]So many ideas have been proposed to prevent Replay attack. In this paper we have to show the improved method by using triple password scheme. At the same time ticket Granting server sends one password to application server as it helps to prevent replay attack.
The importance of cloud is due to its unlimited supply of services. Users enjoy this advantages and take care of security issues in which the consumer provider extend their hands. The appropriate service and cost involved for the security provision.
In this paper we surveyed technical elements of video surveillance systems & proposed several measurements to manage a number of keys for encryption. The proposed solutions. Selectively implement a Kerberos approach for secure video surveillance systems.
This paper represents the security issues of storing sensitive data in a cloud storage service. It issues a cryptographic scheme for cloud storage. Our solution has several advantages. So that unauthorized users cannot access data without client's authorization.

III. KERBEROS KDC

[9]Kerberos is a protocol which is used to provide authentication for network security. It provides strong authentication services for client and server application for exchanging confidential messages by using secret key cryptography, while preventing from eavesdropping, reply attacks or man in the middle attacks. Kerberos performs secure verification on the bases of user and services on the concept of a trusted third party known as Kerberos key distribution center (KDC).Objectives of Kerberos server are: the Kerberos authentication system consists three servers they are

1. Authentication server: It provides authentication to the client and server.
2. Ticket granting server: It grant a ticket to the client on the request for service.
3. Real server: Kerberos network identified by name, mostly this is the domain name.

Working of Kerberos

- The user sends request for service to authentication server (AS).
- The AS sends a following messages to user
- Message A: TGS session key encrypted with user secret key.
- Message B: Ticket-Granting-Ticket TGT encrypted using secret key of the TGS.(note which cannot decrypt by user) TGT (user id, user network address, ticket validity and ticket session key)
- Once user receives the message A and b it attempts to decrypt message A with the valid secret key generated from the password entered by user and obtains the TGS session key which is used further communication.
- The user request services to the TGS,
- Message C: composed of the TGT from message B and the id of requested service.
- Message D: Authentication (which is composed of user id and time stamp) encrypting using the TGS session key.
- Upon receiving the message of C and D, the TGS retrieve message B out of message C and decrypt message B using TGS secret key and get the TGS session key. Then it TGS decrypt the message D and sends message to user.
- Message E: User to server ticket (which composed of user id, user network address, and validity period and server session key) encrypted using services secret key.
- Message F: server session key encrypted with the TGS session key.
- The CSP servers receives the message E and F from TGS and decrypt the message using its own key to retrieve the server session key and the server provides the requested services to the client.

IV. IDENTITY BASED ENCYPTION (IBE)

[10]IBE is a very strong encryption protection for communication and resource sharing over the electronic media. It is a public key cryptography and also known as ID Based Cryptography. Such as it is a type of public key

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 11, November 2016

encryption where randomly pick a piece of unique information (by applying some mathematical code) from identity of user (e.g. email id, phone number, contact names and address etc.) to create a public key for encrypting and decrypting a message, one key is public and other one is known private key (known to the recipient) which is obtain from private key generator (PKG) this feature enabling data to be protected without the need of certificates.[11]In 1984, ADI SHAMIR introduced the concept of identity based cryptography where it removes the need for public key queries or certificates because the server generates the private key, key recovery no longer require a separate private key database. In this sender does not need to contact the key sever to get an encryption key instead, the encryption key is mathematically derived from receivers identity. The receiver must contact the key server once to authenticate and get required decryption key. [11]The server is able to construct the receiver decryption key mathematically eliminating the need for database at the key server and making key recovery extremely straight forward. [12]

- A recipient's public key is derived from his identity so no certificates needed.
- Pre-enrollment not required.
- Keys expire, don't need to be revoked. In a public-key system, keys must be revoked if compromised.
- Less vulnerable.
- Enables postdating of messages for future decryption.
- Enables automatic expiration, rendering messages unreadable after a certain date.

Working of IBE
Step 1: it takes security entity by randomly selecting piece from identity (~) and output the public key PK and the master key MK. The MK is kept secret at PKG.
Step 2: private key generation (MK, $USER_{ID}$) = the private key generation which takes input as MK and user's identity and returns a private key secret key by the user ID is $SK_{ID.}$
Step 3: encryption (M, PK_{ID}) = the encryption run by sender which takes as input as receiver ID and a message M to be encrypted with PK_{ID} gives out as cipher text CT.
Step 4: decryption (CT, SK_{ID}) = the decryption run by receiver takes as input cipher text CT and get secure private key SK_{ID} from PKG and returns the message M. In case the key is not correct it shows error.

$$(M, PK_{id}) = \text{encrypt}$$

$$\text{Encrypt } (M, PK_{id}) = CT$$

$$\text{Decrypt } (CT, SK_{id}) = M$$

V. RESULTS

The combined approach gives solution for cloud computing security, where Kerberos does not support non repudiation, this weakness is reduced by applying PKG private key generator.

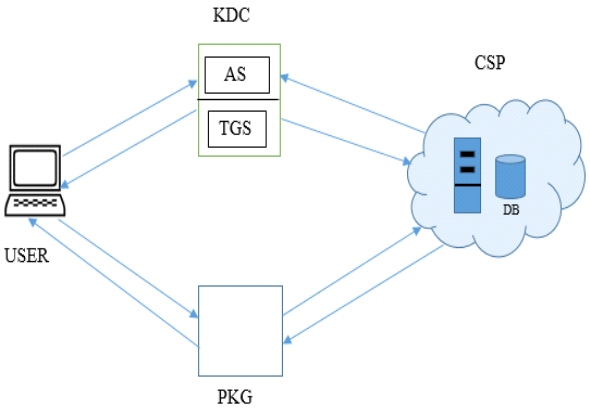

Figure 1 PROPSED METHOD

Step 1: Get data or information which is going to be on cloud infrastructure.
Step 2: For encryption the user takes receiver public key (piece of identity of receiver) will be generated by PKG.
Step 3: System will use KDC for third party authentication.
Step 4: decryption the user request the secure private key from PKG.
Step 5: where PKG use IBE identity based encryption creates a secure master private taking the part of identity from the receiver id.
Step 6: Cloud computing infrastructure will communicate with both KDC and PKG for secure transaction of data and information over the network.

VI. EXPERIMENTAL RESULTS

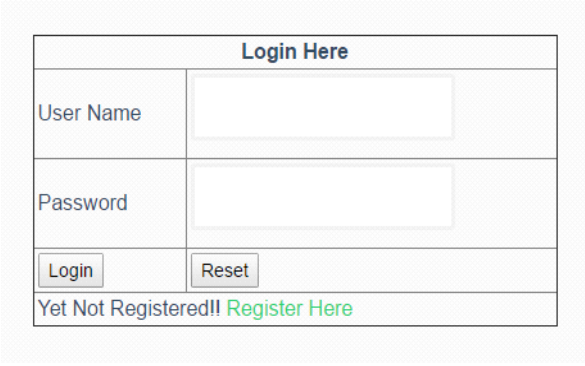

Figure 2 register and login page

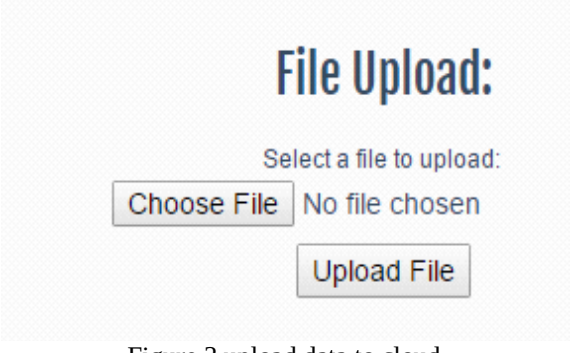

Figure 3 upload data to cloud

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 11, November 2016

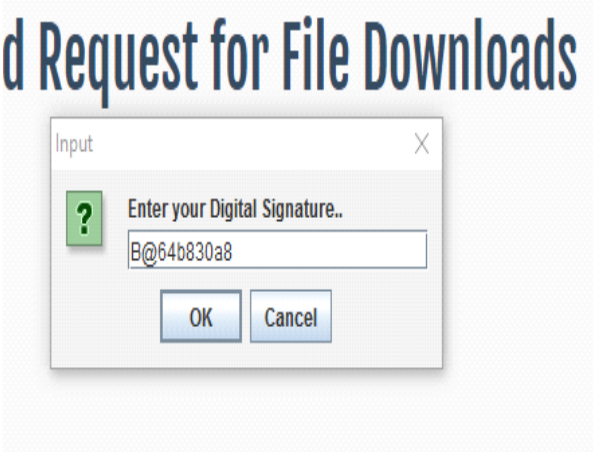

Figure 4 using private key to download the data

1 .User register and login into the cloud application.
2. User select his data and upload his data.
3. After uploading the data, it will be encrypted and stored in cloud. The encrypted data cannot be viewed for anyone including cloud service provider.
4. If the user need to view his data he should contact with PKG to generate a secret key (private key) to decrypt the data.

VII. CONCLUSION

To achieve good security in cloud computing there are several techniques and ideas are proposed and implemented. Where rapidly increase of using cloud computing in society drew the attention of security and privacy of data. Therefore the sharing of resources and data over the unauthorized public network will be unsecure to transfer from user to cloud and vice versa, because of malicious attacks like man in middle and reply attacks etc. Other one we cannot trust every Cloud service provider (CSP). In this paper we propose a framework which uses the identity based encryption and Kerberos to provide high security in transfer of data over the network to cloud. Kerberos provide the authentication and secrecy. Kerberos performs secure verification of users and services based on the concept of a trusted third party (KDC). The weakness of Kerberos that does not provide non-repudiation which will fulfil by identity based encryption which is used as private key generator. It provides the ability of privacy can take into their user hands.

REFERENCES

[1] Dereje Yimam and B. Fernandez Eduardo, "A survey of compliance issues in cloud computing," springer, 2016.
[2] Keiko Hashizume, David G Rosado, Eduardo Fernández-Medina and Eduardo B Fernandez, "An analysis of security issues for cloud computing," springer, 2013.
[3] Randeep Kaur and Jagroop Kaur, "CLOUD COMPUTING SECURITY ISSUES AND ITS SOLUTION: A REVIEW," INTERNATIONAL JOURNAL OF COMPUTERS & TECHNOLOGY, vol. 14, 2014.
[4] Jin Li, Yan Kit Li, Xiaofeng Chen, Patrick P. C. Lee and Wenjing Lou, "A Hybrid Cloud Approach for Secure Authorized Deduplication," IEEE, 2014.
[5] Pradeep K Va and V.Vijayakumar, "Survey on the Key Management for securing the Cloud," ELSEVIER, 2015.
[6] Kyungroul Lee, Hyeungjun Yeuk, Jaein Kim, Hyungjoon Park and Kangbin Yim, "An efficient key management solution for privacy masking, restoring and user authentication for video surveillance servers," ELSEVIER, 2015.
[7] Sean Lancaster, David C. Yen and Shi-Ming Huang, "Public key infrastructure: a micro and macro analysis," ELSEVIER, 2003.
[8] Gagan Dua, Nitin Gautam, Dharmendar Sharma and Ankit Arora, "REPLAY ATTACK PREVENTION IN KERBEROS AUTHENTICATION PROTOCOL USING TRIPLE PASSWORD," INTERNATIONAL JOURNAL OF COMPUTER NETWORKS & COMMUNICATION(IJCNC) , vol. 5, 2013.
[9] Yun-yun Du, Hong-yun Ning, Ping Yang and Yan-xia Cui, "Improvement of Kerberos Protocol Based on Dynamic Password and "One-time Public Key," IEEE, 2014.
[10] Carl Youngblood, "An Introduction to Identity-based Cryptography," 2014.
[11] Nesrine Kaaniche, Aymen Boudguiga and Maryline Laurent, "ID-Based Cryptography for Secure Cloud Data Storage," 2013.
[12] Jin Li, Jingwei Li, Xiaofeng Chen, Chunfu Jia and Wenjing Lou, "Identity-based Encryption with Outsourced Revocation in Cloud Computing," IEEE, 2013.