IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 4, Issue 1, Feb - March, 2016
ISSN: 2320 – 8791 (Impact Factor: 2.317)
www.ijreat.org

Security Enhancement of Cloud Data using Policy File Encryption and Multiple Key Management Service Providers

R.Sangeetha[1], A.Vasantha[2], B.Ravikumar[3]

[1,2]CSE Department, GKM College of Engineering and Technology,

Perungalathur, Chennai-600 063.

[3]Assistant Professor of CSE Department, GKM College of Engineering and Technology,

Perungalathur, Chennai-600 063.

Abstract-Cloud computing paradigm has achieved the widespread popularity due to its tremendous potential in managing the resources located at third-party service providers. To safeguard the outsourced data, cryptographic encryption can be used, yet maintaining and protecting the encryption keys will create a major security issue. In this paper we propose a data security scheme that uses multiple key manager servers for the management of cryptographic keys and performs policy file encryption and decryption to avoid man-in-the-middle attack. The confidentiality and consistency of data services are achieved through symmetric keys that are secured by using asymmetric keys. This paper concludes that the proposed data security scheme can be effectively used for secure data storage, access and deletion.

Keywords: *Cloud Computing, Key managers, Policy file, Man-In-The-Middle Attack.*

1. Introduction

Cloud computing is an emerged computing model that shares computing resources to multiple customers instead of having personal systems or local servers to handle various applications. The process of transferring all or part of a user's data, software and services from on-site data storage to the cloud, where the information can be provided on an on-demand basis over the network. Cloud enables the companies to use data resources as utilities and provides many attractive benefits for the users. Some of the privileges of cloud computing are

- **Self-Service Provisioning**: The end users can obtain the resources for any type of workload on-demand.
- **Elasticity**: The users can scale up or scale down the usage of resources based on their needs.
- **Pay-Per-Use**: The users are allowed to pay only for the resource they use.

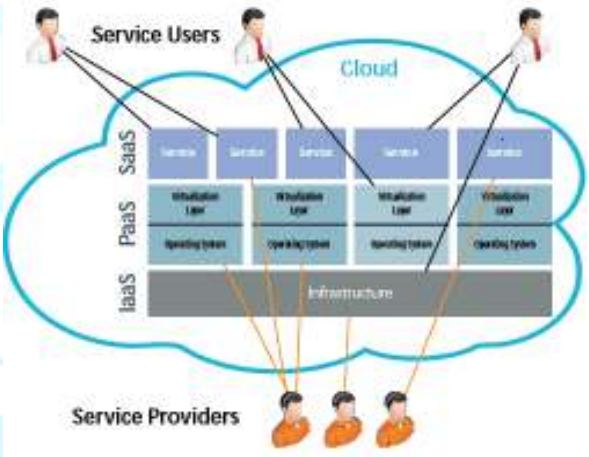

Fig 1: Cloud Computing

Cloud storage is an important service provided by cloud, in which the information's are maintained, managed and stored remotely and made available to users over a network. It can provide a greater benefits of accessibility and reliability; rapid implementation; strong protection for data storage and data recovery purposes; and lower overall data storage costs, since the user need not want to purchase, manage and maintain expensive software and hardware.

2. Data Security Problems

Cloud computing offers enormous benefits to both end users and all kinds of businesses. Despite benefits like flexibility, reliability and cost-effectiveness, there are many limitations arising which makes security the largest hurdle to leap. Some of the main security issues are data leakage, key management, and so on.

2.1 Data Leakage

Many organizations, companies and businesses that greatly benefits from using cloud storage are refraining because of data leakage problem. Sharing storage hardware and placing sensitive data in the hands of a vendor seems to be very risky. Data leakage may happen accidentally or even due to a malicious hacker attack and it would be a major security violation. The best way to overcome the problem of data leakage is that the user has to send only encrypted files to the cloud. User should not depend on the cloud provider or an intermediary to encrypt those files then they'll be able to decrypt them as well. With the cloud, all data and metadata should be encrypted at the edge, before it leaves the user premises.

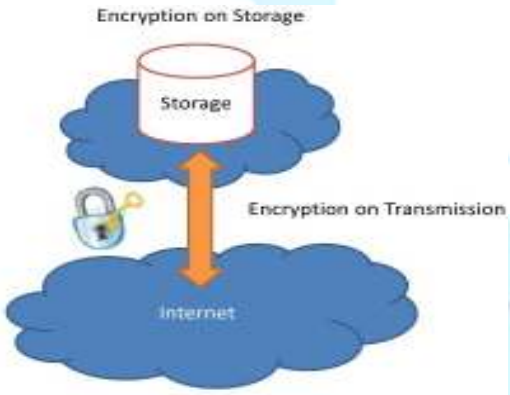

Fig 2: Storage of Encrypted Files

Even encrypted data can be vulnerable if other customers could obtain the user credentials and access their data. They may not be able to decrypt it, assuming that it is encrypted, but they may delete the files. By securing the user's own unique credentials, their files will be reliable. No one else will be able to log into the user account and delete their data.

2.2 Man-In-The-Middle Attack

It is an attack where the attacker secretly modifies the communication between the client and server who assumes that they are directly communicating with each other. This attack exploits the processing of real time transactions, communications or transfer of data. The attacker intercepts, send and receive data which are meant for others and not for them.

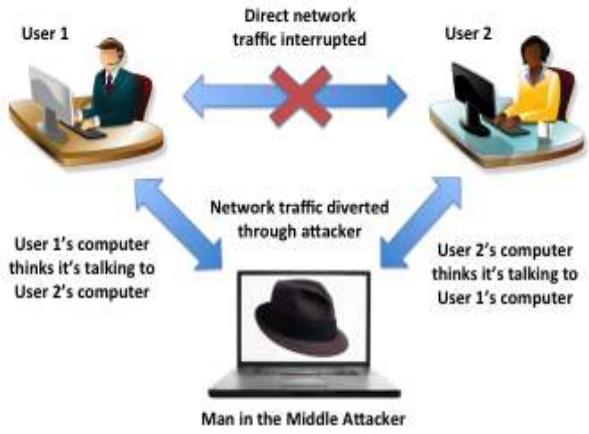

Fig 3: Man-In-The-Middle Attack

2.3 Key Management

While encryption enables access control to the user data, insecure key management and storage can lead to it being compromised. The challenge of keeping encryption keys secure becomes much harder, when we add the additional risk of having a third-party managing the physical and logical access to infrastructure. Access to encryption keys gives the provider access to private data.

3. Existing System Concepts

In the existing system File Assured Deletion scheme was used. FADE is a trivial and flexible technique that assures the deletion of files from cloud when the user sends the request. However, during our analysis, FADE has some issues on security of keys and authentication of participating parties. In this existing process there is a Man-In-The-Middle Attack (intruder) between Client and Key Manager. The intruder can intercept

user policy and send modified policy to KM. As the policies are modified the client didn't receive appropriate key from KM, this compromise may lead to the loss of data.

3.1 Drawbacks

- Key Management becomes a prime issue in the case of encryption. Cryptographic keys need to be stored and protected. Compromise or failure of a key storage mechanism may lead to the loss of data.
- Man-In-The-Middle Attack.

4. Proposed System Concepts

We propose a data security scheme that uses multiple key management service providers for managing the cryptographic keys. Shamir's (k, n) threshold scheme is used for the management of key by which the user breaks up secret key into n shares and encrypts each key share with the public key of the respective key manager and it uses k shares out of n to rebuild the key. To avoid man-in-the-middle attack and data leakage problem, user access is ensured through a policy file encryption and decryption where the policy file that states policies under which access is granted to the keys. This scheme makes use of both symmetric and asymmetric keys. The reliability and confidentiality of data services are achieved using symmetric keys which are secured by asymmetric keys. Asymmetric key pairs are generated by third party KM's. Out of the keys used, only public key is given to the client. For secure transmission of keys, a secret key is established between client and KM through STS protocol.

5. Module Implementation

- Cataloguing of Users & Policy Setting.
- File Upload & Policy File Creation
- File Download
- Policy Revocation & Renewal

5.1 Cataloguing of Users & Policy Setting

In this module user has to register to become a member OF cloud. Once they registered user has to choose some attributes (e.g. name, email, address etc..,) and also give some user defined attributes to encrypt their policy file which is created during the file uploading process. This Attribute Based Encryption is performed using Elgamal algorithm.

5.2 File Upload and Policy File Creation

After completing the registration process, authentication process will be performed between the user and the key manager using Diffie-Hellman key exchange Algorithm. After that user will encrypt their file using secret key which is provided by cloud, based on user attributes and then the encrypted file will be uploaded into cloud and also policy file is generated simultaneously and it contains username, filename and access permission, by default user access permission will be allowed. Now user breaks up the secret key into n shares (S1, S2…Sn) by using Shamir's key sharing technique and user encrypts their i-th key share with public key of i-th key manager.

5.3 File Download

If the user has to download a file from cloud, they have to send request to Key-Manager with appropriate attributes (default and user defined attributes). Key-Manager will verify their attributes and if it matches with the original attributes, it then decrypt the users appropriate Policy File and check the users file access permission to authenticate appropriate user. After authentication, the Key-Manager decrypts the user secret key by using their own private key and they provide decrypted i-th share to the requested user. The secret key will be reformed by Shamir's secret key sharing scheme only if the attributes and credentials are proven. Now user will receive their secret key and download their file from cloud and decrypt it using their secret key.

5.4 Policy Revocation & Renewal

In this phase user will perform revocation and renewal of policies. For policy revocation, user will send revocation request to the key manager. Revocation is nothing but user will remove all the policies that he/she set before. Once user's policy revocation request is sent to key manager, they

delete all the policies of the user which in turn deletes all files of that user from the cloud. In policy renewal key manager will allow the user to renew the user existing policy. Once he/she got approval from key manager user can renew their policy. Now key manager will generate new set of keys and encrypt the user's Policy File by using user's new policy.

6. Architecture

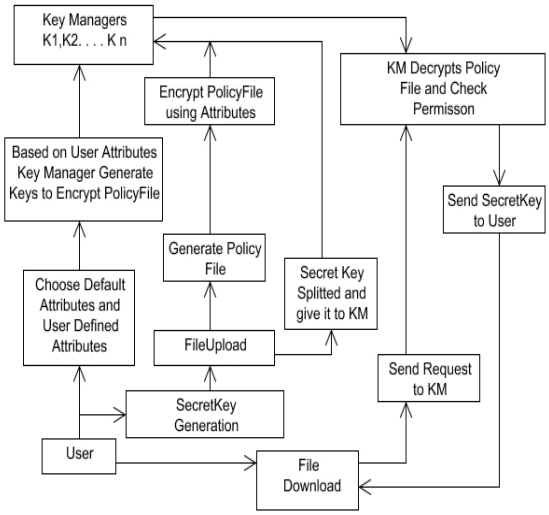

Fig 4: Architecture of proposed system

- To become a member in cloud, the user has to register with two types of attributes namely, default and user defined attributes
- Once registered, a secret key will be generated and also based on the given user attributes the key manager generates a key to encrypt the Policy File.
- User splits the secret key into n numbers and gives it to n key managers after the process of encrypting the secret key with the public key of the key managers.
- With the help of the secret key the user encrypts the file and uploads it into the cloud and simultaneously Policy File will be generated.
- Using the code generated based on the user attributes, the Policy file will be encrypted and given to the key managers.
- In order to download a file, the user has to give the registered attributes and a code is generated based on those attributes.
- If the currently generated code matches with the code generated during registration, the Policy file will be decrypted by the key manager and it checks the file access permission.
- If the permission is granted, the multiple key managers will decrypt the secret key share by using their own private keys and give the key shares to the user.
- The secret key is rebuild from the key shares using Shamir's secret key sharing technique and given to the user. With that he/she can download the file from cloud and decrypts it.

7. Algorithms & Techniques Used

- Diffie-Hellman.
- RSA.
- Elgamal.
- Data Encryption Standard.
- Shamir's (k, n) sharing.

7.1 Diffie-Hellman

Diffie-Hellman algorithm is used for the generation of shared secret key which is used for the exchange of information between two parties across an insecure channel. It is also used for securely exchanging cryptographic keys between the user and the key manager.

7.2 RSA

RSA algorithm is widely used for the encryption and decryption of data. It is an asymmetric cryptographic algorithm which uses two different keys. Since one of the key can be given to everyone, it is also known as public key cryptographic algorithm. In this system, we use RSA algorithm for the exchange of keys between the user and key manager. The public key is given to every users to encrypt their key shares and the key managers uses the private key for decrypting the secret key shares.

7.3 Elgamal

Elgamal algorithm is used for the process of encryption and digital signature. It is an asymmetric key encryption algorithm that performs encryption and decryption with the pair of different cryptographic keys. In this system, elgamal algorithm is used for the encryption of Policy File with the code generated based on the user attributes.

7.4 Data Encryption Standard

DES algorithm is symmetric which is used for encrypting and decrypting data with the same cryptographic key. In this system, the DES algorithm is used for the encryption and decryption of file using the single secret key given to the user at the time of registration.

7.5 Shamir's (k, n) sharing

Shamir's (k, n) sharing technique is used for sharing the secret key. In this technique the secret key is divided into several parts and each part is given to different participants. To rebuild the secret key some or all the parts are needed. In this system, the secret key is divided into n shares and given to n key managers using this technique. It uses k shares out of n shares to rebuild the secret key.

8. Conclusion

In the proposed system, we introduced an enhanced data security model which can be used for secure data storage, access and deletion. Considering partial trustworthy cloud servers, an improved privacy and security is given to the users by encrypting the policy file based on their own credentials. This system addresses the challenges of key management and thus enhances the security of secret key by utilizing RSA algorithm for encrypting the key shares. Hence the proposed system is efficient for the access of outsourced data when compared to the previous works.

Acknowledgement

We would like to thank IJREAT for giving us an opportunity for publishing this paper and we also like to thank our Assistant Professor, Mr.B.Ravikumar for his full support and guidance.

References

[1]. Yang Tang, Patrick P. C. Lee, John C. S. Lui, Radia Perlman, "FADE: Secure Overlay Cloud Storage with File Assured Deletion," IEEE Transaction on Dependable and Secure Computing, Nov 2012, Vol: 9, Issue: 6.

[2].M.Ali, R.Dhamotharan, E.Khan, S.U.Khan, A.V.Vasilakos, K.Li, A.Y.Zomaya, "SeDaSC: Secure Data Sharing in Clouds," IEEE System Journal, Jan2015, Vol: PP, Issue: 99.

[3]. M.Armbrust, A.Fox, R.Griffith, A.D.Joseph, R.Ktaz, A.Konwinski, G.Lee, D.Patterson, A.Rabkin, I.Stoics, and M.Zaharia, "A View of Cloud Computing," Communications of the ACM, Vol.53, No.4, 2010.

[4]. Ashish Kumar, "World of Cloud Computing & Security," International Journal of Cloud Computing and Services Science, Vol.1, No.2, June 2012.

[5].Shuhua Wu, Yuefei Zhu, "Improved Two-Factor Authenticated Key Exchange Protocol," The International Arab Journal of Information Technology, Oct 2011, Vol. 8, No.4.

[6].Dai Yuefa, Wu Bo, Gu Yaqiang, Zhang Quan, Tang Chaojing, "Data Security Model for Cloud Computing," International Workshop on Information Security and Application,Nov 2009.

[7].Lingfang Zeng, Zhan Shi, Shengjie Xu, Dan Feng, "SafeVanish: An Improved Data Self-Destruction for Protecting Data Privacy," IEEE International Conference on Cloud Computing Technology and Science, Nov 2010.

[8].Faiza Fakhar, "Management of Symmetric Cryptographic Keys in Cloud Based Environment," International Conference on Advanced Communication Technology, Jan. 2013.

[9].B.SowmyaSri, Mr.S.Vikramphaneendra,"A Secure Way for Data Storage and Forwarding in Cloud," International Journal of Advanced

Research in Computer Science and Software Engineering, Sep 2013, Vol.3, Issue 9.