ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

Cloud Storage Security Using Decentralized Access Control

[I]Ajit Bhise, [II]Chandan Kadam, [III]Gaurav Lonkar, [IV]Prashant Patil, [V]Sudarshan Borade
[I,II,III,IV,V]ISB&M School of Technology, Nande, Pune, India

Abstract
We propose a new scheme for secure cloud storage using decentralized access control that supports anonymous/unacknowledged authentication. In this, the cloud verifies the authenticity without knowing the user's details or identity before storing data. We also added feature of access policy control or authority in which only valid users are able to decrypt the stored information. Our scheme prevents replay attacks and supports creation, reading, and writing or modification data stored in the cloud. We also address user revocation policy.

Keywords
Access Control, Authentication, ABS(Attribute Based-Signature), ABE(Attribute Based-Encryption), Cloud Storage.

I. Introduction

Now a day's cloud computing is a developed technology to store data from more than one client at remote location. Cloud computing is an environment that enables users stores their data Remotely. The term 'cloud' is analogical to the internet. It helps organization and government agencies reduce their financial overhead of data management. Cloud computing is based on cloud drawing used in to represent telephone network later to depict internet. Cloud computing is internet oriented computing where virtual share servers provide software service, platform service, infrastructure service devices and other resources and hosting to customers on a pay-as-you basis. Cloud computing customers do not own the physical structure; rather they rent the usage from a third-party provides.

There are three objectives to be main issue:

Confidentiality – Confidentiality means to limiting information access and sensitive information should kept secret from individuals who are not authorized to see the information.

Integrity – Integrity should not be altered without detection.

Availability – Availability means to availability of information resources.

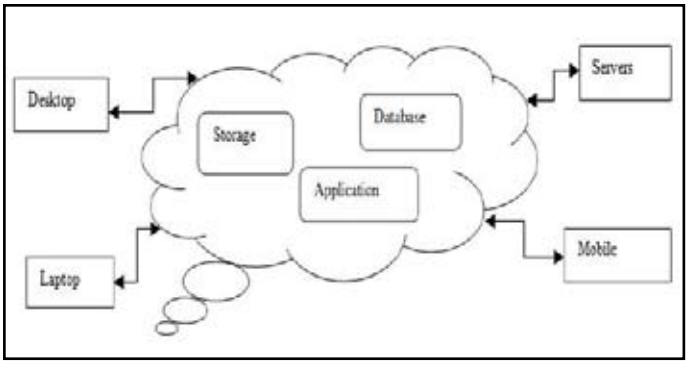

Fig.1: Example of data sharing with cloud storage.

To achieve data transaction secure in cloud, we used suitable cryptography method. The data owner must encrypt the file and store this file to the cloud. If a third person downloads the file, he may view the record if he had the key which is used to for decrypt the encrypted file. Sometimes this may be collapse because of the technology development and the hackers. We studied the Anonymous Authentication for data storing to clouds[1]. Anonymous authentication is the process of without the user details or attributes of the user. So the cloud server doesn't know the user details or user identity, which provides privateness to the users to hide their details from other users of that cloud[1].

Access control is the gaining importance in social networking where user store their personal information, pictures, videos & shared them with group of users. so, we have studied Access control in social networking. such data are being stored in cloud. It is very important that only authorized users given access to those information. A similar situation arises when the data stored in clouds[2]. E.g. dropbox.

In this paper, we studied Attribute Based Encryption scheme is used to avoid unauthorized access[3]. revocation scheme is used for time based file assured deletion[2]. This paper addresses this open issue by, on one hand, characteristics and implementation of access policies based on data qualities, and, then again, allowing the data owner to deputy the majority of the computation undertakings included in fine-grained data access control to mistrusted cloud servers without exposing the underlying data substance. We accomplish this goal by combining and exploiting techniques of decentralized key policy Attribute Based Encryption (KP-ABE) [2,3].

II. Key Management

In this paper, cryptographic keys to protect data files stored on the cloud

Public Key: The Public key is binary key, generated and maintained by the Key manager, which is used for encryption/ decryption purpose.

Private Key: It is the combination of the username, password and two safety question of user's choice. The secret key is maintained by client, which is used for encrypt / decrypt the file.

Access key: It is associated with a access policy. The access key is built on attribute based encryption. access policy is of read or write.

III. Proposed Work

A. Encryption/Decryption

We used RSA algorithm for encryption/Decryption purpose. This algorithm is used for secure transaction of data. we use the RSA algorithm with key size of 2048 bits. The key distribution is possible . If a user wants to access the file he may need to provide the four set of data to produce the single secret key to manage encryption as well as decryption.

B. File Upload/Download

1. File Upload

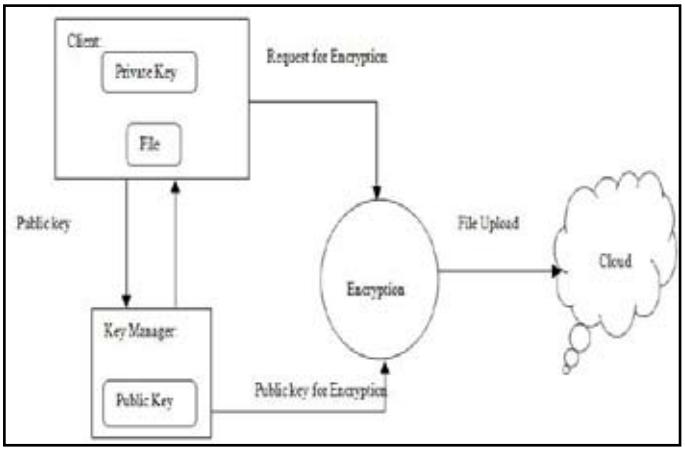

Fig 2: File upload process.

The client send request to the key manager for the public key, which will be generated according to the access policy associated with the file. Different access policies for files, public key also different. But for same public key for same access policy will be generated. Then the client generates a secret key by combining the username, password and safety credentials. Then the file is encrypted with the public key and secret key and forwarded to the cloud.

2. File Download

The user can download the file after the authentication process. As the public key maintained by the manager, the client send the request to the key manager for public key. The authenticated user can get the public key. Then the user can decrypt the file with the public key and the secret key. The users credentials were stored in the user itself. During download the file the cloud will identify the authenticate user. But the cloud doesn't have any the details of the user.

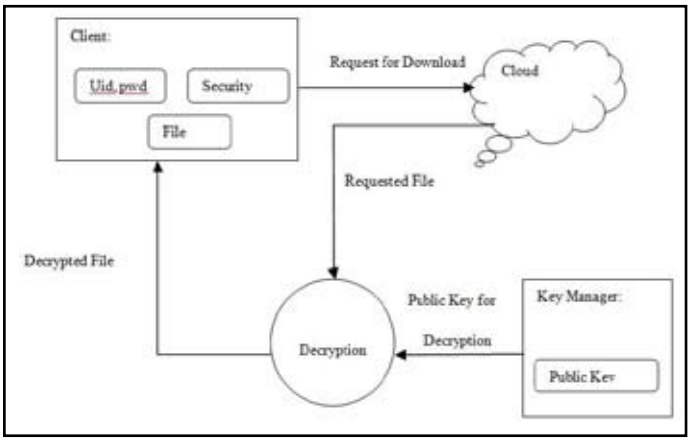

Fig. 3: File download process

C. Policy Revocation

The access policy of a file may be revoked under the request by the user, when expiring the time period or completely move the files from one cloud to another cloud. When any of the above criteria exists the access policy will be revoked and the key manager will totally removes the public key of the file. So no one recover the control key of a revoked file in future. For this reason we can say the file is easily deleted [2,3].

D. File Access Control

Ability to control the access to host systems and applications with the help of communication links. To achieve, access must be authenticated. After achieved the authentication process the users must associate with correct access policies with the files.

IV. Conclusion

We have presented a secure cloud storage using decentralized access control technique with anonymous/unknowledged authentication, which provides to prevents replay attacks and user revocation. The cloud don't know the attribute of the user who stores information but only verifies the user's credentials.

References

[1]. *S Sushmita Ruj, Milos Stojmenovic and Amiya Nayak, "Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS*

[2]. *S. Jahid, P. Mittal, and N. Borisov, "EASiER: Encryption-Based Access Control in Social Networks with Efficient Revocation," Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS), 2011.*

[3]. *Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. ACM Conf. Computer and Comm. Security, pp. 89-98, 2006.*

[4]. *M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia. A View of Cloud Computing. Comm. of the ACM, 53(4):50 – 58, Apr 2010.*

[5]. *A.B. Lewko and B. Waters, "Decentralizing Attribute-Based Encryption," Proc. Ann. Int'l Conf. Advances in Cryptology (EUROCRYPT), pp. 568-588, 2011.*

[6]. *H.K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-Based Signatures," Topics in Cryptology - CT-RSA, vol. 6558, pp. 376-392, 2011.*

[7]. *R.L. Rivest, A. Shamir, and Y. Tauman, "How to Leak a Secret," Proc. Seventh Int'l Conf. Theory and Application of Cryptology and Information Security (ASIACRYPT), pp. 552-565, 2001.*

[8]. *R.K.L. Ko, P. Jagadpramana, M. Mowbray, S. Pearson, M. Kirchberg, Q. Liang, and B.S. Lee, "Trustcloud: A Framework for Accountability and Trust in Cloud Computing," HP Technical Report HPL-2011-38, http://www.hpl.hp.com/techreports/ 2011/HPL-2011-38.html, 2013.*