International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) e-ISSN: 2395-5325
Volume3, Issue 6 (June '2017)

ENSURING CLOUD SECURITY THROUGH ACCESS CONTROL WITH DUAL ENCRYPTION SCHEME

K.Ganagavalli,
Assistant Professor,
Computer Science and Engineering,
Bannari Amman Institute of Technology,
Sathyamangalam, India.

V. Krishnamoorthy,
Assistant Professor,
Information Technology,
Adhiyamaan college of Engineering,
Hosur, India.

A.Banu,
Assistant Professor,
Computer Science and Engineering,
Bannari Amman Institute of Technology,
Sathyamangalam, India.

Abstract: In the upcoming computer world cloud computing has been becoming an emerging technology for sharing resources and outsourcing of data. While storing the data in cloud, the data owners need not to run and keep their data in their personal devices. Instead, the data will be maintained by the cloud servers which are maintained by a third party. From users' point of view, putting sensitive data on the cloud and losing control of these data may increase the risk of being abused. Access control is a mechanism that is used for preventing unauthorized access of the resource. This service provides controls over the data such that who can access to a resource, under what conditions their access can occur, and also restricts the actions performed by a person on the resources. To achieve this, an identity-based proxy re-encryption scheme has been adopted which allows a user to encrypt his data under his identity and to delegate his data management capability to the cloud. The cloud, which could grant the access to an authorized user by transforming the cipher text encrypted with the data owner's identity to the one with the sharer's identity. This algorithm achieves more security than the existing algorithms in data management and also restricting the resource access control.

Keywords: Cloud, Access control, Proxy Re-Encryption.

I. INTRODUCTION

Cloud computing is an emerging infrastructure where both of data storage and the data processing happen outside of the device from which an application is launched. It portends a major change in the way of storing information and running applications. Instead of running applications and related data in local computer, everything will be hosted in the "cloud" an external server**.** Cloud computing offers customers a more flexible way to obtain computation and storage resources on demand. Cloud computing lets you access all your applications and documents from anywhere in the world, freeing you from the confines of the desktop and making it easier for group members in different locations to collaborate. With traditional desktop computing, you run copies of software programs on each computer you own. The documents you create are stored on the computer on which they were created. Although documents can be accessed from other computers on the network, they can't be accessed by computers outside the network. This phenomenon is PC-centric.

With cloud computing, the software programs aren't run from our personal computer, but are rather stored on servers accessed via the Internet. If one computer crashes, the software is still available for others to use. Same goes for the documents you create; they are stored on a collection of servers accessed via the Internet. Anyone with permission can access the documents in real time. Unlike traditional computing, cloud computing isn't PC centric, it's document-centric.

II. SURVEY OF EXISTING EVASION TECHNIQUES, TOOLS AND COUNTERMEASURES

To provide privacy and enhance security for cloud users, there are quite a few security proposals like Attribute based encryption schemes and Identity based encryption schemes. In Key Policy attribute based encryption scheme(KPABE) for helping the data owner to enjoy fine-grained access control of data stored on un trusted cloud servers, a feasible solution would be provided by encrypting data through certain cryptographic primitives, and disclosing decryption keys only to authorized users. Unauthorized users, including cloud servers, are not able to decrypt since they do not have the data decryption keys.

One critical issue with this branch of approaches is how to achieve the desired security goals without introducing a high complexity on key management and data encryption. Resolve this issue either by introducing a per file access control list (ACL) for fine-grained access control, or by categorizing files into several file groups for efficiency. As the system scales, however, the complexity of the ACL-based scheme would be proportional to the number of users in the system. The file group-based scheme, on the other hand, is just able to provide coarse-grained data access control. It actually still remains open to simultaneously achieve the goals of fine-grainedness,

scalability, and data confidentiality for data access control in cloud computing. The complexity of encryption is just related the number of attributes associated to the data file, and is independent to the number of users in the system. It achieves high scalability and data confidentiality.

It achieves fine grained access control.Not flexible in attribute management. Not scalable in multiple levels attributes Multi Recipient algorithm is another access control mechanism widely used. It is a public key cryptography primitive for one to- many communications. Exploring the MRE, the size of cipher text is less than the trivial *n*-recipient solutions which is just a concatenation of independently encrypted messages for *n* recipients using a single-recipient public key encryption algorithm. However predefining a set of sharers in advance makes it difficult to implement in a scalable dynamic cloud. When changing the access policy of sharing, data owner has to retrieve the data from the cloud, decrypt cipher text, re-encrypt the data corresponding to distinct user. The expensive cost on computation and communication in the updating of access policy makes it impractical in the cloud. This technique is easy to implement in a scalable cloud environment. Predefining a set of sharers in advance is not possible in a dynamic cloud environment. It also produces communication overhead and it's quite expensive.

III. OVERVIEW

Due to the dynamic network topology of networks the existing security proposals presented which could achieve both of the confidentiality and data access control may not be suitable in dynamic cloud computing . Specifically, the attribute based encryption or multi-recipient encryption which is more suitable for a static and small-scale network rather than for the dynamic network and potentially comprised of millions of users who could join or leave the network arbitrarily. Moreover one user may possess many attribute and conversely one attributes may be possessed by many users which makes the data owner difficult to set up the correspondence between the users and attributes. These observations motivate us to propose a novel data service mechanism in dynamic cloud computing.

IV. SECURITY MODEL

In this proposed system, a user-efficient and secure data service mechanism in dynamic cloud computing, which enables the users to enjoy a secure outsourced data services at a minimized security management overhead. The core idea of project is that it outsources not only the data but also the security management to the mobile cloud in a trusted way. To achieve this, we adopt an identity-based proxy re-encryption scheme which allows a mobile user to encrypt his data under his identity to protect his data from leaking and, at the same time, to delegate his data management capability to the mobile cloud. Furthermore the mobile user could delegate his access control capability to the cloud, which could grant the access of an authorized user by transforming the cipher text encrypted with the data owner's identity to the one with the sharer's identity.

For that proxy re-encryption the cloud uses the secret key of the sharer who is an authorized user had already registered with the data owner. So that it could be decrypted by sharers in the future using their secret key generated based on their identity. And different sharer's identity corresponding to different proxy re-encryption key is generated at the time of their registration. Given the proxy re-encryption key by the owner, the cloud can convert the cipher text outsourced by the data owner to the cipher text that can be decrypted by the sharer.

As mentioned above, in my proposal the role of the cloud is:

- Providing secure storage for the users.
- Serving as the secure proxy.

From the perspective of the user, the task of convert cipher text is relinquished to the cloud, and the user just only needs to upload a key whose size is far less than the whole file.

V. PROTOCOL

The illustration is given in Figure 1. In this the data owner uploads the encrypted file to the cloud. Then the cloud performs the Proxy-Reencrytion using the sharer's identity and stores it in the database. Whenever the user wants to access the file he retrieves it by decrypting the file using his secret identity.

VI. MODULE DESCRIPTION:

The major modules of this project are as illustrated in :

- System Set up
- Data Encryption
- Data sharing
- Proxy re-encryption.
- Data Access

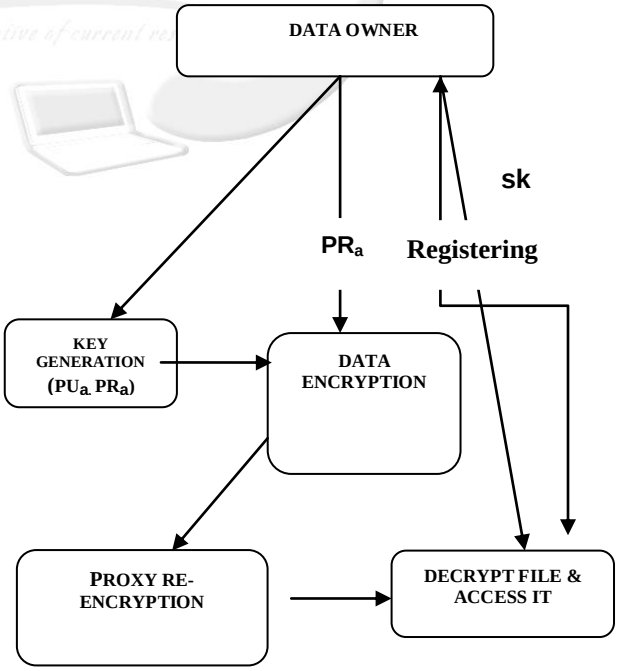


FIGURE : PROTOCOL MODEL

6.1 SYSTEM SET UP:

In this phase, two important tasks are done.

- The system setup
- Key Generation.

In the system set up the system parameters are built up. The system is to guarantee the authorized sharers who can access the data. In the Key Generation phase a pair of keys is generated for the data owner using a public key cryptographic algorithm. Here I adopted a public cryptography algorithm at the owner side. A pair of keys **(PU_a, P_{Ra})** is generated. In this each user needs to register with the system using his identity to obtain a secret key corresponding to his identity. The data owner can share his public key($PU_{a)}$ only with the identity of the registered sharers.

6.2 DATA ENCRYPTION:

In the data encryption phase the data owner runs the Encrypt algorithm and generates

$$Mi=(PU_a;F.e(PR_a;H1(ID))) \quad (6.1)$$

As mentioned in the previous phase the keys for encryption are generated whenever the data owner choose a file for uploading .

$$C(F)=(F.e(PR_a) \quad (6.2)$$

The data owner performs a first level encryption using a public key cryptographic algorithm with his private key ($PR_{a)}$ after that the cipher text can be transformed to the cloud where a second level encryption (IB-PRE) is performed.

6.3 DATA SHARING:

In this phase the proxy re-encryption key generation algorithm is using an algorithm RK Gen(sk). Each sharer has to register with the system and obtain a secret key corresponding to his identity,

$$sk=H1(ID_u)=IBE(ID_u) \quad (6.3)$$

The secret key is generated as the Hash function of the sharer's identity. The re encryption key s*k* will be used by the cloud to transform the cipher text *F* to the cipher text under sharer's secret key. The data owner forwards s*k* to the cloud which means that the cloud is delegated to manage the data in behalf of the owner. The cloud can deploy the re-encrypt key s*k* to permit the authorized user to get the cipher text decrypted with his own secret key.

6.4 DATA ACCESS:

When the sharer wants to access the file, he sends a request to the cloud server. The cloud determines the validity of the sharer by checking if it has a re-encryption key to the sharer. With the re-encryption key is existed, the cloud server can run the RKGen algorithm and achieve the re-encryption ciphertext

$$C = (E(IBE(ID_s),(c(f)) = (E(sk,(F.e(PR_a)) \quad (6.4)$$

Then the sharer fetches the re-encrypted data from the cloud servers, and runs the Decrypt algorithm on *Mi* with his secret key to obtain the

$$D(F)=C(F)=Dec(sk,C); \quad (6.5)$$

Then for obtaining the original file uploaded by the owner,the user have to perform another decryption using the owner's public key($PU_{a).}$ The original file is generated as

$$F=Dec(PU_a,D(F)); \quad (6.6)$$

As any sharer can obtain the required file with the permission of the data owner.

6.5 ADVANTAGES OF THE PROPOSED SYSTEM:

- Strong access control: Only authorized user can decrypt the data.
- Flexibility: Our protocol is flexible to operate and scalable with the growth of data sharers.
- Low overhead: The cost of achieve, change and update access policy is relatively lower.

6.6 EXPERIMENT RESULTS:

As the scheme relatively reduces the communication overhead this intern reduces the computation cost. The reduction of communication overhead is shown in the following graph by making ratio between the transferred file size and the number of users.

In the Multi Recipient algorithm the data transferred to cloud is the data which is encrypted n times for n number of users individually and then the whole data is transmitted.

The data transferred to cloud can be calculated as

$$\text{Transferred data} = \sum_{i=0}^{n} ([E(Ki,M)]) \text{ for } i=1 \text{ to } n \quad (6.7)$$

In this M is the data file which is to be encrypted.

Ki is the secret key of the user i.

E(Ki,M) is the data file encrypted using the ith user's secret key.

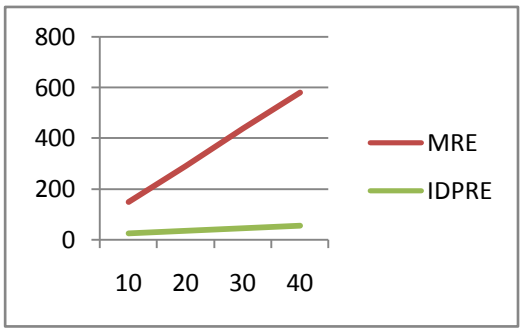
In IB-PRE the transferred data consists of the encrpted file and the key of the user at his time of registeration. Here the transferred data can be calculated as

$$\text{Transferred data} = E(PRa,M) + \sum_{i=0}^{n} ski \quad (6.8)$$

In this E(PRa,M) is the encrypted data file with the owners private key.

PRa is the private key of the data owner.

Ski is the secret key of the ith user.



VII. CONCLUSION:

In this project I explored identity based proxy re-encryption scheme to make the users easily implement fine-grained access control of data and also guarantee the data privacy in the cloud. At the same time, the cost of updating of access policy and communication is also reduced in this mechanism.

As the keys are generated only by the administrator there will be no abuse of keys. Each user has an identical key based on their identity there will be no duplicates. Each user is

registered with the Administrator and the secret key is only known to the user and owner there will be no unauthorized access. As the data is forwarded to the cloud in encrypted format, it does not have any knowledge about the data. Though the hackers get the data from the cloud they don't know the logic and cannot decrypt the data. As the encrypted data and keys only transferred the computation cost will be comparatively low. There will no limitation in the number of the sharer.

VIII.REFERENCE

[1] Weiwei Jia *yz*, Haojin Zhu*y*, Zhenfu Cao*yx*, Lifei Wei*y*, Xiaodong Lin "A Secure Data Service Mechanism in Mobile Cloud Computing"
[2] S.Yu, C.Wang, K. Ren, and W.Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in INFOCOM 2010, pp. 534–5
[3] K. Kurosawa, "Multi-recipient public-key encryption with shortened ciphertext," in Public Key Cryptography, 2002, pp. 48–63.
[4] Juniper, "Mobile cloud computing: $9.5 billion by2014,"Juniper,http: www.readwriteweb.com/archives, Tech. Rep., 2010.
[5] K. D. Bowers, A. Juels, and A. Oprea, "Hail: a high-availability andintegrity layer for cloud storage," in ACM Conference on Computer and Communications Security, 2009, pp. 187–198.
[6] R. Curtmola, O. Khan, R. C. Burns, and G. Ateniese, "Mr-pdp: Multiplereplicaprovable data possession," in ICDCS, 2008, pp. 411–420.
[7] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," in INFOCOM, 2010, pp. 525–533.
[8] S. Creese, P. Hopkins, S. Pearson, and Y. Shen, "Data protection-aware design for cloud services," in CloudCom, 2009, pp. 119–130.
[9] R. Sandhu, E. Coyne, H. Feinstein, and C. Youman, "Role-based access control models," Computer, vol. 29, no. 2, pp. 38–47, 2002.
[10] R. Sandhu and P. Samarati, "Access control: principle and practice," Communications Magazine, IEEE, vol. 32, no. 9, pp. 40–48, 2002.
[11] S. D. C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, "Over-encryption: Management of access control evolution on outsourced data," in VLDB, 2007, pp. 123–134.
[12] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," SIAM Journal on Computing, vol. 32, no. 3, pp. 586–615,nb2003.
[13] R. Curtmola, O. Khan, R. C. Burns, and G. Ateniese, "Mr-pdp: Multiple replica provable data possession," in ICDCS, 2008, pp. 411–420.
[14] . C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," in INFOCOM, 2010, pp. 525–533.
[15] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing," in ESORICS, 2009, pp. 355–370.
[16] Ruoyu Wu, Xinwen Zhang, Gail-Joon Ahn, Hadi Sharifi, Haiyong Xie, "Design and Implementation of Access Control as a Service for IaaS Cloud" in Scienceengineering.org ,2013, vol.2, no.3, pp. 115-130.
[17] Jan Kolter, Rolf Schillinger, Günther Pernul,"Building a Distributed Semantic-aware Security Architecture" in IFIP, 2007, vol.232, pp 397-408.