International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

IJIEMR Transactions, online available on 16th July 2017. Link :
http://www.ijiemr.org/downloads.php?vol=Volume-6&issue=ISSUE-5

Title: Autogenously Destructed Secure Framework For Cloud Computing.

Volume 06, Issue 05, Page No: 1890 – 1893.

Paper Authors

*** M.NAGARAJU, B.NEHRU.**

* Dept of CSE, Sri Venkateshwara Engineering College.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

AUTOGENOUSLY DESTRUCTED SECURE FRAMEWORK FOR CLOUD COMPUTING

***M.NAGARAJU, **B.NEHRU**

*PG Scholar, Dept of CSE, Sri Venkateshwara Engineering College, Suryapet, T.S, India

**Assistant Professor, Dept of CSE, Sri Venkateshwara Engineering College, Suryapet, T.S, India

ABSTRACT:

Cloud computing provides many services and simple ways of data sharing and collaboration. Since this new computing technology requires users to entrust their valuable data to cloud providers, there have been increasing security and privacy concerns on outsourced data. This project helps them to store files in cloud and revoke them in a secure manner. Identity based schemes like Attribute-Based Encryption (ABE) have been proposed for access control of outsourced data in cloud computing, however, most of them suffer from inflexibility in implementing complex access control policies. The proposed scheme used is Hierarchical Attribute-Set-based encryption by extending cipher text-policy Attribute-Set-Based Encryption (ASBE) with a hierarchical structure of users. This paper reviews some security mechanisms along with attribute based encryption (ABE) where the data is encrypted even prior to its storage on the cloud and also the issue of revoked users, where the revoked user should be restrained to access the data stored on the cloud.

Keywords: Attribute-Based Encryption, Revocation

INTRODUCTION

Cloud computing is a computing technology, and the internet has grown in recent years. It can share the software and hardware resource, and provides resources to a user's computer or mobile device. The user can obtain a more efficient service because cloud computing can integrate resources. Thus, cloud service providers have joined to build cloud environments and provide services to the user. The main objective of this project to provide the better service to the cloud user with file security. Mainly used to develop a better communication between the user and the cloud service provider. User can get the cloud request and upload the files with encryption and re encryption format. When the out sourcing process the particular user can send the file revocation request to the cloud server. After the completion of revocation request it should be combine the process with private key and updated key. PKG (private key generator) can generate the private key and send to the user and KU-CSP (key update cloud service provider). Cloud can send the updated Key to the user when the file revocation process. Finally the files are downloaded from the server with combine key process.

Related Work: Recently, some attribute revocable ABE schemes have been proposed. We described storage systems and individual storage devices themselves become networked, they must defend both against the usual attacks on messages traversing an untrusted potentially public network as well as attacks on the stored data itself. This is a challenge because the primary purpose of networked storage is to enable easy sharing of data, which is often at odds with data security. To protect stored data, it is not sufficient to use traditional network security techniques that are used for securing messages between pairs of users or between clients and servers. Thinking of a stored data item as simply a message with very long network latency is a misleading analogy. Since the same piece of data could be read by multiple users, when one user places data into a shared storage system, the eventual recipient of this "message (stored data item) is often not known in advance. In addition, because multiple users could update the same piece of data, a third user may from time-to-time update "the message" before it reaches its eventual recipient. Stored data must be protected over longer periods of time than typical message round-trip times.

In the ABE system, an attribute is supposed to be shared by a group of users. Then it is a considerable situation where the members may change frequently in the group. However, a new user might be able to access the previous encrypted data before the user comes to hold the attributes until the data is re-encrypted with the update attribute keys by periodic rekeying which was named backward secrecy. On the other hand, a revoked user would be able to access the encrypted data until the next expiration time which was named forward secrecy. Therefore, the uncontrolled period has serious vulnerability.

Representative Approaches: Before introducing representative approaches, we explain the system model in Figure 1, and list all notations used in this paper.

• The Data Owner: An individual consumer or organization has a lot of data files and needs to store in the cloud. The data owner is responsible for defining (attribute-based) access policy, and encrypting own data under the policy before distributing it.

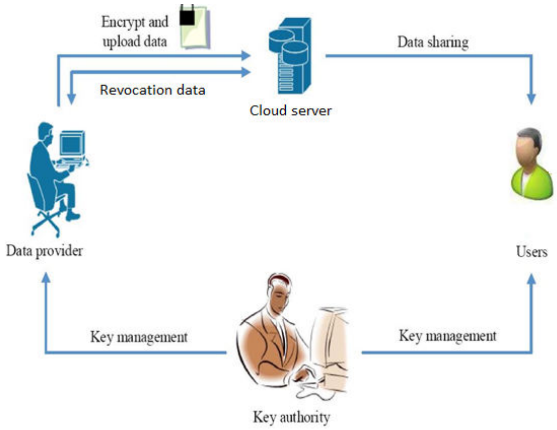

Fig1: Architecture of ABE based Revocation

• Users: User wants to access the data from the data owner. If a user possesses a set of attributes satisfying the access policy of the encrypted data, he/she will be able to decrypt the ciphertext and obtain the data.

• Cloud Storage Server (CSS): A cloud service provider has huge storage space, computation resource and shared service to provide the clients. It is responsible for controlling the data storage in outside users' access, and provides the corresponding contents.

- Trusted Authority (TA): A trusted organization has expertise and capabilities that the clients do not have. It generates public and secret parameters for ABE, then responsible for issuing, revoking and updated attribute key for the user. It also grants differential access rights to individual users based on their attributes.

Revocation in ABE: It is a challenging problem to revoke attributes and users efficiently and on-demand in ABE. Several attribute revocable ABE schemes have been proposed recently. Yang et al. proposed a new CP-ABE scheme that resolves the issue of revocation including the entire user access privilege and just partial access right of the user. They realized revocation by revoking attribute itself using timed rekeying mechanism, which is implemented by setting expiration time on each attribute. However, these approaches have two main problems. First problem is the security degradation in terms of the backward and forward secrecy. The other is the scalability problem. The attribute authority periodically announces the unrevoked users to update their keys. Hence, immediate revocation schemes instead of periodical revocation have been proposed. We introduce a mediator which maintains a revocation list so as to implement immediate attributes revocation. The data owner may make a choice between the direct revocation model and the indirect revocation model. The data owners and the attribute authority can delegate most of laborious tasks to revocation proxy servers with the technique of proxy re-encryption. However, these revocation schemes will cause the key update operation of large numbers of users.

User Revocation:

A.REVOCATION USING ABE In this scheme revocation is done using CP-ABE. The users in a group are assigned a set of attributes in their secret key and are distributed to the user, when a user is revoked, then the data is re-encrypted making the secret key of the revoked user useless, this scheme is secure but involves more computational overhead as, the data needs to be encrypted whenever there is an user revocation.

B.REVOCATION USING PRE Revocation is done using the idea of proxy re-encryption, data owner's private key is divided into two parts .one half part is stored at data owner's place and other half is stored in the cloud proxy, the owner encrypts the data with the key available with him and the cloud encrypts the data again using the other part of the key .Any user who has access rights can decrypt the data with two parts of the key .When the data owner wishes to revoke any user, informs cloud to remove the user's key piece from the cloud, this method of revocation does not require re-encryption of data thereby reducing the computational cost but, likely hood of collusion attacks are more and also the cloud proxy may suffer from too many encryption and decryption operations.

C.REVOCATION USING C-PRE AND COMBINED CPABE This scheme is a combination of Clock based proxy re-encryption and attribute based encryption. Each user is associated with set of attributes and eligible time, attributes and the time does not satisfy when the user is revoked. The advantage of this technique is re-encryption which is delegated to the cloud instead of data owner.

When very large data files are considered this scheme is not very efficient.

CONCLUSION

In this paper, securely share the data file among the dynamic groups. Without revealing their identity members in the same group can share the data efficiently. This project can be very help full to the user and the cloud service provider. Data sharing and collaboration has become prominent in the current day scenario, therefore much importance is given to the security of data stored in the cloud. Since the data is dynamic, many security and access control schemes are proposed, in this paper, few recent approaches in data security and also some access control mechanisms for revoked users have been presented.

REFERENCES

[1] Z. Wan, J. Liu, R. H. Deng, "HASBE: A hierarchical attribute-based solution for flexible and scalable access control in cloud computing," IEEE Transactions on Information Forensics and Security, vol. 7, no. 2, pp. 743-754, 2012.

[2] J. Wu, Q. Shen, T. Wang, J. Zhu, J. Zhang, "Recent advances in cloud security," Journal of Computers, vol. 6, no. 10, pp. 2156-2163, 2011.

[3] Z. Ma, K. Fan, M. Chen, Y. Yang, X. Niu, "Trusted digital rights management protocol upporting for time and space constraint," Journal on Communications, vol. 29, no. 10, pp. 153-164, 2008.

[4] X. Wang, Y. Lin, "An efficient access control scheme for outsourced data," Journal of Computers, vol. 7, no. 4, pp. 918-922, 2012.

[5] D. Koo, J. Hur, H. Yoon, "Secure and efficient data retrieval over encrypted data using attribute-based encryption in cloud storage," Computers & Electrical Engineering, vol. 39, no. 1, pp. 34-46, 2013.

[6] M. Luo, C. Zou, J. Xu, "An efficient identity-based broadcast signcryption scheme," Journal of Software, vol. 7, no. 2, pp. 366-373, 2012.

[7] J. Hur, D. Noh, "Attribute-based access control with efficient revocation in data outsourcing systems," IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 7, pp. 1214-1221, 2011.