International Journal of Science Engineering and Advance Technology, IJSEAT, Vol 2, Issue 9, September-2014 | ISSN 2321-6905

International Journal of Science Engineering and Advance Technology

Sheltered Compound Vendor Data Apportioning For Vibrant Clusters In The Cloud

A Madhusudhana Rao#1,O Srinivas#2
#1 Student of M.Tech Department of Computer Science Engineering G.V.R&S college of Engineering & Technology.
#2 Department of Computer Science Engineering G.V.R&S college of Engineering & Technology, GUNTUR

ABSTRACT:

Cloud computing is an emerging computing paradigm in which resources of the computing infrastructure are provided as services over the Internet. Sharing data in a multiowner manner while preserving data and identity privacy from an untrusted cloud is still a challenging issue, due to the frequent change of the membership. To preserve data privacy, a basic solution is to encrypt data files, and then upload the encrypted data into the cloud. In this paper we are further extending the basic MONA by adding the reliability as well as improving the scalability by increasing the number of group managers dynamically. This paper proposes how user can access data after the time out. The storage overhead and encryption computation cost of our scheme are independent with the number of revoked users.

Index Terms— Cloud Computing, dynamic groups, data sharing, reliability, integrity, scalability,privacy-preserving.

INTRODUCTION

CLOUD computing is recognized as an alternative to traditional information technology due to its intrinsic resourcesharing and low-maintenance characteristics. In cloud computing, the cloud service providers(CSPs), such as Amazon, are able to deliver various services to cloud users with the help of powerful datacenters. By migrating the local data management systems into cloud servers, users can enjoy highquality services and save significant investments on their local infrastructures. One of the most fundamental services offered by cloud providers is data storage. Let us consider a practical data application.

A company allows its staffs in the same group or department to store and share files in the cloud. By utilizing the cloud, the staffs can be completely released from the troublesome local data storage and maintenance. However, it also poses a significant risk to the confidentiality of those stored files. Specifically, the cloud servers managed by cloud providers are not fully trusted by users while the data files stored in the cloud may be sensitive and confidential, such as business plans. To preserve data privacy, a basic solution is to encrypt data files, and then upload the encrypted data into the cloud .

Unfortunately, designing an efficient and secure data sharing scheme for groups in the cloud is not an easy task due to the following challenging issues.

EXITING SYSTEM

In the literature study we have seen many methods for secure data sharing in cloud computing, however most methods failed to achieve the efficient as well as secure method for data sharing for groups. To provide the best solutions for the problems imposed by existing methods, recently the new method was presented called MONA [1]. This approach presents the design of secure data sharing scheme, Mona, for dynamic groups in an untrusted cloud. In Mona, a user is able to share data with others in the group without revealing identity privacy to the cloud.

Additionally, Mona supports efficient user revocation and new user joining. More specially, efficient user revocation can be achieved through a public revocation list without updating the private keys of the remaining users, and new users can directly decrypt files stored in the cloud before their participation. Moreover, the storage overhead and the encryption computation cost are constant. Therefore practically in all cases MONA outperforms the existing methods.

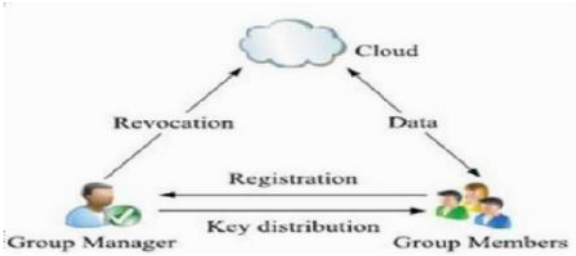

Fig 3.1 Existing System Model *Revocation*

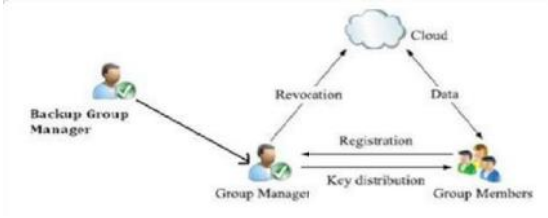

Fig 4.1 Proposed System Model

RELATED WORK

E. Goh, H. Shacham, N. Modadugu, and D. Boneh [4] the use of SiRiUS is compelling in situations where users have no control over the file server (such as Yahoo! Briefcase or the P2P file storage provided by Farsite). They believe that SiRiUS is the most that can be done to secure an existing network file system without changing the file server or file system protocol. Key management and revocation is simple with minimal out-ofband communication. File system freshness guarantees are supported by SiRiUS using hash tree constructions. SiRiUS contains a novel method of performing file random access in a cryptographic file system without the use of a block server. Extensions to SiRiUS include large scale group sharing using the NNL key revocation construction. B. Wang, B. Li, and H. Li, [5] in this paper, we propose Knox, a privacy-preserving auditing scheme for shared data with large groups in the cloud. They utilize group signatures to compute verification information on shared data, so that the TPA is able to audit the correctness of shared data, but cannot reveal the identity o f the signer on each block. With the group manager's private key, the original user can efficiently add new users to the group and disclose the identities of signers on all blocks. The efficiency of Knox is not affected by the number of users in the group.

PROPOSED SYSTEM

To achieve the reliable and scalable in MONA, in this paper we are presenting the new framework for MONA. In this method we are further presenting how we are managing the risks like failure of group manager by increasing the number of backup group manager, hanging of group manager in case number of requests more by sharing the workload in multiple group managers. This method claims required efficiency, scalability and most importantly reliability.

Advantage

To overcome the disadvantage of existing system MONA, in the proposed MONA is if the group manager stop working due to large number of requests coming from different groups of owners, then backup group manager will remains available. Here user get extra time for accessing data after the time out by sending request to the cloud.

Scheme Description

This section describes system, initialization, user registration, user revocation, file generation, file deletion and file access.

Cloud Computing

In cloud computing, the word cloud is used as a metaphor for "the Internet" so the phrase cloud computing means "a type of Internetbased computing," where different services - such as servers, storage and applications -- are delivered to an organization's computers and devices through the Internet.

System Initialization

The group manager takes charge of system initialization
as follows: Generating a bilinear map group system

Cloud Module

In this module, we provide priced abundant storage services. The users can upload their data in the cloud. We develop this module, where the cloud storage can be made secure. However, the cloud is not fully trusted by users since the CSPs are very likely to be outside of the cloud users' trusted domain. Similar to we assume that the cloud server is honest but curious. That is, the cloud server will not maliciously delete or modify

user data due to the protection of data auditing schemes, but will try to learn the content of the stored data and the identities of cloud users.

Group Manager Module
Group manager takes charge of followings,

1. System parameters generation,
2. User registration,
3. User revocation, and
4. Revealing the real identity of a dispute data owner.

Therefore, we assume that the group manager is fully trusted by the other parties. The Group manager is the admin. The group manager has the logs of each and every process in the cloud. The group manager is responsible for user registration and also user revocation too.

Group Member Module

Group members are a set of registered users that will

1. Store their private data into the cloud server and

2. Share them with others in the group. Note that, the group membership is dynamically changed, due to the staff resignation and new employee participation in the company. The group member has the ownership of changing the files in the group. Whoever in the group can view the files which are uploaded in their group and also modify it. The group meme

File Security Module

1. Encrypting the data file.

2. File stored in the cloud can be deleted by either the group manager or the data owner. (i.e., the member who uploaded the file into the server).

Group Signature Module

A group signature scheme allows any member of the group to sign messages while keeping the identity secret from verifiers. Besides, the designated group manager can reveal the identity of the signature's originator when a dispute occurs, which is denoted as traceability.

User Revocation Module

User revocation is performed by the group manager via a public available revocation list (RL), based on which group members can encrypt their data files and ensure the confidentiality against the revoked users.

CONCLUSION

In this paper, we design a secure data sharing scheme, for dynamic groups in an untrusted cloud. A user is able to share data with others in the group without revealing identity privacy to the cloud. Additionally, Its supports efficient user revocation and new user joining. More specially, efficient user revocation can be achieved through a public revocation list without updating the private keys of the remaining users, and new users can directly decrypt files stored in the cloud before their participation. Moreover, the storage overhead and the encryption computation cost are constant. Extensive analyses show that our proposed scheme satisfies the desired security requirements and guarantees efficiency as well.

REFERENCES

[1]Xuefeng Liu, Yuqing Zhang, Boyang Wang, and Jingbo Yan, "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 24, NO. 6, JUNE 2013.

[2]M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A View of Cloud Computing," Comm. ACM, vol.53, no. 4, pp. 50-58, Apr. 2010.

[3] S. Kamara and K. Lauter, "Cryptographic Cloud Storage," Proc. Int'l Conf. Financial Cryptography and Data Security (FC), pp. 136- 149, Jan. 2010.

[4] E. Goh, H. Shacham, N. Modadugu, and D .Boneh, "Sirius: Securing Remote Untrusted Storage," Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 131-145, 2003. [5]B. Wang, B. Li, and H. Li, "Knox: Privacy-Preserving Auditing for

Shared Data with Large Groups in the Cloud," Proc. 10th Int'l Conf. Applied Cryptography and Network Security, pp. 507-525, 2012.

[6] A. Fiat and M. Naor, "Broadcast Encryption," Proc. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 480-491, 1993.

[7] V. 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 (CCS), pp. 89-98, 2006.

[8] D. Pointcheval and J. Stern, "Security Arguments for Digital Signatures and Blind Signatures," J. Cryptology, vol. 13, no. 3, pp. 361-396, 2000.

[9] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing," Proc. ACM Symp. Information, Computer and Comm. Security, pp. 282-292, 2010.

[10] D. Naor, M. Naor, and J.B. Lotspiech, "Revocation and Tracing Schemes for Stateless Receivers," Proc. Ann. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 41-62, 2001. [11] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," Proc. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 213-229, 2001.

[12] D. Boneh, X. Boyen, and H. Shacham, "Short Group Signature," Proc. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 41-55,2004.

[13] B. Sheng and Q. Li, "Verifiable PrivacyPreserving Range Query in Two-Tiered Sensor Networks," Proc. IEEE INFOCOM, pp. 46- 50, 2008.

[14] D. Boneh, B. Lynn, and H. Shacham, "Short Signature from the Weil Pairing," Proc. Int'l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology, pp. 514-532, 2001.

AUTHORS PROFILE:

A MADHUSUDHANA RAO is a student of Computer Science Engineering from G.V.R&S college of Engineering & Technology Presently pursuing M.Tech (CSE) from this college. He received MCA from ANU in the year of 2011.

O SRINIVAS is a Assistant Professor at G.V.R&S college of Engineering & Technology, Guntur. He received M.Tech in Computer science engineering from JNTUK. He gained 2 years of Experience on Teaching. He is a good Researcher in Programming Languages.