International Journal of Electrical Electronics & Computer Science Engineering
Special Issue - EEECOS 2014, ISSN : 2348 2273
Available Online at www.ijeecse.com

Secure Cloud Multi Owner Data Sharings

V.Rupesh Kumar,Y. C. Ashok Kumar, K.Siva Ramakrishna.
Department of Computer Science and Engineering, Andhra Loyola Institute of Engineering and Technology, Vijayawada.
ycashokkumar@gmail.com,vadugu.rupesh@gmail.com.

Abstract: ***File Sharing among cloud users although not uncommon and most prevalent it's evolution in terms of a secure shared group resource service provided by the cloud service provider(csp) is a technical challenge. First it should be economical, then it should support the existing architectures without major revamps. Considering the frequent activity scenarios like membership management, multi party file sharing in such a large scale cloud requires security policies of high standards in terms of efficiency and ease to use. So we intend to propose and develop a secure multi-owner data sharing scheme, for frequent and dynamic activities in the cloud. We further propose to use group signature schemes with on-the-fly broadcast ciphers that can help any cloud user securely share or revoke files with others with much less complexity in terms of storage overhead and encryption computation and communication cost. This advanced technical tweak which we term broadcast group key method (BGKM) modifies the functioning of secure data sharing in cloud and the results will back up our statement.***

Keywords: Cloud computing, Cloud API, Cloud Provisioning, Load Balancing, Meta clouds.

I. INTRODUCTION

Without the guarantee of identity privacy, cloud users may be unwilling to join in cloud computing systems because their real identities could be easily disclosed to cloud providers and attackers. It is a style of computing in which dynamically scalable and often virtualization resources are provided as a service over the internet. One of the most fundamental services offered by cloud providers is data storage. Maintaining the integrity of data plays a vital role in the establishment of trust between data subject and service provider. For example, a misbehaved staff can deceive others in the company by sharing false files without being traceable. What is more serious is that for saving money and storage space the service provider might neglect to keep or deliberately delete rarely accessed data files which belong to an ordinary client. Cloud computing is the long dreamed vision of computing as a utility, where data owners can remotely store their data in the cloud to enjoy on demand high-quality applications and services from a shared pool of configurable computing resources. Although envisioned as a promising service platform for the Internet, the new data storage paradigm in "Cloud" brings about many challenging design issues which have profound influence on the security and performance of the overall system. Identity privacy is one of the most significant obstacles for the wide deployment of cloud computing. However, it also poses a significant risk to the confidentiality of those stored files. Cloud computing is Internet ("cloud") based development and use of computer technology ("computing"). One of the biggest concerns with cloud data storage is that of data integrity verification at untrusted servers. Cloud computing is one of the greatest platform which provides storage of data in very lower cost and available for all time over the internet Cloud computing is Internet-based computing, whereby shared resources, software and information are provided to computers and devices on demand. Specifically, the cloud servers managed by cloud providers are not fully trusted by cloud users while the data files stored in the cloud may be sensitive and confidential, such as business plans. However, it also poses a significant risk to the confidentiality of those stored files. To preserve data privacy, a basic solution is to encrypt data files, and then upload the encrypted data into the cloud. Several trends are opening up the era of Cloud Computing, which is an Internet -based development and use of computer technology. Let us consider a practical data application. Cloud Computing means more than simply saving on IT implementation costs. Cloud offers enormous opportunity for new innovation, and even disruption of entire industries. By utilizing the cloud, the staffs can be completely released from the troublesome local data storage and maintenance. A company allows its staffs in the same group or department to store and share files in the cloud. In cloud computing, the cloud service providers (CSPs), such as Amazon, are able to deliver various services to cloud cloud users with the help of powerful datacenters. One of the most fundamental services offered by cloud providers is data storage. A company allows its staffs in the same group or department to store and share files in the cloud. By migrating the local data management systems into cloud servers, cloud users can enjoy high-quality services and save significant investments on their local infrastructures.

II. RELATED WORK

B. Wang, H. Li, B. Li troika [2] proposed Knox, a privacy-sustaining public auditing scheme for shared file data with large groups owning the data being present in the cloud. They consider and implement group signatures to compute verification hashes information on shared data, so that the Third party auditor(TPA) is able to audit the validity of the shared data, but at the same time cannot reveal the identity of the signer on each block. With the group admin's private key, the original uploaded/owner can efficiently add new members to the group with administrative access and discloses the identities of signers on all data

chunks. The efficiency of Knox is independent by the total number of users in the group. M. Armbrust, D.A. Patterson, A. Rabkin, I. Stoica, R.H. Katz, R. Griffith, A. Fox, A.D. Joseph, A. Konwinski, G. Lee and M. Zaharia [3] concluded that the data centers hardware and software infrastructure is what we will call typically a cloud. When a cloud with such remote resources is made available in an on the fly and pay-as-you-go paradigm to the general public, they call it a public cloud; the service being sold in question is termed as utility computing. The term private cloud refers to the same process being replicated within the internal data centers of a business or other organization, not made available to the general public, when they are huge enough to benefit from the advantages of cloud computing that we highlighted here. Thus most cloud computing file sharing services are the mostly the combination of SaaS and utility computing, but does not include or consider small or medium-sized data centers, even if these systems rely on virtualization for management of technical needs such as storage and processing. Consumers can be users or providers of utility computing or users or providers of SaaS. The focus is on the cloud providers, which have received more attention than security implementations. Key management and revocation is simple with minimal out -of-band communication. E. Goh, N. Modadugu, H. Shacham, D. Boneh [1] advocated the use of SiRiUS is a compelling factor in situations where cloud users have no control over the file server (such as Mediafire or the P2P file storage provided by Lime wire). They claimed that SiRiUS is the most advanced system that can secure an existing network file system without changing the file server or file system protocol. SiRiUS contains a novel method of performing file random access in a cryptographic file system without the use of a block server. Many File system platforms are supported by SiRiUS using hash tree constructions. Future upgrades to SiRiUS include huge group sharings using the NNL key revocation construction. S. Kamara, K. Lauter [4] considered the problem of building a secure cloud data storage services on top of a public cloud hardware infrastructure where the service provider is partially trusted by the customer. They describe, at a macro level, several feasible architectures that combine many recent advances and non-standard custom cryptographic primitives in order to achieve the security goals. Comparative study of the benefits of such architectures would provide a great deal of benefit to both customers and service providers and give a foresight of recent advances in cryptography driven security implementations specifically by and for the cloud storages. V. Goyal, B. Waters, O. Pandey, A. Sahai [6] developed a new custom cryptosystem for One-grained sharing of encrypted data which they call Key-Policy Attribute-Based Encryption (KP-ABE) scheme. In cryptosystem, ciphered contents are labeled with sets of attributes and private keys that are associated with access structures that control which ciphered contents a user is entitled to decrypt. They demonstrate the applicability of the security implementation to sharing of audit-log information and broadcast encryption procedures. Our implementation supports events delegation of private keys which consists Hierarchical Identity-Based Encryption (HIBE). The data owner uses a random key to encrypt a file, where the random key is further encrypted with a set of attributes using KP-ABE. Then, the group manager assigns an access structure and the corresponding secret key to authorized users, such that a user can only decrypt a cipher text if and only if the data file attributes satisfy the access structure. To achieve user revocation, the manager delegates tasks of data file reencryption and user secret key update to cloud servers. However, the single owner manner may hinder the implementation of applications with the scenario, where any member in a group should be allowed to store and share data files with others. A. Fiat, M. Naor [6] put forward a new theoretical measure for a more better qualitative and quantitative evaluations of data security schemes designed especially for broadcast transmissions. The idea is to allow a central broadcast station such as a storage server to broadcast secure transmissions to an arbitrary set of recipients through mailing services while minimizing key management(revokes) related transmissions. They consider several schemes that allow centers to share a secret to any subset of privileged users chosen by the owner out of a pool of coalitions of users not in the privileged set fails to learn the secret.

III. PROPOSED SCHEME

To achieve the secure reliable and scalable cloud sharing in Multi Owners Named Attributes (MONA), in this paper we are proposing the new framework for MONA implementations. We are further proposing the scheme for accessing and assessing control in cloud computing driven data sharing and extended the cipher text policy attribute set based encryption. MONA's security for data based on public key and master key implementations with the help of a Domain Authority Check is vital for the survival of this architecture. This method claims required efficiency, scalability and most importantly reliability.

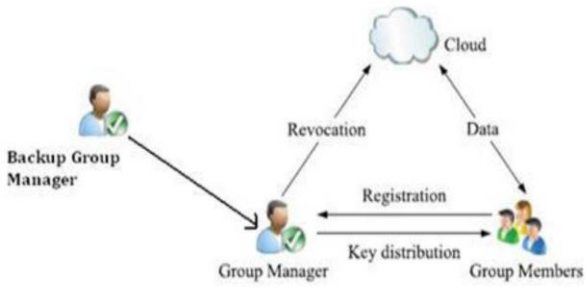

Fig. 1: MONA System Architecture

To overcome the disadvantage of prior systems of MONA, in the proposed system is better equipped to handle secure request claims.

Limitations of MONA are:

- Key generation based on file meta data is subject to prediction attacks or client collaboration attacks;
- File meta data based key generation incorporates high computational cost for cloud service provider.

Without utilizing public key cryptography and by allowing users to dynamically derive the symmetric keys at the time of encryption, we can address the above issues. We propose to implement a new key management scheme called broadcast group key management (BGKM). The idea of BGKM is to give some secrets to users based on the identity attributes they have and later allow them to derive actual symmetric keys based on their secrets and some public information.

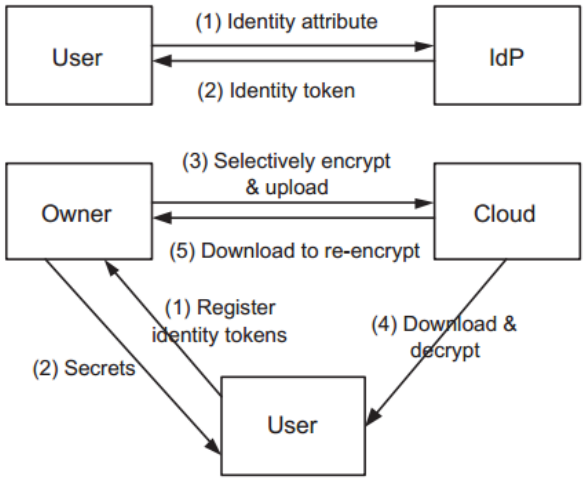

Fig. 2: BGKM System Architecture

A key advantage of the BGKM scheme is that adding users/revoking users or updating access control policies can be performed efficiently by updating only some public information and content sharing is much better with more number of unique dynamic keys.

Modified MONA Scheme Layout Description:

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

System Initialization

The group manager takes charge of system initialization as follows: Generating a bilinear map group system S=(q, G1, G2,e(.,.)).

The system parameters including (S, P, H, H0 ,H1 ,H2, U, V , W , Y , Z, f, f1, Enc()), where f is a one-way hash function: {0,1}* —> Z*q ; f1 is hash function: {0,1}* —> G1; and Enck() is a secure symmetric encryption algorithm with secret key k.

User Registration

For the registration of user i with identity IDi, the group manager randomly selects a number xi belong to Z*q and computes Ai, Bi as the following equation:

$$A_i = \frac{1}{\gamma + x_i}, P \in G_1$$

$$B_i = \frac{x_i}{\gamma + x_i}, G \in G_1$$

Then, the group manager adds (Ai, xi, IDi) into the group user list, which will be used in the traceability phase. After the registration, user i obtains a private key (xi, Ai, Bi), which will be used for group signature generation and the file decryption.

Revocation List:

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. The list is characterized by time stamp t1,t2,...tr. In the proposed system once the user time stamp over does not wait for the group manager to update the time stamp or revocation list here once the time over the user immediately send request for extra time for access the data to the cloud. Then the cloud will send that request to the group manager once the see it and give permission then the cloud will time to access the data but if the group manager did not give permission then the cloud will not give permission for access of the data.

File Generation:

To store and share a data file in the cloud, a group member performs the following operations: Getting the revocation list from the cloud. In this step, the member sends the group identity IDgroup as a request to the cloud. Then, the cloud responds the revocation list RL to the member. Verifying the validity of the received revocation list. First, checking whether the marked date is fresh. Second, verifying the contained signature sig(RL) by the equation e(W, f1 (RL)) = e(P, sig(RL)). If the revocation list is invalid, the data owner stops this scheme. Encrypting the data file M. Selecting a random number T and computing fT. The hash value will be used for data file deletion operation

File Deletion:

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). To delete a file IDdata, the group manager

computes a signature and sends the signature along with IDdata to the cloud.

File Access:

Without loss of generality, we set q=160 and the elements in G1 and G2 to be 161 and 1,024 bit, respectively. In addition, we assume the size of the data identity is 16 bits, which yield a group capacity of 2K data files. Similarly, the size of user and group identity are also set as 16 bits.

IV. CONCLUSION AND FUTUREWORK

In this paper, we proposed, designed and implemented a secure cloud data sharing scheme for multi owner dynamic groups in untrusted public cloud architecture. A cloud member is able to share files data with others in the group without compromising on security policies in the cloud. Additionally, it supports efficient member revocation and new member joining. More specially, efficient member revocation can be achieved through a public revocation list using a BGKM tree without updating the private keys of the remaining members, and new members can directly decrypt files stored in the cloud before their participation and they remain unaffected with the changes made to other members keys. Moreover, the storage overhead, length of the cryptographic signature and the running time of the signing algorithms are independent with the total number of group members. Cloud Data Migration happens to be an interesting future research.

V. REFERENCES

[1] 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.

[2] 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.

[3] 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.

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

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

[6] 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.