International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 12 Issue 2 –JANUARY 2015.

Mona Protocol for Secure Data Sharing in Cloud Computing

SHAIK BABA FAKRUDDIN[1] and B.SOWMYA[2]

[1]*PG Student, Dept. of CSE, Intell Engineering College, Affiliated to JNTUA, Andhra Pradesh, India*
[2]*Assistant Professor in Dept. of CSE, Intell Engineering College, Affiliated to JNTUA, Andhra Pradesh, India*

***Abstract*— Cloud Computing refers to both the applications delivered as services over the Internet and the hardware and systems software in the data centers that provide those services. Software stacks have improved interoperability among platforms, but the storage API's for Cloud Computing are still essentially proprietary. Cloud computing provides an economical and efficient solution for sharing group resource among cloud users. sharing data in a multi-owner manner while preserving data and identity privacy from an untrusted cloud is still a challenging issue, due to the frequent change of the membership. In this work, a secure multi owner data sharing scheme for dynamic groups is analyzed which leverages the group signatures and dynamic broadcast encryption techniques.**

Keywords: Dynamic groups, collusion secure, identity privacy, group user identity.

I. INTRODUCTION

Cloud Computing refers to both the applications delivered as services over the Internet as well as the hardware and systems software in the large datacenters that provide those services. The construction and operation of extremely large-scale, commodity-computer datacenters at low-cost locations was the key necessary enabler of Cloud Computing. Any application needs a model of computation, a model of storage, and a model of communication. The statistical multiplexing necessary to achieve elasticity and the illusion of infinite capacity requires each of these resources to be virtualized to hide the implementation of how they are multiplexed and shared. Enforcing an application structure of clean separation between a stateless computation tier and a stateful storage tier is required.

Security is one of the most often-cited objections to cloud computing where companies ask "who would trust their essential data 'out there' somewhere?" There are also requirements for audit ability which should not be over-looked.

Let us consider a practical data application. A company allows its staffs in the same group, domain or department to store and share files in the cloud. By utilizing the cloud, the concerned staffs can be completely released from the troublesome, unreliable local data storage and maintenance. It also poses a significant risk to the confidentiality of those stored files. Hence, the cloud user is responsible for application-level security. To preserve data privacy, a basic solution is to encrypt data files, and then upload the encrypted data into the cloud. At this point of time, identity privacy is one of the most significant challenges for the cloud service providers. The cloud provider is responsible for physical security, and likely for enforcing external firewall policies. Security for intermediate layers of the software stack is shared between the user and the operator, lower the level of abstraction exposed to the user, the more responsibility for security goes with it. Also unconditional identity privacy may incur the abuse of privacy. For example, within an organization, a misbehaved staff can deceive others in the company by sharing false files without being traceable. While cloud computing makes external-facing security easier, it does pose the new problem of internal-facing security. Cloud providers need to guard against theft or denial of service attacks by users. Users need to be protected against one another. Therefore, traceability, which enables the group manager to reveal the real identity of a user, is essential.

At the other hand, it is highly recommended that any member in a group should be able to fully enjoy the data storing and sharing services provided by the cloud, which is defined as the multiple-owner manner. Not only the group manager will be able to store and modify the data each user in the group is provided to fully enjoy the data storing and modification abilities for his/her part of the file. Also the properties for dynamic groups say new staff participation; current staff revocation in the company should also be taken into consideration.

II. EXISTING SYSTEM

One of the most fundamental services offered by a cloud is its virtualized data storage. By this any organisation can be released from the trouble some local data storage and maintenance. At the same time , the cloud storage offered by the cloud storage servers are questioned for the factors of

integrity, authenticity, security for the uploaded data. At the same time, group of employees are normally dynamic in practice.

In the existing schemes for data sharing on untrusted servers, the data owners say clients or organisations store the encrypted data content on the third party storage service vendors and distribute the corresponding decryption keys only to authorized users. By this unauthorized users cannot learn the data content but do not have the knowledge of decryption keys. Also the complexity increases as the number of users or data owners increases. Hence the concept of group of users is supported to reduce the complexity. By defining a single attribute for the group identification, based on an attribute based encryption technique, any member in the group can share the data with others.

Drawbacks of Existing System

The following are the drawbacks of the existing approach:

1. Does not effectively support dynamic groups.
2. Any member in the group is not effectively allowed to share the data or utilize the cloud resources.
3. The computational complexity increases as the number of users increases.
4. The overhead of encryption increases as the number of users increases.

III. Proposed System

In the proposed approach for multi-owner data sharing, any user in the group can securely share the data with others through the untrusted storage servers. In this scheme, the group owner has the real identities of the group members which can be revealed when an employee tries to deceive with the name of other employee.

The dynamic groups are supported using NNL scheme. When a new user joins a group, the private key defined for each user will be updated in the NNL scheme. The data owner encrypts a blocks of content with unique and symmetric content keys, which are further encrypted with a master public key.

In this a group manager will be responsible for storing the parameters for user registration, user revocation, revealing the real identity of the user in case of disputes. In this case, a group manager is assumed to be trusted by all other parties.

Group members are those set of registered users who will store their private data into the cloud server and can share the same with others in the group. In this case of group membership, the data has to be dynamically updated for the cases of new staff participation or any staff resignation in the company.

In the proposed scheme, the group encryption and dynamic broadcast techniques are combined. Group signature scheme enables users to anonymously access the cloud resources whereas the dynamic broadcast technique allows data owners to securely share the data with the old users as well as the newly joined users.

This work describes the scheme for user registration, user revocation, file generation, file deletion, file access and traceability.

Scheme Description

System Initialization

The group manager invokes the system initialization process as given below:

ID_{group}	A_1	x_1	t_1	P_1			
	A_2	x_2	t_2	P_2			
	.	.	.	.			
	A_r	x_r	t_r	P_r	Z_r	t_{RL}	$sig(RL)$

User Registration

For a new user registration i with identity IDi, the group manager randomly selects a number $x_i \in Z_q^*$ the equation is given as below:

$$\begin{cases} A_i = \dfrac{1}{\gamma + x_i} \cdot P \in G_1 \\ B_i = \dfrac{x_i}{\gamma + x_i} \cdot G \in G_1 . \end{cases}$$

Then the group manger adds (Ai,xi, IDi) into the group user list which will be used later for the group traceability.

User Revocation

In this group members can encrypt their data files and ensure the confidentiality against the revoked users. The group manager updates the revocation list each day even there is no revocation by the user so that the freshness of the data can be maintained. The revocation list is bounded by a signature sig (RL) to declare its validity.

File Generation

Once a user from the revocation list places the request for uploading the file into the cloud, it checks for the genuinely of the user from the list. If the user id is present in the freshly generated list, it sends a response for file upload. Otherwise it prevents the user from uploading. For the file to be uploaded, a random number λ is generated for which the function f g(λ) is generated.

File Deletion

For the file to be deleted which is stored in the cloud can be deleted by either the group manager or the data owner. To

delete a file ID data, the group manager computes a signature γf1 (IDdata) and sends the signature along with IDdata to the cloud. The cloud will delete the file if the equation e(γf1(IDdata ,P)=e(W, γf1(IDdata)) holds.

ADVANTAGES OF PROPOSED SYSTEM

1. As user traceability is facilitated, group manager can reveal the identity of the signature originator when a dispute occurs.
2. Dynamic group properties are supported.
3. Reduces the computation overhead involved in encrypting the files and cipher text size.
4. Independent of revocated users.

IV. CONCLUSION

The proposed secure data sharing scheme supports dynamic groups in an untrusted cloud. At the same time, a group user is able to share data with others in the cloud without revealing the actual identity to the cloud. A user revocation list can be obtained without containing the privacy keys of the remaining users. A new user can participate in learning the data content without contacting the group owner. The storage and encryption overheads for the computation remain constant as the number of users increases.

TABLE 2 COMPUTATION COST OF THE CLOUD

Request	The number of revoked users		
	0	50	100
File generation (100 MB)	0.065	0.154	0.271
File generation (10 MB)	0.045	0.125	0.226
File access (100 MB)	0.045	0.150	0.237
File access (10 MB)	0.045	0.151	0.240
File deletion (100 MB)	0.041	0.153	0.240
File deletion (10 MB)	0.042	0.156	0.238

REFERENCES

[1] Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud Xuefeng Liu, Yuqing Zhang, Member, IEEE, Boyang Wang, and Jingbo Yan

[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] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing," Proc. IEEE INFOCOM, pp. 534-542, 2010.

[5] The Pairing-Based Cryptography Library (PBC), http://crypto.stanford.edu/pbc/howto.html, 2013.

[6] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," Proc. IEEE INFOCOM, pp. 525-533, 2010.