GLOBAL JOURNAL OF ENGINEERING, DESIGN & TECHNOLOGY
(Published By: Global Institute for Research & Education)
www.gifre.org

SUODY-Preserving Privacy in Sharing Data with Multi-Vendor for Dynamic Groups

T.Vijayalakshmi[1], Balika J Chelliah[2] & R. Jegadeesan[3]
[1]M.Tech Student, Department of Computer Science and Engineering, S.R.M. University Chennai.
[2]Asst.Professor (OG), S.R.M. University Chennai, [3]Ph.D Research Scholar, Anna university-Chennai (india)

Abstract

Cloud computing has a character of low manintance which will provide an effective solution to share resource among group of users in the cloud. Major problem in public cloud is how to share data's and documents based on fine grained access control policies, due to frequent change of the membership data sharing in dynamic groups to preserve data and identity privacy from a cloud which is a untrusted one is still a challenging issue. Encrypting the Document with different key such as Attribute Based Encryption and Proxy Re-Encryption have many draw backs .These approaches is efficient to handle user registration and revocation. It requires maintaining many encrypted copies of the single document, which incurs high computational costs. In this paper we propose a privacy preserved multi owner data sharing scheme, named Suody.By taking maximum advantage of group signature to construct homomorphic authenticators, signed receipts and dynamic broadcast encryption techniques, a user in the cloud can share the data with others using withheld authorship. At the same time overhead in the storage and computation cost for encryption of our scheme for the number of users revoked are independent .Additionally, we also analyze schemes security with rigorous proofs.

***Index Keywords**: Cloud computing, data sharing, dynamic groups.*

I. INTRODUCTION

Cloud Computing is a type of computing that concentrates more on sharing resources instead of having a local server or device to handle personal application .Cloud Computing s new emerging technology for IT sector because it provides Scalable services with minimum operational Cost. Most famous cloud computing providers are Amazon, Google, Microsoft, Yahoo and Sales force are able to provide deliver various services to the cloud users with the help of powerful data centers . In general cloud computing involves delivering services over the internet. The Services are categorized as Infrastructure, Software, Platform, Network. **Infrastructure - In** this service the Cloud Service provider supplies the resources on demand basis from their Data centers. The resources are Software bundles, Raw, Virtual local area networks, load balancers, file based storages. **Software -** In this Service Users are provided access to software applications and Databases. This is also called as On Demand Software services. **Platform –** In this the Cloud Service provider a computing platform to the program developers. Computing platform includes operating system, programming language execution environment, database, and web server. **Network - the** Cloud Service provider provides **network**/transport connectivity services and/or inter-cloud network connectivity services to the users.

There are two types of cloud Private and Public cloud. By using public cloud any user can buy services over the internet. A private cloud is a network with a data center that provides required hosted services to a limited number of users. A service provider uses public cloud resources to create their private cloud; the result is a virtual private cloud.The users of Cloud are not the owners of the resources. The cloud providers reduces the management overhead of the client as the users do not own the resources.

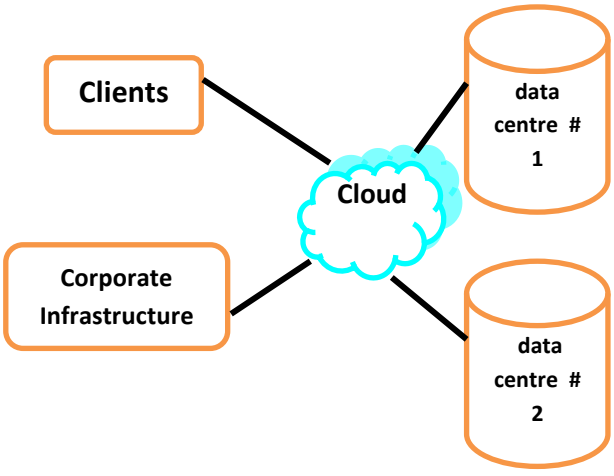


Fig. 1.1 Cloud Architecture

1.2 Cloud Deployment Models:

Private Cloud : A Single private organization owns this infrastructure.

Public Cloud : Open for all , that available in public networks. Need some cloud security considerations?

Community cloud : This is Owned by several organization to share the resourses and it is managed by a thir dparty.

Hybrid cloud : Two or more Private, Public and Community clouds combine to form a hybrid cloud.

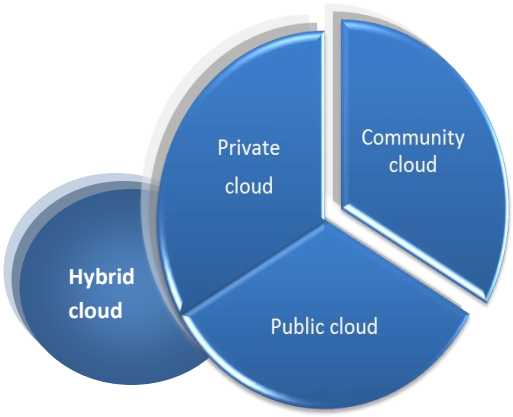


Fig. 1.2 Cloud Models

One of the important services offered by cloud providers is data storage. For Example in a company the staffs can store and share the data in the cloud as they were released from local data storage and maintenance. It poses a risk of Confidentiality of those file. In fact, data privacy and security issues have been major concerns for many organizations utilizing such services. Data often encode sensitive information and should be protected. Commonly adopted approach is encryption to protect the confidentiality of the data. Basic solution preserve data privacy is to encrypt data files, and then upload the encrypted data into the cloud [1]. Due to the following challenging issues It is very tough task to design a secure data sharing scheme for groups in the cloud. First, identity privacy without any guarantee the users will not join the group as their secret information can be easily known to the CSPs and attackers. Second, any member in the group should be able to get the full benefits of data storing and sharing services provided by the cloud, which is defined as the multi -owner scheme, as compared to single-owner scheme [2], Third, new member participation and current member revocation in a group It is extremely difficult for a new granted users to contact with data owners who is not known, and obtain the respective decryption keys. A systematic membership re-vocation mechanism without updating of the secret keys of the remaining users minimize the complexity of key management , signed receipt is collected after every member revocation in the group it minimizes the multiple copies of encrypted file and also reduces computation cost.

2. RELATED WORKS

In [3], proposed a scalable and fine-grained data access control system in cloud based on the KP-ABE technique. The data owner encrypts the file with a random key and futher the random key is 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 ciphertext 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 is supported in this implementation.

In [4],proposed encrypted storage model which that enables file sharing on untrusted servers ina secured manner , named Plutus. By dividing files into group of files and encrypting them with a unique file-block key, the data owner can share with others by using the corresponding lockbox key, where the lockbox key is used to encrypt the file-block keys. However, it results in heavy key distribution overhead in the case of large-scale file sharing and the file-block key needs to be updated for a user revocation.

In [5], files stored on the untrusted server include two parts: file metadata and file data. The file metadata includes access control information such as a series of encrypted key blocks, each of which is encrypted under the public key of authorized users. The size of the file metadata is proportional to the number of authorized users. The user revocation in the scheme is not possible for large-scale sharing, Hence the file metadata needs to be updated.

In [10], the extension version of [5], the NNL construction is used for key revocation. When a new user joins the group, the private key of each user in an NNL system needs to be recomputed, which limits the application for dynamic groups. The computation overhead of encryption linearly increases with the sharing scale.

In [6] leveraged proxy re encryptions is used for secure distributed storage. Specifically, the data owner encrypts content using unique and symmetric content keys, which are further encrypted under a master public key. For access control, the server uses proxy cryptography to directly reencrypt the appropriate content key(s) from the master public key to a granted user's public key. Unfortunately, a collusion attack raises which enables to learn the decryption keys of all the encrypted blocks.

In [7], proposed a secure provenance scheme, which supports group signatures and cipher text-policy attribute-based encryption techniques. This system has set with a single attribute. Each user obtains two keys after the registration: a group signature key and an attribute key. Thus, any user is able to encrypt a data file using attribute-based encryption and others in the group can decrypt the encrypted data using their attribute keys. However, user revocation is not supported in their scheme.

From the above analysis, it is observed that how to securely share data files in a multiple-owner manner for dynamic groups while preserving identity privacy from an untrusted cloud remains to be a challenging issue. In this paper, we propose a novel *Suody* protocol for secure data sharing in cloud computing. Compared with the existing works, *Suody* offers unique features as follows:

1.Any user in the group can store and share data files with others by the cloud.
2.The Size and complexity of the encrypted cipher text are independent.
3.With our updating the private keys of the remaining users revocation process can be achieved.
4.Direct decryption can be achieved by the new users on the files in the cloud before his participation.
5.The Group manager and the group owner will be selected from the members by using Leader Polling algorithm.

3. PROPOSED SCHEME

To solve the above challenge, we propose *Soudy*, a secure multi-owner data sharing scheme for dynamic groups in the cloud. The main contributions of this paper include:

1. We propose a secure sharing scheme for multi-owner. It implies that any user in the group can securely share data with others by the untrusted cloud.
2. Our scheme will support dynamic groups efficiently. Specifically, decryption can be done directly without contacting the data owner.
3. A Novel revocation list which contains the secrect keys without updating is used for user revocation. The size and computation overhead of encryption remains constant and independent with the number of revoked users.
4. The real identities of data owners can be revealed by the group manager when disputes occur.
5. We provide a leader polling algorithm to elect the group manager and group owner.

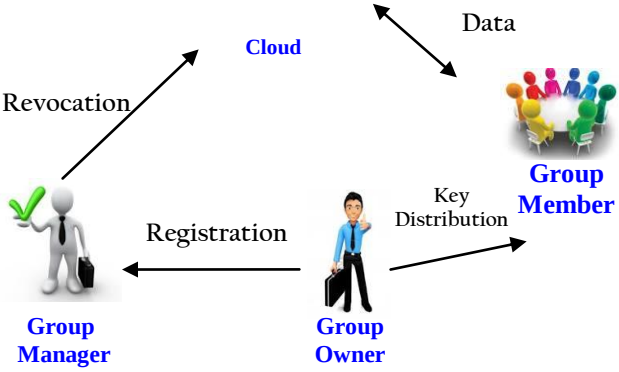


Fig. 3.1 Cloud Architecture

3.1 Components

Cloud is operated by CSPs and provides priced abundant storage services. Similar to [3] we assume that the cloud will not delete or modify the data due to the protection of data auditing schemes[17][18]

Group manager will takes the charge of Access control,system parameter generation,,user revocation..For example the group manager is acted by administrator of the company.Hence he is fully a trusted party.

Group owner is the one selected from the group members.He will take the charges of user registration,distributing updated revocation,assigning ID,traceablity.

Group Memebrs are a set of registered users that will store the private data into the cloud server and share them with others in the group.They are responsible for selecting the group owner as well the group manager if nedded.For example the staff will play this role.The membership is dynamic so that any staff can resign and new employee can participate in the company.

3.2 Design goals

Access Contro l: The group members are able to use the cloud resource for data operations .unauthorized users cannot access the cloud resource at any time, and revoked users will be incapable of using the cloud once again they are revoked.

Data Confidentiality: An important and challenging issue for data confidentiality is to maintain its availability for dynamic groups. New users should decrypt the data stored in the cloud before their participation, and revoked users is unable to decrypt the data moved into the cloud after the revocation.

Anonymity and Traceability: Anonymity guarantees that group members can access the cloud without revealing the real identity it enables effective protection for user identity.

Efficiency:. Any group member can store and share data files with others in the group by the cloud. User revocation can be achieved without involving the remaining users.

Data sharing: To achieve privacy preserved data sharing for dynamic groups in the cloud, the scheme combines the group signature, signed receipt and dynamic broadcast encryption techniques.

3.3 Group Signature

A Group signature scheme is a method for allowing a member of a group to anonymously sign a message on behalf of the group which introduced by David Chaum and Eugene van Heyst in 1991. For example, a group signature scheme could be used by an employee of a large company where it is sufficient for a verifier to know a message was signed by an employee, but not which particular employee signed it. Essential to a group signature scheme is a group owner and group manager, who is in charge of adding group members and has the ability to reveal the original signer in the event of disputes. The basic requirements are SoundnessandCompleteness,Unforgeable,Traceability,Unlinkability,NoFraming,Unforgeable tracing verification.

3.4 Dynamic Broad cast Algorithm

Broadcast encryption [16] enables a broadcaster to transmit encrypted data to a set of users so that only a privileged subset of users can decrypt the data. Besides the above characteristics, dynamic broadcast encryption also allows the group manager to dynamically include new members while preserving previously ccomputed information which is a user decryption key need ot to be updated or recomputed,the structure and size of the cipher text are constant.the formal definition and the construction of dynamic broad cast algorithm are based on bilinear pairing techniques[14].

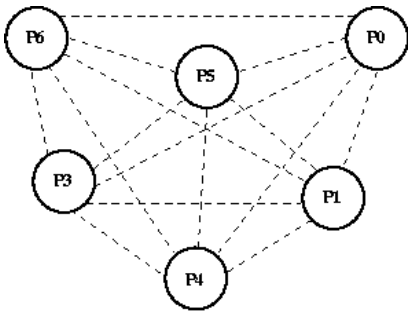
3.5 Leader polling Algorithm

The **Leader Polling algorithm** is a method for dynamically electing a group owner by using the unique member ID number. The member with the highest unique member ID number is selected as the group owner.

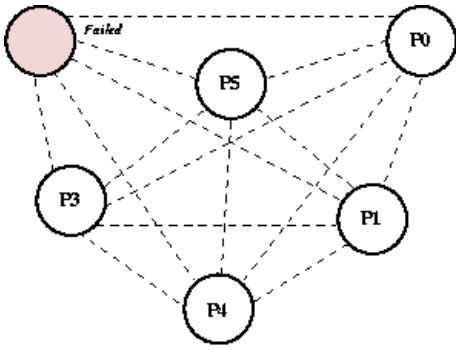
When a group member G determines that the current Owner is down because of message timeouts or failure of the coordinator it performs the following sequence of actions:

1. G sends an election message (inquiry) to all other members with higher Member IDs, expecting an "I am alive" response from them if they are alive.
2. If G doesn't receive any reply from the member with a higher member ID than it, it wins the election and broadcasts victory.
3. If G receives a message from the member with a higher ID, G waits a certain amount of time for any process with a higher ID to broadcast itself as the leader. If it does not receive this message in time, it re-broadcasts the election message.
4. If G gets an election message (inquiry) from another process with a lower ID it sends an "I am alive" message back and starts new elections.

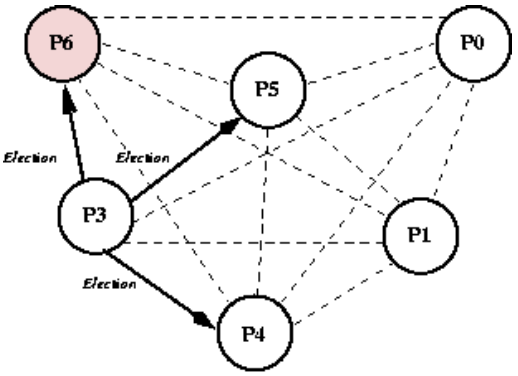
We start with 6 processes,
all directly connected to each other.
Process 6 is the leader,
as it has the highest number.



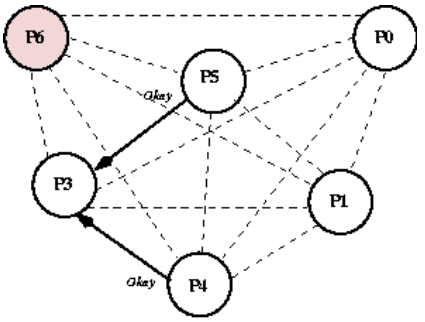
Step 1:Process 6 fails.



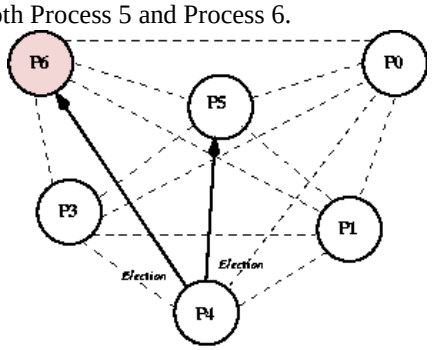
5. Step 2:sProcess 3 notices that Process 6 does not respond So it starts an election, notifying those processes with ids greater than 3.



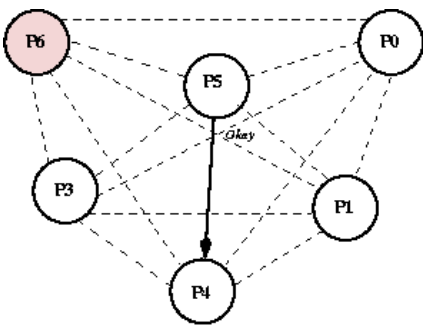
Step 3 :Both Process 4 and Process 5 respond, telling Process 3 that they'll take over from here.



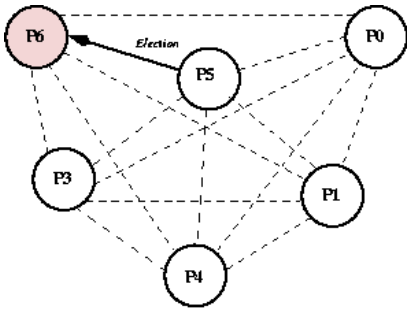
Step 4:Process 4 sends election messages to both Process 5 and Process 6.



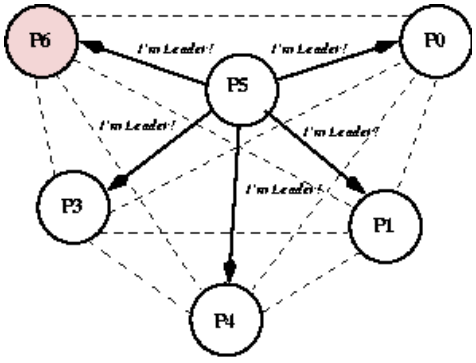
Step 5: Only Process 5 answers and takes over the election.



Step 6:Process 5 sends out only one election messag to Process 6.



Step 7 :When Process 6 does not respond Process 5 declares itself the winner.



4. CONCLUSION

In this paper, we design a secure data sharing scheme, Suody, for dynamic groups in an untrusted cloud. In Suody, a user can share data with others in the group without revealing identity privacy to the cloud. Additionally, Suody supports efficient user revocation and new user registration. More specially, efficient user revocation can be achieved without updating the private keys of the remaining users using the revocation list, and decryption can be done directly on the stored files in the server before participation. Moreover, the storage overhead and the encryption computation cost are constant. Our scheme satisfies the desired security requirements and guarantees efficiency as well.

5. REFERENCES

[1] 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.

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

[3] 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.

[4] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu,"Plutus: Scalable Secure File Sharing on Untrusted Storage," Proc. USENIX Conf. File and Storage Technologies, pp. 29-42, 2003.

[5] 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.

[6] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage," Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 29-43, 2005.

[7] 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.

[8] B. Waters, "Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization," Proc. Int'l Conf. Practice and Theory in Public Key Cryptography Conf. Public Key Cryptography, http://eprint.iacr.org/2008/290.pdf, 2008.

[9] 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.

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

[12] 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.

[13] 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.

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

[15] 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.