International Journal of scientific research and management (IJSRM)
||Volume||2||Issue||4 ||Pages|| 719-723||2014||
Website: www.ijsrm.in ISSN (e): 2321-3418

SECURE DATA SHARING FOR DYNAMIC GROUPS IN THE CLOUD USING BROADCASTING ENCRYPTION TECHNIQUES

S.Senthil Kumar[1] Christo Paul.E[2] Nilutpal Bose[3]

[1]PG Scholar, Computer Science and Engineering, Srinivasan Engineering College
senthilkumar.au1987@gmail.com

[2]PG Scholar, Computer Science and Engineering, Srinivasan Engineering College
echristopaul@gmail.com

[3]Assistant Professor, Computer Science and Engineering, Srinivasan Engineering College

***Abstract*-Cloud computing provides an economical and efficient solution for sharing group resource among cloud users. General sharing schemes protect data confidentiality, and also limit the functionality of the storage system because some operations are supported over encrypted data .Now a day's sharing doesn't provide any security. The new proposed scheme is to provide secure multi owner data sharing scheme for dynamic groups in the cloud. Also provide a group signature and dynamic broadcast encryption techniques, any cloud user can anonymously sharing data with others. Meanwhile, to reduce the storage overhead and encryption computation cost. Then cloud service provider blocking the users who are entering wrong authentication keys more than some times.**

***Index Terms*- Cloud computing, data sharing, privacy-preserving, access control, dynamic groups**

I.INTRODUCTION

Cloud computing is recognized as an alternative to traditional information technology due to its intrinsic resource-sharing and low-maintenance characteristics. In the cloud computing, the cloud service providers are able to deliver various services to cloud users with the help of powerful datacenters. By migrating local data management systems into cloud servers, users can enjoy higher quality services and save significant investments on their local infrastructures. One of the most important services offered by cloud providers is data storage. Let us consider the following example. A company allows its staffs in the same group or department to store and share files in the cloud. By utilizing the cloud, a staff can be completely released from the troublesome local data storage and maintenance. It also poses a significant risk to the confidentiality of those stored files. Specifically, cloud servers managed by cloud providers are not fully trusted by users while the data files stored in cloud will 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. Designing an efficient and secure data sharing scheme for groups in the cloud is not an easy way due to the following challenging issues.

First, identity privacy is one of the most significant obstacles for the wide usage of cloud computing. Without the guarantee of identity privacy, users may be unwilling to join in cloud computing systems because their real identities could be easily disclosed to cloud providers and attackers. And on another way, unconditional identity privacy may incur the abuse of privacy. For example, misbehaved staff can deceive others in the company by sharing false files without being traceable. Therefore, traceability, which enables the group manager to reveal the real identity of a user, is also highly desirable.

Second, it is highly recommended that any member in a group should be able to fully enjoy the sharing and data storing services provided by the cloud. The multiple-owner manner the single-owner where only the group manager can store and modify data in the cloud, the multiple-owner

manner is more flexible in practical applications. More concretely, each user in the group is able to not only read data, but also modify his/her part of data in the entire data file shared by the company.

Third, groups are normally dynamic in practice, e.g., new staff participation and current employee revocation in a company. The changes of membership make secure data sharing extremely difficult. On one hand, the anonymous system challenges new granted users to learn the content of data files stored before their participation, because it is impossible for new granted users to contact with anonymous data owners, and obtain the corresponding decryption keys. On the other hand, an efficient membership revocation mechanism without updating the secret keys of the remaining users is also desired to minimize the complexity of key management. Several security schemes for data sharing on untrusted servers have been proposed. In these approaches, data owners store the encrypted data files in untrusted Storage and distribute the corresponding decryption keys only to authorized users. Thus, unauthorized users as well as storage servers cannot learn the content of the data files because they have no knowledge

of the decryption keys. To solve the challenges presented above, the proposed paper is a secure multi-owner data sharing scheme for dynamic groups in the cloud. The main contributions of this paper include:

1. The proposed scheme is to a secure multi-owner data sharing. It implies that any user in the group can securely share data with others by the untrusted cloud.

2. The proposed scheme is able to support dynamic groups in the organization. Specifically, new users directly data files upload or download data files before their participation without contacting with data owners. User removing can be easily achieved through a novel revocation list without updating the passwords of the remaining users. The size and computation overhead of encryption are constant and independent with the number of revoked users.

3. To provide secure and privacy-preserving access control to users, which guarantees any member in a group to anonymously utilize the cloud resource .Moreover, the real identities of data owners can be revealed by the group manager when disputes occur.

4. It provides rigorous security analysis, and performs extensive simulations to demonstrate the efficiency of the scheme in terms of storage and computation overhead.

II RELATED WORK

The cloud, the group members can be completely released from the troublesome local data storage and maintenance. It also poses a significant risk to the confidentiality of those stored files.

First, identity privacy is one of the most significant obstacles for the wide deployment of cloud computing. Traceability, which enables the group manager (e.g., a company manager) to reveal the real identity of a user, is also highly desirable.

Second, 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. Compared with the single-owner manner, where only the group manager can store and modify data in the cloud, the multiple-owner manner is more flexible in practical applications. More concretely, each user in the group is able to not only read data, but also modify his/ her part of data in the entire data file shared by the company.

Cloud Computing, the long-held dream of computing as a utility, has the potential to transform a large part of the IT industry, making software even more attractive as a service and shaping the way IT hardware is designed and purchased. Developers with innovative ideas for new Internet services no longer require the large capital outlays in hardware to deploy their service or the human expense to operate it. They need not be concerned about over-provisioning for a service whose popularity does not meet their predictions, thus wasting costly resources, or under-provisioning for one that becomes wildly popular, thus missing potential customers and revenue. Moreover, companies with large batch-oriented tasks can get results as quickly as their programs can scale, since using 1000 servers for one hour costs no more than using one server for 1000 hours. This elasticity of resources, without paying a premium for large scale, is unprecedented in the history of IT.The goal of this paper to reduce that confusion by clarifying terms, providing simple figures to quantify comparisons between of cloud and conventional Computing, and identifying the top technical and non-technical obstacles and opportunities of Cloud Computing.

The problem of a Center transmitting data to a large group of receivers so that only a predefined subset is able to decrypt the data is at the heart of a growing number of applications. Among them are pay-TV applications, multicast communication, secure distribution of copyright-protected material (e.g. music) and audio streaming. The area of Broadcast Encryption deals with methods to efficiently broadcast information to a dynamically changing group of users who are allowed to receive the data. It is often convenient to think of it as a Revocation Scheme, which addresses the case where some subset of the users are excluded receiving the information. In such scenarios it is also desirable to have a Tracing Mechanism, which enables the efficient tracing of leakage, specifically, the source of keys used by illegal devices, such as pirate decoders or clones.

Scientific computing often requires the availability of a massive number of computers for performing large scale experiments. Traditionally, these needs have been addressed by using high-performance computing solutions and installed facilities such as clusters and super computers, which are difficult to setup, maintain, and operate. Cloud computing provides scientists with a completely new model of utilizing the computing infrastructure. Compute resources, storage resources, as well as applications, can be dynamically provisioned (and integrated within the existing infrastructure) on a pay per use basis. These resources can be released when they are no more needed. Such services are often offered within the context of a Service Level Agreement (SLA), which ensure the desired Quality of Service (QoS). Aneka, and enterprise Cloud computing solution, harnesses the power of compute resources by relying on private and public Clouds and delivers to users the desired QoS. Different solutions are available to move from the traditional science Grids and embrace the Cloud computing paradigm. Some vendors, such as Amazon Web Services and VMware base their offering on hardware level virtualization and provide bare compute and storage resources on demand. Google AppEngine and Microsoft Azure are more focused on application level virtualization by enforcing a specific application model that leverage their large infrastructure and scale up and down on demand. Other solutions provide end users with a platform for developing Cloud computing applications that can rely on, or compose, some of the existing solutions thus providing a better Quality of Service to the end user. Aneka is a Cloud computing platform for developing applications that can scale on demand by harnessing the CPU cycles of virtual resources, desktop PCs, and clusters. Its support for multiple programming models provides scientists with different options for expressing the logic of their applications: bag of tasks, distributed threads, dataflow, or Map Reduce. Its service oriented architecture provides users with an extremely customizable infrastructure that can meet the

desired Quality of Service for applications. The adoption of Cloud computing as a technology and a paradigm for the new era of computing has definitely become popular and appealing within the enterprise and service providers. It has also widely spread among end users, which more and more host their personal data to the cloud. For what concerns scientific computing, this trend is still at an early stage.

III.OUR SYSTEM AND ASSUMPTIONS

System components and relations. To solve the challenges presented above, a secure multi-owner data sharing scheme for dynamic groups in the cloud. The main contributions of this paper include:

This project proposes a secure multi-owner data sharing scheme. It implies that any user in the group can securely share data with others by the un-trusted cloud. Proposed scheme is able to support dynamic groups efficiently. Specifically, new granted users can directly decrypt data files uploaded before their participation without contacting with data owners.

User revocation can be easily achieved through a novel revocation list without updating the secret keys of the remaining users. The size and computation overhead of encryption are constant and independent with the number of revoked users.

Provide secure and privacy-preserving access control to users, which guarantee any member in a group to anonymously utilize the cloud resource.

Provide rigorous security analysis, and perform extensive to demonstrate the efficiency of scheme in terms of storage and computation overhead.

To achieve secure data sharing for dynamic groups in the cloud, to get the expected outcome to combine the group signature and dynamic broadcast encryption techniques. Particularly, the group signature scheme enables users to anonymously use the cloud resources, and the dynamic b This Technique allows data owners to securely share their data files with others including new joining users. each user has to compute revocation parameters to protect the confidentiality from the revoked users in the dynamic broadcast encryption scheme, which results in that both the computation overhead of the encryption and the size of the cipher text increase with the number of revoked users. Thus, the heavy overhead and large cipher text size may hinder the adoption of the broadcast encryption scheme to capacity-limited users. To tackle this challenging issue. The group manager compute the revocation parameters and make the result public available by migrating them into the cloud. Such a design can significantly reduce the computation overhead of users to encrypt files and the cipher text size. Specially, the computation overhead of users for encryption operations and the cipher text size is constant and independent of the revocation users.

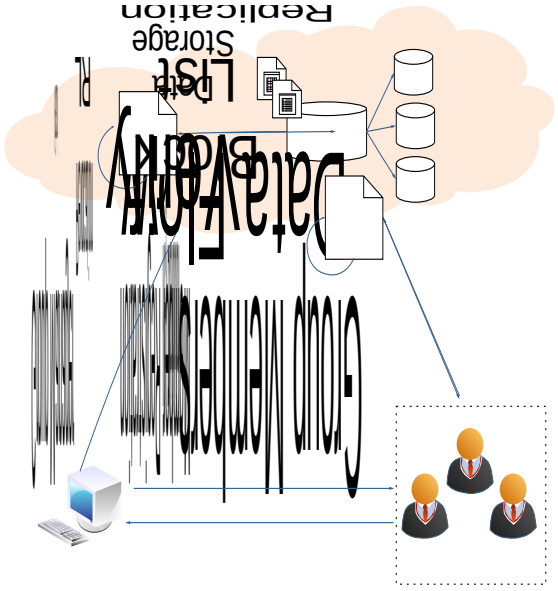

Fig 1.Architecture Diagram For Data Sharing

We consider a cloud computing architecture by combining with an example that a company uses a cloud to enable its staffs in the same group or department to share files. The system model consists of three different entities: the cloud, a group manager (i.e., the company manager), and a large number of group members (i.e., the staffs) as illustrated in Fig. 1.

Cloud is operated by CSPs and provides priced abundant storage services. However, the cloud is not fully trusted by users since the CSPs are very likely to be outside of the cloud users' trusted domain. 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 takes charge of system parameters generation, user registration, user revocation, and revealing the real identity of a dispute data owner. In the given example, the group manager is acted by the administrator of the company. Therefore, we assume that the group manager is fully trusted by the other parties.

Group members are a set of registered users that will store their private data into the cloud server and share them with others in the group. In our example, the staffs play the role of group members. Note that, the group membership is dynamically changed, due to the staff resignation and new employee participation in the company.

IV.SYSTEM PRELIMINARIES

Bilinear Mapping Algorithm. An additive cyclic group and a multiplicative cyclic group of the same prime order q. Let G1 and G2 be an additive cyclic group and a

multiplicative cyclic group of the same prime order q, respectively. Let e: G1 ×G1 ->G2 denote a bilinear map constructed with the following properties of Bilinear, No degenerate and Computable.

Diffie Hellman Algorithm. This algorithm used for encrypts the data and forward to cloud server and cloud Users also.This algorithm very useful in secure storage and secure forwarding process successfully created.

Dynamic Broadcasting Encryption. Broadcast encryption enables a broadcaster to transmit encrypted data to a set of users so that only a privileged subset of users can decrypt the data.

Revocation List. The revocation list is bounded by a signature sig (RL) to declare its validity. The signature is generated by the group manager with the BLS signature algorithm, i.e., sig (RL) = f1 (RL). Finally, the group manager migrate the revocation list into the cloud for public usage

V.EXPERIMENTAL EVALUATION

In this section we experimentally evaluate the computation overhead the proposed scheme brings to a cloud storage system that has been dealing with static data with only confidentiality requirement.

The experiments are conducted using .NET on a system with an Intel(R) Xeon (R) 2-GHz processor and 3GB RAM running Windows XP. Algorithms (hashing, broadcast encryption, digital signatures, etc.) are implemented using MIRACL library version 5.5.4. For a 128-bit security level, bENC uses an elliptic curve with a 256-bit group order. In the experiments, we utilize SHA-256, 256-bit BLS signature, and Barreto-Naehrig (BN) [50] curve defined over prime field GF(p) with p = 256 bits and embedding degree = 12 (the BN curve with these parameters is provided by the MIRACL library). To evaluate the computation overhead on the owner side due to dynamic operations, we perform 100 different block operations from which 50% are executed following revocations (this percent is higher than an average value in practical applications).

Scalability (i.e., how the system performs when more users are added) is an important feature of cloud storage systems. The access control of the proposed scheme depends on the square root of the total number of system users.

It is easily observed that the computation cost in Mona is irrelevant to the number of revoked users. On the contrary, the computation cost increases with the number of revoked users in ODBE. The reason is that the parameters P and Q can be obtained from the revocation list without sacrificing the security in Mona, while several time-consuming operations including point multiplications in G1 and exponentiations in G2 have to be performed by clients to compute the parameters in ODBE. We can find out that sharing a 10-Mbyte file and a 100-Mbyte one, cost a client about 0.2 and 1.4 seconds in our scheme, respectively, which implies that the symmetrical encryption operation domains the computation cost when the file is large.

The computation cost of clients for file access operation with the size of 10 and 100 Mbytes . The computation cost in Mona increases with the number of revoked users, as clients require performing Algorithms 3 and 4 to compute the parameter and check whether the data owner is a revoked user. Besides the above operations, P1; P2:::; Pr need to be computed by clients in ODBE. Therefore, Mona is still superior to ODBE in terms of computation cost. Similar to the data generation operation, the total computation cost is mainly determined by the symmetrical decryption operation if the accessed file is large, which can be verified. In addition, the file deletion for clients is about 0.075 seconds, because it only costs a group signature on a message.

To evaluate the performance of the cloud in Mona, we test its computation cost to respond various client operation requests including file generation, file access, and file deletion. Assuming the sizes of requested files are 100 and 10 MB, the test results are given in Table 3. It can be seen that the computation cost of the cloud is deemed acceptable, even when the number of revoked users is large. This is because the cloud only involves group signature and revocation verifications to ensure the validity of the requestor for all operations. In addition, it is worth noting that the computation cost is independent with the size of the requested file for access and deletion operations, since the size of signed message is constant.

VI.CONCLUSION

Design a secure data sharing scheme, for dynamic groups in an un-trusted cloud. The user is able to share data with others in the group without revealing identity privacy to the cloud and then, it supports efficient user revocation and new user joining. The efficient user revocation can be achieved through a public revocation list without updating the private keys of the remaining users, and new users directly decrypt files stored in the cloud before their participation. The storage overhead and the encryption computation cost are constant. Extensive analyses show that the proposed scheme satisfies the desired security requirements and guarantees efficiency as well.

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] Alysson neves bessani,lasige,”From byzantime fault tolerance to intrusion tolerance”,
DSNW '11 Proceedings of the 2011 IEEE/IFIP 41st International Conference on Dependable Systems and Networks Workshops , Pages 15-18

[3] Brent waters,Cipher text-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization.,pp 53-70,IEEE transactions., may 2011.

[4] DalitNaor,MoniNaor,Jeff latspitch,Revocation and Tracing Schemes for Stateless Receivers.,CRYPTO,springer,LNCS2139,pp 41-62,2001.

[5] Eu-Jin Goh,, Hovav Shacham, Nagendra Modadugu, Dan Boneh .,IEEE Transactions pp. 123- 149, Jan. 2010., SiRiUS: Securing Remote Untrusted Storage.

[6] 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.

[7] 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.

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

[9] Sanjay p.Ahuja,sindhu mani," High-Performance Cloud Computing: A View of Scientific Applications", journal of emerging trends in computing and information ,ISDN 2079-8401,Vol.3,February 2012.

[10] Shucheng yu,cong wang,kuiren and wenjing lou," Achieving secure, scalable, and fine-grained data access control in cloud computing",INFOCOM'10 proceedings on IEEEP is gateway page.no-534-542,2010.