Secured Group Data Sharing & Access Control on Cloud

[1]Nisha Melkunde, [2]Rameshwari Konda, [3]Pooja Katurde, [4]Trupti Mohite, [5]Dr.S.A.Ubale

[1,2,3,4]Research Scholar, [5]Head of Department
Department of IT
ZCOER, Pune

***Abstract*: Group data sharing in cloud environments has become a hot topic in recent decades. With the popularity of cloud computing, how to achieve secure and efficient data sharing in cloud environments is an urgent problem to be solved. In addition, how to achieve both anonymity and traceability is also a challenge in the cloud for data sharing. This paper focuses on enabling data sharing and storage for the same group in the cloud with high security and efficiency in an anonymous manner. By leveraging the key agreement and the group signature, a novel traceable group data sharing scheme is proposed to support anonymous multiple users in public clouds.**

On the one hand, group members can communicate anonymously with respect to the group signature, and the real identities of members can be traced if necessary. On the other hand, a common conference key is derived based on the key agreement to enable group members to share and store their data securely. Note that a symmetric balanced incomplete block design is utilized for key generation, which substantially reduces the burden on members to derive a common conference key. Both theoretical and experimental analyses demonstrate that the proposed scheme is secure and efficient for group data sharing in cloud computing.

***Keywords*: RSA (Rivest-Shamir-Adleman), ECC (Elliptic-curve-cryptography), BDH (Bilinear Diffie-Hellman) Deduplication, key Aggregation or conjunctive keyword search, explicite updation.**

Introduction:

Compared with the traditional information sharing and communication technology, cloud computing has attracted the interests of most researchers because of its low energy consumption and resource sharing characteristics. Cloud computing can not only provide users with apparently limitless computing resources but also provide users with apparently limitless storage resources. Cloud storage is one of the most important services in cloud computing, Namely Iaas, Passs, Saas etc.These models on which cloud computing is based.

SaaS(Software as a Service): The term "Software as a Service" (SaaS) is considered to be part of the nomenclature of cloud computing SaaS is closely related to the ASP (application service provider) and on demand computing software delivery models. The hosted application management model of SaaS is similar to ASP: the provider hosts the customer's software and delivers it to approved end users over the internet. In the software on demand SaaS model, the provider gives customers network-based access to a single copy of an application that the provider created specifically for SaaS distribution. The application's source code is the same for all customers and when new features are functionalities are rolled out, they are rolled out to all customers. Depending upon the service level agreement (SLA), the customer's data for each model may be stored locally, in the cloud or both locally and in the cloud. Example of SaaS is Google Apps, Email, face book.

Pass(Platform as a Service):Platform as a service (PaaS) is a cloud computing model in which a third-party provider delivers hardware and software tools usually those needed for application development to users over the internet. A Pass provider hosts the hardware and software on its own infrastructure. As a result, Pass frees users from having to install in-house hardware and software to develop or run a new application. Hosted applications environment for building and deploying cloud applications.-Amazon EC2, Microsoft Azure

Iaas(Infrastructure As A Service): Infrastructure as a service (IaaS) is a form of cloud computing that provides virtualized computing resources over the internet. IaaS is one of the three main categories of cloud computing services, alongside software as a service (SaaS) and platform as a service (Pass).In an IaaS model, a cloud provider hosts the infrastructure components traditionally present in an on-premises data center, including servers, storage and networking hardware, as well as the virtualization or hypervisor layer.

Amazon Simple Storage Service (S3): Companies today need the ability to simply and securely collect, store, and analyze their data at a massive scale. Amazon S3 is object storage built to store and retrieve any amount of data from anywhere – web sites and mobile apps, corporate applications, and data from IoT sensors or devices. It is designed to deliver 99.999999999% durability, and stores data for millions of applications used by market leaders in every industry. S3 provides comprehensive security and compliance capabilities that meet even the most stringent regulatory requirements. It gives customers flexibility in the way they manage data for cost optimization, access control, and compliance. S3 provides query-in-place functionality, allowing you to run powerful analytics directly on your data at rest in S3. And Amazon S3 is the most supported cloud storage service available, with integration from the largest community of third-party solutions, systems integrator partners, and other AWS services.

Group data sharing has many practical applications, such as electronic health networks , wireless body area networks , and electronic literature in libraries. There are two ways to share data in cloud storage. The first is a one-to-many pattern, which refers to the scenario where one client authorizes access to his/her data for many clients [8]. The second is a many-to-many pattern, which refers to a situation in which many clients in the same group authorize access to their data for many clients at the same time. Consider the following real-life scenario: in a research group at a scientific research institution, each member wants to share their results and discoveries with their team members. In this case, members on the same team are able to access all of the team's results (e.g., innovative ideas, research results, and experimental data). However, the maintenance and challenges caused by the local storage increase the difficulty and workload of information sharing in the group. Outsourcing data or time-consuming computational workloads to the cloud solves the problems of maintenance and challenges caused by local storage and reduces the redundancy of data information, which reduces the burden on enterprises, academic institutions or even individuals. However, due to the unreliability of the cloud, the outsourced data are prone to be leaked and tampered with. In many cases, users have only relatively low control in the cloud service and cannot guarantee the security of the stored data. In addition, in some cases, the user would prefer to anonymously achieve data sharing in the cloud.

Related work:

In order to overcome the above vulnerabilities, an effective access control for cloud computing was proposed by which attempts to protect the outsourced data from attackers and revoked malicious users. With respect to the key policy attribute-based encryption (KA-ABE) technique, it provides effective access control with fine grainedness, scalability and data confidentiality simultaneously. Specifically, each data file is encrypted with a random key chosen by the user. Subsequently, the random key will be encrypted by the KA-ABE. An access structure and secret key maintained by the group manager are distributed to authorized users, which can be used to decrypt the outsourced data. Note that if and only if the attribute of the data satisfies the access structure can the outsourced data be decrypted. However, the scheme is designed only for a general one-to-many communication system, which makes it inapplicable for the many-to-many pattern. On the other hand, a number of studies have been proposed to protect users' privacy [15]. In [16], a traceable privacy preserving communication scheme was proposed for vehicle to- grid networks in smart grids. However, this scheme is only suitable for two entities (i.e., vehicles and the central aggregator or the local aggregator); thus, it cannot be applied in cloud environments for the purpose of group data sharing. An example of group data sharing in cloud computing was proposed In [17], a secure scheme was proposed to support anonymous data sharing in cloud computing. Both anonymity and traceability are well supported by employing the group signature technique. In addition, efficient user changes are achieved by taking advantage of the dynamic broadcast encryption. However, this scheme suffers from the collusion attack performed by the cloud server and the revoked malicious user. In addition, compared with the broadcast encryption, we believe that the decentralized model is more suitable for data sharing in the cloud. Specifically, in [18], the key management system falls into two categories. The first is key distribution, in which the generation and distribution of the key is completely accomplished by a centralized controller. The second is key agreement, where all the members in the group fairly contribute, negotiate and determine a common conference key together. In the cloud environment, key distribution may be vulnerable since the centralized controller is the bottleneck of the system. Moreover, the large amount of computation and distribution for a common conference key may cause a large burden for the centralized controller. Many researchers have devoted themselves to the design of data sharing schemes in the cloud. But the problems existing in the above research still need to be resolved. In this paper, we focus on constructing an efficient and secure data sharing scheme that can support anonymous and traceable group data sharing in cloud computing. Note that the collusion attack is considered and addressed. Moreover, many-to-many group data sharing is supported in the proposed scheme.

Organization: The remainder of this paper is organized as follows. Section 2 presents some preliminaries in cryptographic and combinatorial mathematics. Section 3 describes the system model and our design goals. Section 4 presents the proposed scheme in detail. Section 5 and Section 6 perform the security and performance analyses, respectively. Section 7 concludes this paper and our work.

Motivation:

Our main motivation is to securely save the data on the cloud and access it securely. In this project authentication services and efficient access control are achieved with respect to the group signature technique. We main motive is to secure and fault-tolerant key agreement for group data sharing in a cloud storage scheme.

System Architecture: The architecture of our cloud computing scheme is considered by combining with a concrete example: users with similar interests and specialists in the related areas hope to store and share their works in the cloud (e.g., results and discoveries). The system model contains three entities: cloud, group manager (e.g., an active specialist) and group members(e.g., bidder).

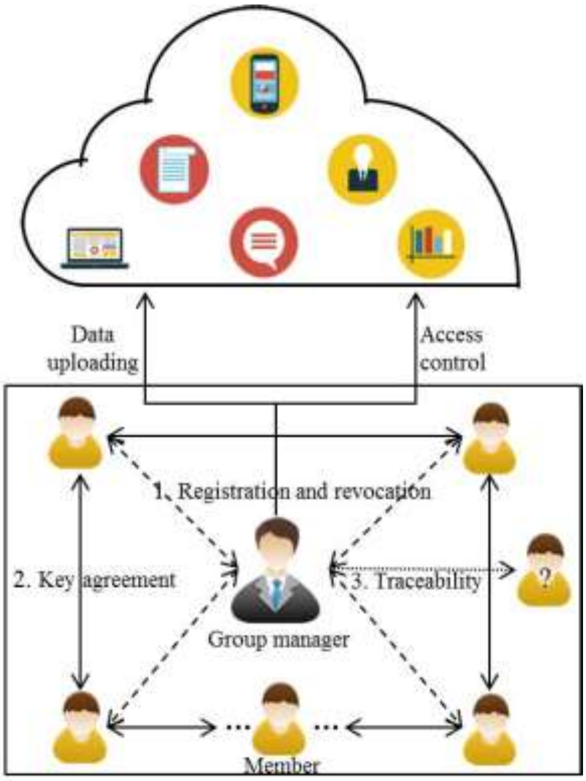

Fig 1. System Overview

1) Cloud: provides users with seemingly unlimited storage services. In addition to providing efficient and convenient storage services for users, the cloud can also provide data sharing services. However, the cloud has the characteristic of honest but curious [11], [24]. In other words, the cloud will not deliberately delete or modify the uploaded data of users, but it will be curious to understand the contents of the stored data and the user's identity. The cloud is a semi-trusted party in our scheme.

2) Group Manager: is responsible for generating system parameters, managing group members (i.e., uploading members' encrypted data, authorizing group members, revealing the real identity of a member) and for the fault tolerance detection. The group manager in our scheme is a fully trusted third party to both the cloud and group members.

3) Members: are composed of a series of users based on the SBIBD communication model. In our scheme, members are people with the same interests (e.g., bidder, doctors, and businessmen) and they want to share data in the cloud. The most worrying problem when users store data in the cloud server is the confidentiality of the outsourced data. In our system, users of the same group conduct a key agreement based on the SBIBD structure. Subsequently, a common conference key can be used to encrypt the data that

Will be uploaded to the cloud to ensure the confidentiality of the outsourced data. Attackers or the semi-trusted cloud server cannot learn any content of the outsourced data without the common conference key. In addition, anonymity is also a concern for users. Our scheme uses a technique called group signatures, which allows users in the same group to anonymously share data in the cloud.

Objective:

1) Dynamic Change: The intractable problem when sharing data in the cloud using the group manner is to ensure the security of the data when group members dynamically join and quit the group. A scheme that can support users' dynamic changes should guarantee that new users can access the previous data, whereas revoked users will not be able to obtain data in the cloud.

2) Data Confidentiality: In the cloud storage, data confidentiality requires that the outsourced data are invisible to the cloud server and to illegal users. Taking advantage of the key agreement, a common conference key can be derived among all the group members such that they can encrypt their data prior to uploading it to the cloud. Moreover, with respect to the SBIBD, the communication and computation complexities for generating the common conference key are relatively small compared.

3) Anonymity: Personal data are expected to be shared in the cloud without making the real identity public. Otherwise, few users are willing to share their information. Therefore, anonymity should be supported in the proposed scheme.

4) Traceability: Although data are shared anonymously in the cloud, a well-designed scheme should be able to locate the owner of the controversial data in disputes.

Conclusion:

In this paper we are implementing the secure group data sharing System. We developed the diffident technique to use the system to share secure data on the cloud. Its removing the redundancy of the data and the improving the performance of the system .and We analyze in this system about secured data transition through the cloud and We can store data on a cloud with Owen access control and share this data into a group.

Reference:

[1] J. Shen, T. Zhou, D. He, Y. Zhang, X. Sun, and Y. Xiang, “Block design-based key agreement for group data sharing in cloud computing,” IEEE Trans. Depend. Sec.Comput., to be published, doi: 10.1109/TDSC.2017.2725953.

[2] X. Chen, J. Li, J. Ma, Q. Tang, and W. Lou, “New algorithms for secure outsourcing of modular exponentiations,” IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 9, pp. 2386–2396, Sep. 2014.

[3] X. Chen, J. Li, X. Huang, J. Ma, and W. Lou, “New publicly verifiable databases with efficient updates,” IEEE Trans. Depend. Sec. Comput., vol. 12, no. 5, pp. 546–556, Sep. 2015.

[4] J. Li, Y. Zhang, X. Chen, and Y. Xiang, “Secure attribute-based data sharing for resource-limited users in cloud computing,” Comput. Secur., vol. 72, pp. 1–12, Jan. 2018, doi: 10.1016/j.cose.2017.08.007.

[5] Q. Liu, G. Wang, and J. Wu, “Time-based proxy re-encryption scheme for secure data sharing in a cloud environment,” Inf. Sci., vol. 258, pp. 355–370, Feb. 2014.

[6] H. Wang, Q. Wu, B. Qin, and J. Domingo-Ferrer, “FRR: Fair remote retrieval of outsourced private medical records in electronic health networks,” *J. Biomed. Inform.*, vol. 50, pp. 226–233, Aug. 2014.

[7] X. Chen, J. Li, J. Weng, J. Ma, and W. Lou, “Verifiable computation over large database with incremental updates,” *IEEE Trans. Comput.*, vol. 65, no. 10, pp. 3184–3195, Oct. 2016.

[8] J. Shen, J. Shen, X. Chen, X. Huang, and W. Susilo, “An efficient public auditing protocol with novel dynamic structure for cloud data,” *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 10, pp. 2402–2415, Oct. 2017.

[9] J. Shen, S. Moh, and I. Chung, “Identity-based key agreement protocol employing a symmetric balanced incomplete block design,” *J. Commun. Netw.*, vol. 14, no. 6, pp. 682–691, Dec. 2012.

[10] J. Yu, K. Ren, C. Wang, and V. Varadharajan, “Enabling cloud storage auditing with key-exposure resistance,” *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 6, pp. 1167–1179, Jun. 2015.