International Journal of Research
Available at
https://journals.pen2print.org/index.php/ijr/
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 13
December 2019

Anonymous and Traceable Group Data Sharing in Cloud Computing

Saima Ishaq M. SC (IT), King Khalid University.

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 betraced 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.

1. 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 [1]–[3]. Cloud storage is one of the most important services in cloud computing, which enables the interconnection of all types of electronic products. Moreover, various forms of data information can freely flow with respect to the cloud storage service, for instance, social networks, video editing and home networks. However, little attention has been given to group data sharing in the cloud, which refers to the situation in which multiple users want to achieve information sharing in a group manner for cooperative purposes [4], [5]. Group data sharing has many practical applications, such as electronic health networks [6], wireless body area networks [7], 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. Our goal is to achieve anonymous data sharing under a cloud computing environment in a group manner with high security and efficiency. To achieve this goal, the following challenging problems should be taken into consideration.

Our goal is to achieve anonymous data sharing under a cloud computing environment in a group manner with high security and efficiency. To achieve this goal, the following challenging problems should be taken into consideration. Firstly, an arbitrary and variable number of group members should be supported. In practical applications, the number of members in each group is arbitrary, and the dynamic joining and exiting of group members is frequent. A desired scheme not only supports the participation of any number of users but also supports efficient key and data updating.

Secondly, the confidentiality of the outsourced data should be preserved. Since the uploaded data may be sensitive and confidential business plans or scientific research achievements, data leakages may cause significant losses or serious consequence. Without the guarantee of confidentiality, users would not like to be involved in the cloud to share data. Thirdly, the way that data are shared should follow the many to-any pattern, which makes the information sharing more convenient and efficient. Rather than the single-owner manner in which data storage and deletion can only be completed by the group manager, we need a multiple-owner manner, where users have greater authority over their stored data.

Specifically, any user in the group can freely store and read their data stored in the cloud, and the deletion of data is performed by the user. Finally, in the many-to-many group data sharing pattern, it is essential to provide authentication services to resist misbehaving users. For instance, a misbehaving user may deliberately upload faulty data or misleading data to disturb and influence the cloud storage system. In addition, to resist the different key attack, a fault-tolerant property should be supported in the scheme.

2. OVERVIEW OF THESYSTEM

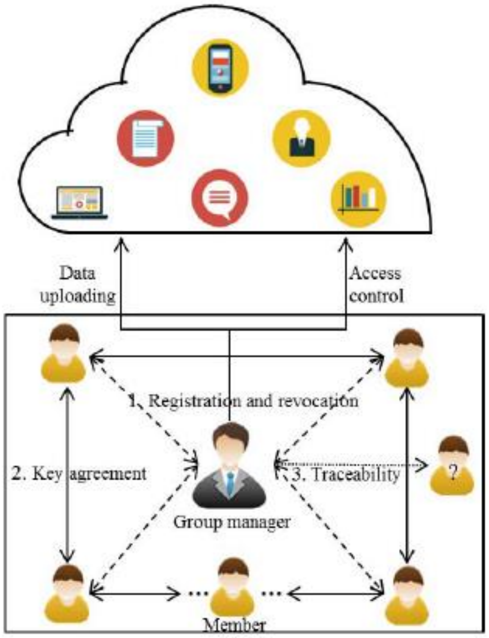


Fig 2.1 System Overview

2.1 EXISTING SYSTEM

- Previous works proposed a proxy re-encryption scheme to manage distributed file systems that attempt to achieve secure data storage in the semi-trusted party.

- Other works were proposed in 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.

3.2 DISADVANTAGES OF EXISTING SYSTEM:

- Proxy re-encryption scheme provides a stronger concept of security compared with [14], it is still vulnerable under collusion attacks and revoked malicious users.
- In KA-ABE scheme 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.

3.3 PROPOSED SYSTEM:

- To address the above challenges, we present a novel traceable group data sharing scheme for cloud computing with traceability and anonymity. The main contributions of this paper include the following.

- **Arbitrary Number of Users and Dynamic Changes Are Supported:**

To address an arbitrary number of users in real applications, we introduce the concept of the volunteer, which is used to satisfy the specific structure of the SBIBD such that the number of users can be arbitrary rather than restricted by the value of a prime k. Moreover, in real cloud storage applications, users may join or leave freely. The proposed scheme can efficiently support dynamic changes of users with respect to the access control and the many-to-many data sharing pattern.

- **The Confidentiality of the Outsourced Data Is Preserved:**

In our scheme, the outsourced data are encrypted with a common conference key prior to being uploaded. Attacks or the cloud having no access to the common conference key cannot reveal any information of the data stored in the cloud. The security of the encryption key is based on elliptic curve cryptography (ECC) and the bilinear Diffie-Hellman (BDH) assumption. Consequently, users can safely exchange data with others under the semi-trusted cloud.

- **Traceability Under an Anonymous Environment Is**

Achieved by Our Scheme: With respect to the key agreement, every user in the cloud is able to freely share data with other users. Moreover, users can exchange information in the cloud anonymously with respect to the group signature. Note that the group manager can reveal the real identity of the data owner based on the group signature bound with the data when a dispute occurs.

- **Authentication Services and Fault-Tolerant Property Are**

Provided: During the key agreement, each member exchange messages along with the group signature to declare that their identity is valid. Furthermore, the uploaded data file will be bound with the group signature such that the cloud can verify the validity of the file. In addition, the fault-tolerant property is supported in our scheme, which guarantees that malicious users can be identified and removed such that a unique common conference key can be derived.

3.4 ADVANTAGES OF PROPOSED SYSTEM:

- The proposed approach can generate a common conference key efficiently, which can be used to protect the security of the outsourced data and support secure group data sharing in the cloud at the same time.
- Authentication services and efficient access control are achieved with respect to the group signature technique. In addition, our scheme can support the traceability of user identity in an anonymous environment.

2.5 MODULES:

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

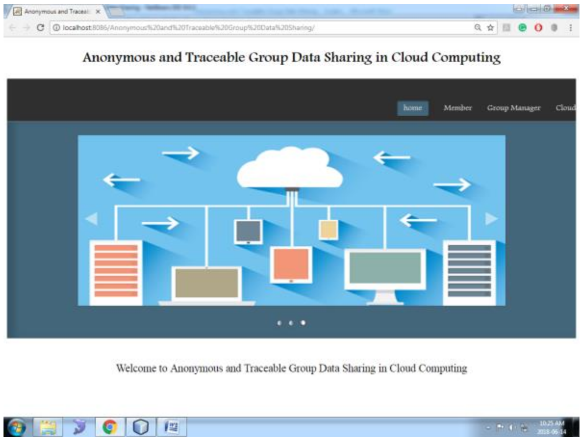
Cloud: provides users with seemingly unlimited storage services. In addition to providing efficient and convenient storage services for users, the cloud can also provide data sharing services. However, the cloud has the characteristic of honest but curious. In other words, the cloud will not deliberately 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.

Group Manager:

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.

Firstly, users with the same interest register at the group manager so as to share data in the cloud. In addition, user revocation is also performed by the group manager. Secondly, all members of the group based on the SBIBD structure jointly negotiate a common session key, which can be used to encrypt or decrypt the outsourced data. Finally, when a dispute occurs, the group manager is able to reveal the real identity of the group member. Note that in our system model, data uploading and access control are performed by the group manager

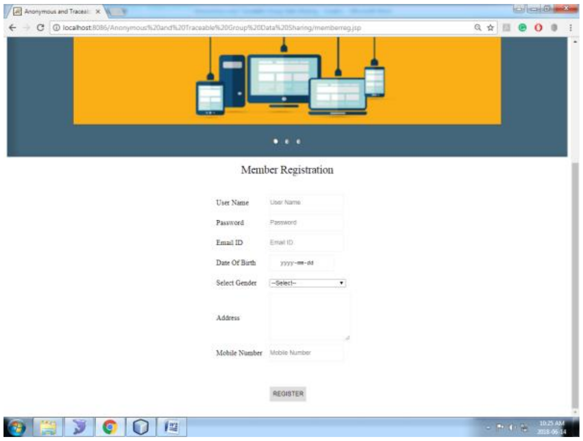
3. OUTPUT RESULTS


localhost:8086/Anonymous%20and%20Traceable%20Group%20Data%20Sharing/

Anonymous and Traceable Group Data Sharing in Cloud Computing

Welcome to Anonymous and Traceable Group Data Sharing in Cloud Computing

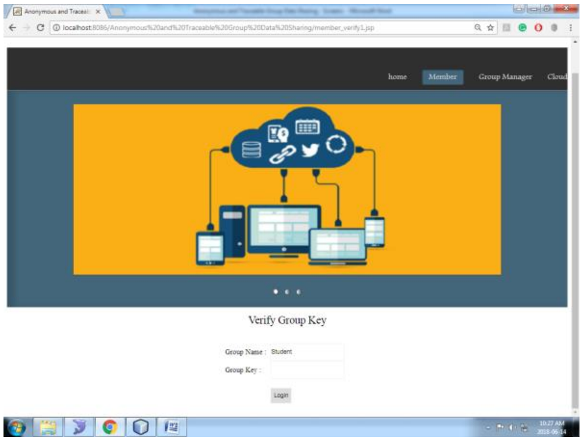
Fig 3.1: Home Page


localhost:8086/Anonymous%20and%20Traceable%20Group%20Data%20Sharing/memberreg.jsp

Member Registration

User Name
Password
Email ID
Date Of Birth
Select Gender
Address
Mobile Number

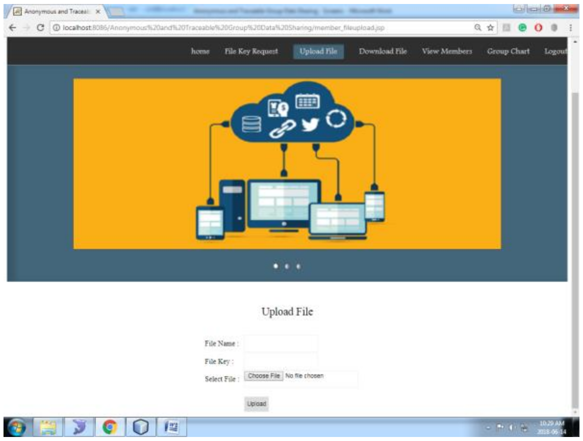
Fig 3.2: Member Registration page


localhost:8086/Anonymous%20and%20Traceable%20Group%20Data%20Sharing/member_verify1.jsp

Verify Group Key

Group Name : Student
Group Key :

Fig 3.3: Verify Group Key Page



Upload File

File Name :

File Key :

Select File : No file chosen

Fig 3.4: File Upload Page

4. CONCLUSION AND FUTURE ENHANCEMENT

In this project, we present a secure and fault-tolerant key agreement for group data sharing in a cloud storage scheme. Based on the SBIBD and group signature technique, the proposed approach can generate a common conference key efficiently, which can be used to protect the security of the outsourced data and support secure group data sharing in the cloud at the same time. Note that algorithms to construct the SBIBD and mathematical descriptions of the SBIBD are presented in this paper. Moreover, authentication services and efficient access control are achieved with respect to the group signature technique. In addition, our scheme can support the traceability of user identity in an anonymous environment. In terms of dynamic changes of the group member, taking advantage of the key agreement and efficient access control, the computational complexity and communication complexity for updating the common conference key and the encrypted data are relatively low.

5. REFERENCES

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

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

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

[4] J. Li, Y. Zhang, X. Chen, and Y. Xiang, “Secure attribute-based datasharing 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] J. Shen, T. Zhou, D. He, Y. Zhang, X. Sun, and Y. Xiang,“Block design-based key agreement for group data sharing in cloudcomputing,” *IEEE Trans. Depend. Sec. Comput.*, to be published,doi: 10.1109/TDSC.2017.2725953.

[6] H. Wang, Q. Wu, B. Qin, and J. Domingo-Ferrer, “FRR: Fair remoteretrieval of outsourced private medical records in

electronic healthnetworks,” *J. Biomed. Inform.*, vol. 50, pp. 226–233, Aug. 2014.

[7] J. Shen, S. Chang, J. Shen, Q. Liu, and X. Sun, “A lightweightmulti-layer authentication protocol for wireless body area networks,”*Future Generat.Comput. Syst.*, vol. 78, pp. 956–963, Jan. 2016,doi: 10.1016/j.future.2016.11.033.

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

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