AN EFFICIENT SECURE DATA SHARING AND PRIVACY PRESERVING APPLICATION FOR CLOUD DATA

BODDUPALLY VINOD KUMAR[1], R SHESHAN[2], SANKE RAVIKUMAR[3]

1 & 2, Associate Professor, CSE department, Brilliant Institute of Engineering & Technology, Hyderabad, TS.

3 Assistant Professor, CSE department, Brilliant Institute of Engineering & Technology, Hyderabad, TS.

ABSTRACT

With almost unlimited storage capacity and low maintenance cost, cloud storage becomes a convenient and efficient way for data sharing among cloud users. However, this introduces the challenges of access control and privacy protection when data sharing for multiple groups, as each group usually has its own encryption and access control mechanism to protect data confidentiality. In this project, we propose a multiple-group data sharing scheme with privacy preservation in the cloud. This scheme constructs a flexible access control framework by using group signature, ciphertext-policy attribute-based encryption and broadcast encryption, which supports both intra-group and cross-group data sharing with anonymous access. Furthermore, our scheme supports efficient user revocation. The security and efficiency of the scheme are proved thorough analysis and experiments

1. INTRODUCTION

Nowadays data have become important resources, sharing is now considered to be an inevitable trend to improve the value of data resources. With the help of cloud service, users can enjoy high quality sharing services while saving a lot of local infrastructure investment. Data sharing in the cloud, however, has a series of privacy and security risks as the cloud is out of the trust domain of the data owner.

There are many practical scenarios for data sharing. Consider the members of a research institution want to store and share their research data with each other. In order to reduce management and storage overhead, they store and share data in the cloud. But some research projects include sensitive commercial or national secrets. To protect data confidentiality, files are often encrypted before uploading to the cloud. Furthermore, users prefer to share data anonymously for preserving identity privacy. In addition, some projects may need to be completed together by multiple research institutions, and data may need to be shared among different groups, but each institution usually has its own encryption and access control mechanism, thus, data sharing for multiple groups presents some challenges.

First, the identity privacy of users is an urgent issue to be considered. On the one hand, they must be authenticated by the cloud to access the data. Without privacy preservation, the cloud may collect their identity information. On the other hand, if the identity privacy of users is unconditionally protected, accountability is difficult when they upload maliciously faulty shared data. Second, the multi-group access control is a thorny problem. To preserve data privacy, data owners usually encrypt their data, and then upload the cipher texts into the cloud.

2. LITERATURE SURVEY

Cloud imposes low maintenance and allows distribution data to be shared with multiple users. Distribution of data among multiple users imposes ownership constraint on data usage. Unfortunately, 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 project, we propose a secure sharing of data among multiple-owners for dynamic groups in the cloud. By leveraging group signature and dynamic broadcast encryption techniques, any cloud user can anonymously share data with others. Meanwhile, the storage overhead and encryption computation cost of our scheme are independent with the number of revoked users.

We consider the problem of building a secure cloud storage service on top of a public cloud infrastructure where the service provider is not completely trusted by the customer. We describe, at a high level, several architectures that combine recent and non-standard cryptographic primitives in order to achieve our goal. We survey the benefits such architecture would provide to both customers and service providers and give an overview of recent advances in cryptography motivated specifically by cloud storage.

This project proposes Privacy Preserving Identity-Based Broadcast Proxy Re-encryption (P2B) - a scheme to provide privacy preserving in identity-based broadcast proxy re-encryption. P2B uses Lagrange interpolation polynomial theorem to provide privacy to identities of the receiver group of broadcasted re-encrypted ciphertext. Proxy re-encryption is an efficient solution to securely share cloud data with receivers. For sharing data with a group of receivers, the sender needs to regenerate the re-encryption key for every receiver, which leads to an overhead on the sender side. To solve the issue, identity-based proxy re-encryption is extensible to identity-based broadcast proxy re-encryption. However, the later poses a privacy issue on the receiver side, as each receiver of the receiver group needs to know the other receiver's identity. We solve the problem using the Lagrange interpolation method. We prove that our scheme is secure against chosen plaintext attack using random oracle model and it successfully hides the identities of the receivers. Finally, we implement P2B and compare it with other existing systems. It is seen that P2B reduces the decryption time by 68% than recent existing Broadcast proxy re-encryption schemes and 98% than the existing privacy preserving schemes.

Cloud computing is an emerging computing paradigm in which resources of the computing infrastructure are provided as services over the Internet. As promising as it is, this paradigm also brings forth many new challenges for data security and access control when users outsource sensitive data for sharing on cloud servers, which are not within the same trusted domain as data owners. To keep sensitive user data confidential against untrusted servers, existing solutions usually apply cryptographic methods by disclosing data decryption keys only to authorized users. However, in doing so, these solutions inevitably introduce a heavy computation overhead on the data owner for key distribution and data management when fine-grained data access control is desired, and thus do not scale well. The problem of simultaneously achieving fine-grainedness, scalability, and data confidentiality of access control actually still remains unresolved. This paper addresses this challenging open issue by, on one hand, defining and enforcing access policies based on data attributes, and, on the other hand, allowing the data owner to delegate most of the computation tasks involved in fine-grained data access control to untrusted cloud servers without disclosing the underlying data contents. We achieve this goal by exploiting and uniquely combining techniques of attribute-based encryption (ABE), proxy re-encryption, and lazy re-encryption. Our proposed scheme also has salient properties of user access privilege confidentiality and user secret key accountability. Extensive analysis shows that our proposed scheme is highly efficient and provably secure under existing security models.

3. EXISTING SYSTEM

Some schemes were proposed to ensure secure data sharing. In these encryption systems, the data owner encrypts the data and specifies authorized visitors who can access the encrypted data. In, the cloud converted cipher text from one encryption system to another encryption system via proxy re-encryption to realize the data sharing among different encryption systems. However, an important issue is the privacy of user identity. The data visitor needs to submit the identity to obtain the decryption key. In addition, the data owner needs to stay online to authorize visitors of other groups.

Liu et al. proposed a multi-owner group data sharing scheme, in which identity-based dynamic broadcast encryption (IBBE) achieves flexible access control, the group administrators are responsible for key management of all users. With respect to the group signature technology, it protects user identity privacy and realizes anonymous and tractable data sharing. However, the scheme requires the identity of all data visitors and is usually only applicable to data sharing within a group. Shen et al.proposed an anonymous traceable group data sharing scheme, which generates shared session keys through multi-person key negotiation to reduce the burden of key management brought by centralized distribution to the central controller, but it can only realize data sharing within the same group.

1.2PROPOSEDSYSTEM

To realize data sharing of security and privacy protection for multiple groups in the cloud, we combine group signature, attribute-based encryption of ciphertext policy and broadcast encryption technology to realize conditional privacy protection and efficient access control. The group manager is responsible for key management within the group, and the key involved in cross-group data sharing is generated by the key generation center. The data owner does not have to manage all the visitors and be online all the time to authorize them.

A. System Construction This section describes the details of our scheme for the system construction, including system initialization, key distribution, file generation, file access and user revocation.

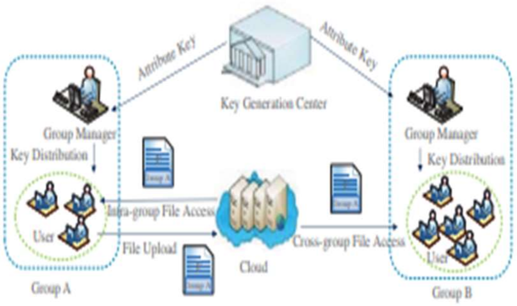
1) System Initialization

System initialization is performed by the key generation center and the manager of each group. The key generation center generates the system public parameter PK and the master key MSK by algorithm AttSetup. The manager is responsible for the initialization within his own group. The group public parameter GPK and the group master key GMK are generated by algorithm GroupSetup.

2) Key Distribution

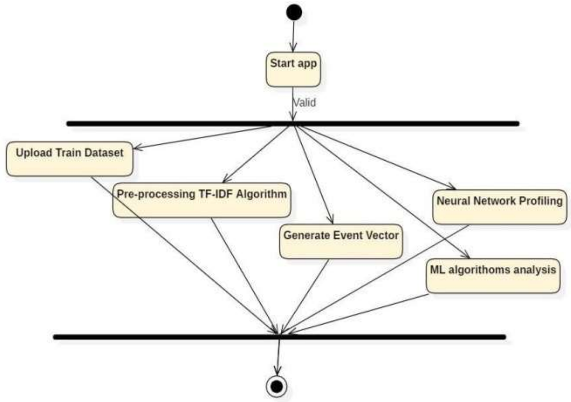
First, the group manager generates a set of attributes S for the group, and uses algorithm Sign(m, Ksig□ to generate the group signature σs for message m = (IDgroup, S), where Ksig denotes the key of the group signature. Then he sends the message (IDgroup, S, σs) to the KGC, where IDgroup stands for group identification. KGC runs algorithm Verify(m, σs, GPK) to verify whether the signature is valid, then runs algorithm AttKeyGen(PK, S, MSK) to generate the corresponding attribute key AttKey and send it to the group manager. After that the group manager runs the algorithm UserKeyGen(GPK, GMK, IDi) to generate the user key SK for each group member, and saves (IDi, SK) into the group user list. Finally, the group manager computes the proxy key PXK and uploads it into the cloud.

4.SYSTEM ARCHITECTURE .



Activity Diagram

A graphical representation of the work process of stepwise exercises and activities with support for decision, emphasis and simultaneousness, used to depict the business and operational well-ordered stream of parts in a framework furthermore demonstrates the general stream of control.



5. SYSTEM IMPLEMENTATION

1. GROUP MANAGER
2. USER
3. CLOUD

5.1.1 GROUP MANAGER

Group managers serve in a leadership role heading a team or division. They are responsible for a wide range of administrator-level tasks and oversee all aspects of daily operations.

□ Login
□ View User
□ View Activity
□ Manage Users
□ Logout

5.1.2 USER

Users can store files and applications on remote servers and then access all the data via the Internet.

□ Register
□ Login
□ Upload Files
□ View files
□ Profile
□ Logout

5.1.3 CLOUD

Anything that involves storing and processing huge volumes of data at high speeds—and requires more storage and computing capacity than most organizations can or want to purchase and deploy on-premises—is a target for cloud computing.

□ Login
□ View Files
□ Check files
□ Integrity
□ Send or Notify
□ Logout

6.1 TYPES OF TESTING

■Unit testing

Unit testing involves the design of test cases that validate that the internal program logic is functioning properly, and that program inputs produce valid outputs. All decision branches and internal code flow should be validated. It is the testing of individual software units of the application .it is done after the completion of an individual unit before integration. This is a structural testing, that relies on knowledge of its construction and is invasive. Unit tests perform basic tests at component level and test a specific business process, application, and/or system configuration. Unit tests ensure that each unique path of a business process performs accurately to the documented specifications and contains clearly defined inputs and expected results.

■Integration testing

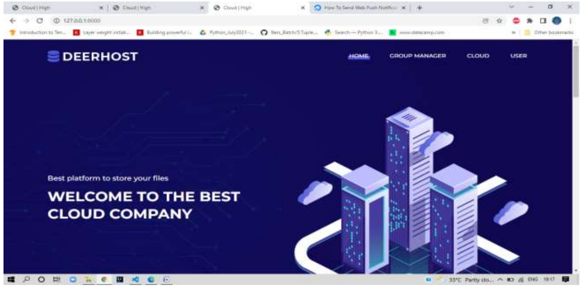
Integration tests are designed to test integrated software components to determine if they actually run as one program. Testing is event driven and is more concerned with the basic outcome of screens or fields. Integration tests demonstrate that although the components were individually satisfaction, as shown by successfully unit testing, the combination of components is correct and consistent. Integration testing is specifically aimed at exposing the problems that arise from the combination of components.

■Functional test

Functional tests provide systematic demonstrations that functions tested are available as specified by the business and technical requirements, system documentation, and user manuals.

Functional testing is centered on the following items:

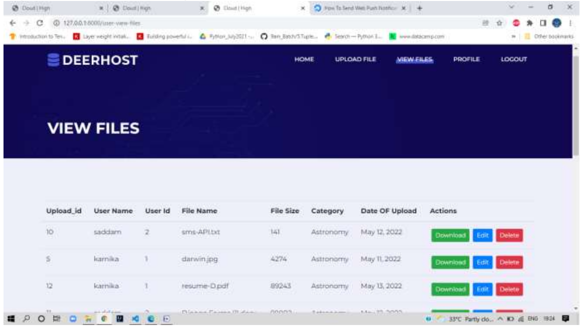
7.RESULTS



Best platform to store your files

WELCOME TO THE BEST CLOUD COMPANY

fig.7. 1 Home page



VIEW FILES

Upload_id	User Name	User Id	File Name	File Size	Category	Date OF Upload	Actions
10	saddam	2	sms-API.txt	141	Astronomy	May 12, 2022	Download Edit Delete
5	karnika	1	darwin.jpg	4274	Astronomy	May 11, 2022	Download Edit Delete
12	karnika	1	resume-D.pdf	89243	Astronomy	May 13, 2022	Download Edit Delete

fig.7.2 view files

8. CONCLUSION & FUTURE WORK

In this project, We proposed a privacy preserving data sharing scheme for multiple groups in the cloud. Users can access the cloud anonymously, and do not need to present their identity to obtain cross-group access rights. In addition, based on CP-ABE and broadcast encryption, Moreover, our scheme supports the flexible access control with efficient user revocation. The analysis shows that the proposed scheme meets the expected safety requirements and ensures the efficiency.

REFERENCES

[1] X. Liu, Y. Zhang, B. Wang and J. Yan, "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud," in IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 6, pp. 1182-1191, June 2013.

[2] S. Kamara and K. Lauter, "Cryptographic Cloud Storage, " Proc.Int'l Conf. Financial Cryptography and Data Security (FC), pp. 136149, Jan. 2010.

[3] S. Maiti and S. Misra, "P2B: Privacy Preserving Identity-Based Broadcast Proxy Re-Encryption," in IEEE Transactions on Vehicular Technology, vol. 69, no. 5, pp. 5610-5617, May 2020.

[4] H. Deng et al., "Identity-Based Encryption Transformation for Flexible Sharing of Encrypted Data in Public Cloud," in IEEE Transactions on Information Forensics and Security, vol. 15, pp. 3168-3180, 2020.

[5] 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.

[6] D. Zheng, B. Qin, Y. Li and A. Tian, "Cloud-Assisted Attribute-Based Data Sharing with Efficient User Revocation in the Internet of Things," in IEEE Wireless Communications, vol. 27, no. 3, pp. 18-23, June 2020.

[7] Y. Zhang, A. Wu, D. Zheng, "Efficient and privacy-aware attribute based data sharing in mobile cloud computing," J. Ambient Intell. Humaniz. Comput. vol. 9, no. 4, pp.1039-1048, August 2018.

[8] J. Shen, T. Zhou, X. Chen, J. Li and W. Susilo, "Anonymous and Traceable Group Data Sharing in Cloud Computing," in IEEE Transactions on Information Forensics and Security, vol. 13, no. 4, pp. 912-925, April 2018.