Volume 6, Issue 5, May 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Cloud Key Register for Data Sharing Methodology

P. Anusuya
Research Scholar, Dept. of Computer Science,
Tamil University, Thanjavur, Tamilnadu, India

A. Senthil Kumar
Asst. Professor, Dept. of Computer Science,
Tamil University, Thanjavur, Tamilnadu, India

Abstract: ***In case of group-shared data, the data face both cloud-specific and conventional insider threats. Secure data sharing among a group that counters insider threats of legitimate yet malicious users is an important research issue. In this paper, we propose the Secure Data Sharing in Clouds methodology that provides. File sharing in particular, is implemented in deferent ways by distinct cloud storage services. To keep sensitive user data confidential against unfrosted 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. By leveraging group signature, signed receipts and dynamic broadcast encryption techniques, any cloud user can anonymously share data with others. As the result the computation cost is reduced and storage overhead and encryption computation cost of our scheme are independent with the number of revoked users so the encryption cost is also reduced.***

Keywords: Encryption, Decryption, Key process.

I. INTRODUCTION

Cloud computing is rapidly emerging due to the provisioning of elastic, flexible, and on-demand storage and computing services for customers. These systems perform sharing through dedicated application servers which are responsible for controlling access to the as well as user groups management, data reduplication, etc. It means that the security of the sharing requires trusting not only the storage service for instance; Drop box is built on top Amazon S3, but also these application servers. Cloud computing is a promising computing paradigm which recently has drawn extensive attention from both academia and industry.

By combining a set of existing and new techniques from research areas such as Service-Oriented Architectures (SOA) and virtualization, cloud computing is regarded as such a computing paradigm in which resources in the computing infrastructure are provided as services over the Internet. 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 as mandated by various organizational policies and legal regulations. Encryption is a commonly adopted approach to protect the Confidentiality of the data.

Especially in the public cloud storage system, how to ensure the confidentiality of sensitive data and privacy, and provide the necessary mechanisms for sharing data security is becoming a hot topic of the current cloud storage security research. Current cloud storage data sharing security threats mainly from the following three aspects:

(1) Confidentiality, ISP intentionally or misuse of information leakage resulting data; (2) the integrity of the data from unauthorized entities modify, insert, delete etc;

(3) cloud storage system in an organization's server cluster failure or loss of data that users cannot access the data.

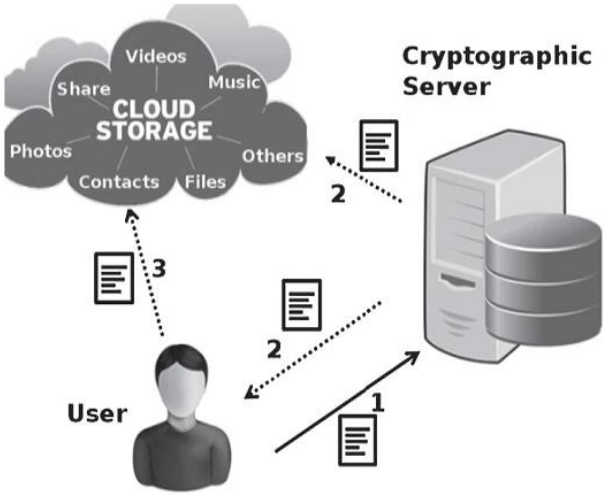
1.1. Key Register:

The user who wishes to access the data sends a download request to the CS. The CS, after authenticating the requesting user, receives the portion of the key from the user and subsequently downloads the data file from the cloud. The key is regenerated by operating on the user portion of the key, and the corresponding CS maintained portion for that particular user. The data are decrypted and sent back to the user. For a newly joining member, the two portions of the key are generated, and the user is added to the ACL. For a departing member, the record is deleted from the ACL.

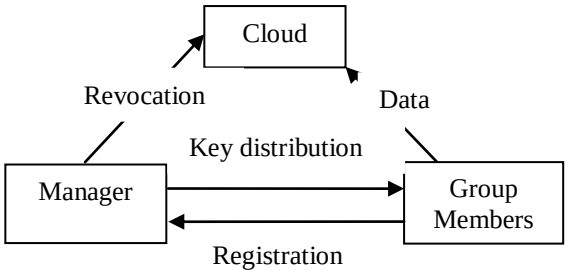
The departing member cannot decrypt the data on its own as he only possesses a portion of the key. Similarly, no frequent decryption and encryption are needed in case of changes in the group membership. Moreover, Seas can be used with the mobile cloud computing paradigm in addition to conventional cloud computing due to the fact that compute-intensive operations are performed by the CS.

II. STORAGE CLOUDS DIRCTRIES

To allow users to share their data, all cloud storage services provide some mach Anises that enable data owners to grant access over their resources to other principals. In all these storage services, the resources can be either buckets or objects. A Bucket, or container, represents a root directory where objects must be stored. There could be several buckets associated with a single cloud storage account. However, in most of the services, buckets must have unique names. Objects are stored in a bucket and can be either or directories.



1) The user in the group can share and store data files with others by the cloud;
2) The complexity and size taken for encryption is independent with the number of revoked users in the system;
3) User revocation can be achieved without updating the private keys of the remaining users and signed receipts will be collected after any revocation that reduces duplication of encrypted copies ;



Manager for group 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 AA manager is acted by the administrator of an organization. Therefore, we assume that the manager is fully trusted by the other parties.

2.1. Cloud

The cloud provides storage services to the user. The data on the cloud need to be secured against privacy breaches. The confidentiality of the data is ensured by storing encrypted data over the cloud. The cloud in the SeDaSC methodology only involves basic cloud operations of file upload and download. Therefore, no changes at the protocol or implementation level on the cloud are required.

2.2. New Group User Inclusion:

If a new user joins the group, the addition of the user is made on the request of the file owner. The request contains the user ID of the joining user, along with the access control parameters to be included in the ACL, and the group ID. The parameters include the IDs of the files for which the user has been granted access rights. It also includes the details indicating the READ and WRITE rights granted to the user. Alternatively, the date can be mentioned from which the access rights are valid for the user. This ensures the backward access control for the joining member. The CS, after receiving the joining request, updates the ACLs related to the files for which the access is granted. The key shares are generated, and the user shares are sent to the user along with the corresponding file IDs.

2.3. Data Confidentiality

Data confidentiality requires that unauthorized users including the cloud are incapable of learning the content of the stored data. 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 are unable to decrypt the data moved into the cloud after the revocation.

2.4. Anonymity and Traceability

Anonymity guarantees that group members can access the cloud without revealing the real identity it enables effective protection for user identity it poses a potential inside attack risk to the system. To tackle the inside attack, the group manager should have the ability to reveal the real identities of data owners.

(1) SP is not credible that the SP may be profitable for some purposes, data analysis stored thereon, and leaked to other non-authorized users.

(2) U is credible, U will not take the initiative to disclose its plaintext data acquisition, control key, the data key and cipher text data, but U may be affected by uncontrollable factors or misuse, etc. lead to information disclosure.

(3) Monitoring the attacker Aggressive behavior.

(4) The attacker's behavior is usually an afterthought. Attacker's typically not aggressive real-time access what data value only after the data is used to determine whether the attacker will attack to get the data.

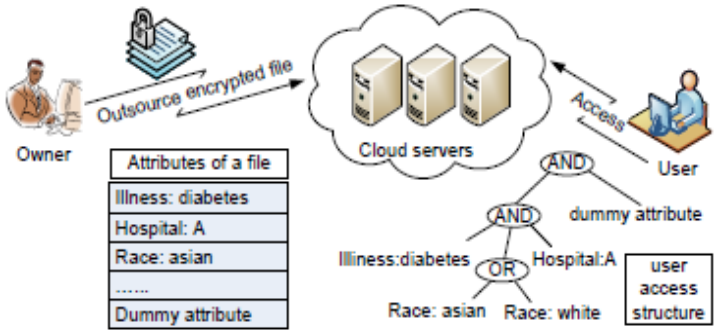
The division and dispersal of the key also helps counter the insider malicious users within the group. The ACL is separately maintained for each group file. Therefore, a valid group user cannot access the group file that is not shared with her. An attempt to access an unauthorized file is also blocked by the fact that the user will not have the key share for that file. Moreover, the ACL of the unauthorized file will not contain any record for the malicious user. Furthermore, the absence of the entire key with the user and the ACL collectively ensures the forward and backward access control for the data.

III. DATA SHARING USER

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. Specially, the group signature and signed receipt scheme enables users to anonymously use the cloud resources, and the dynamic broadcast encryption technique allows data owners to securely share their data files with others including new joining users.

3.1. Main Idea

In order to achieve secure, scalable and fine-grained access control on outsourced data in the cloud, we utilize and uniquely combine the following three advanced cryptographic techniques: KP-ABE, PRE and lazy re-encryption. More specifically, we associate each data file with a set of attributes, and assign each user an expressive access structure which is defined over these attributes. To enforce this kind of access control, we utilize KP-ABE to escort data encryption keys of data files. Such a construction enables us to immediately enjoy Fine-graininess of access control. However, this construction, if deployed alone, would introduce heavy computation overhead and cumbersome online burden towards the data Owner, as he is in charge of all the operations of data management.



As mentioned above, in a private cloud storage conditions proposed scheme based on user privacy protection in data sharing, data sharing process can be divided into stages, and data encryption and decryption phase two parts. In the encryption phase, O generated by D Key Gen data key, the encrypted data block with Enc, while with S key encryption and data fragmentation processing. After the cipher text data and key cipher text C CDK uploaded to DHT network.

3.2. Permissions

To allow users to grantees' capabilities over a shared resource, all clouds provide a set of permissions with documented semantics. As explained before, the same permission could have semantics in clouds. The available permissions for buckets and objects in several cloud storage providers.

As can be seen, Amazon S3 and Luna Cloud provide the largest set of permissions among all the services studied. They permit users to give read, write, read acp, write acp and full control permissions over both buckets and objects. Google Storage has almost the same set of permissions. The is that Google Storage does not allow users to apply read acp and write acp permissions separately. Instead, it put together these two Permissions into the full control one. This means that if a user wants to give other users the capability of read some resource's ACL, he is forced to also grant the capability to write or update that ACL.

The permissions provided by these two clouds are from the set of permissions we in Section 5, therefore, this protocol is more costly than the protocol in that section. For instance, Rule A is not respected in the second step: there is no permission on the bucket that allows grantees to read all objects inside it. This leads to the third and fourth step described above: when an object is uploaded to the shared bucket we need to associate an ACL with it to ensure read access to all grantees.

IV. CONCLUSIONS

Among them, the homomorphism key agreement allows authorized users get more control key and in order to achieve the purpose of file sharing. The encryption and decryption functionalities are performed at the CS that is a trusted third party in the SeDaSC methodology. The proposed methodology can be also employed to mobile cloud computing due to the fact that compute-intensive tasks are performed at the CS. We described the permissions provided by the services, their semantics, and the access-granting techniques that are used to apply these permissions to users. Additionally, a set of protocols for sharing data securely in several public storage clouds were presented. These protocols were by extending an ideal set of properties required for sharing data between users of a cloud service.

REFERENCES

[1] J. Wu, P. WyckoffandD. K. Panda,"PVFS over InfiniBand: Design and Performance Evaluation",In: Proceedings of 2003 International Conference on Parallel Processing, (**2003**), pp. 107-115.

[2] S. A. Weil, K. T. Pollack and S. A. Brandt, „Dynamic Metadata Management for Petabyte-Scale File Systems", In: Proceedings of the ACM/IEEE SuperComputing Conference, pp. 35-47.

[3] D. Ellard, J. Ledlie and P. Malkani, "Passive NFS Tracing of Email and Research Workloads", In: Proceedings of the Second USENIX Conference on File and Storage Technologies (FAST'03), San Francisco, CA, (**2003**) March, pp. 203-216.

[4] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu,"Scalable secure file sharing on untrusted storage," in Proc. OfFAST, 2003, pp. 29-42.

[5] E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius:Securing remote untrusted storage," in 2003, pp.131-145.

[6] Google drive. https://drive.google.com/

[7] Google storage documentation. https://developers.google.com/storage/docs/Accesscontrol.

