International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 07
March 2018

Data Sharing Scheme for Dynamic Groups in the Cloud

[1] K. Pavan kumar Reddy
M.Sc (Computer Science)
Besant theosophical college,madanapalli.
[2] D.Venkata Siva Reddy
Head dept. of C.S
Besant theosophical college,madanapalli.

ABSTRACT Users benefit from cloud computing, and can achieve an efficient and economical approach to sharing data among cloud group members with low-maintenance characters and low management costs. In the meantime, we must provide security guarantees to share data files because they are outsourced. Unfortunately, because of the frequent change of membership, sharing data while maintaining privacy is still a difficult issue, especially for an unreliable cloud due to the attack of collusion. Moreover, for existing schemes, key distribution security depends on the secure communication channel, however, assuming that this channel is a strong and difficult enforcement practice. In this paper, we propose a secure data sharing plan for dynamic members. First, we suggest a secure way to distribute keys without any secure connection channels, and users can get their own keys securely from the group manager. Second, our system can achieve strict access control, a user in the group who can use the source in the cloud and cancel users can not access the cloud again after revocation. Third, we can protect the schema from an attack of collusion, which means that users who have been revoked can not get the original data file even if they are plotting with the unreliable cloud. In our approach, by taking advantage of the multi-border function, we can achieve a secure user uninstallation system. Finally, our plan can perform well, which means that previous users do not need to update their own status keys if a new user joins the group or the user is revoked from the group.

Index Terms - Access Control, Privacy Preservation, Key Distribution, Cloud Computing

INTRODUCTION

CLOUD cloud computing, with low data sharing and low maintenance features, provides better resource utilization. In cloud computing, cloud service

Service providers offer unlimited storage space for customers to host data [1]. Customers can help reduce the financial

costs of data management by migrating the local management system to cloud servers. However, security concerns are the main drawback as we are now outsourcing data storage that may be sensitive to cloud service providers. To preserve the privacy of data, the common way is to encrypt data files before clients upload encrypted data to the cloud [2]. Unfortunately, it is difficult to design a secure and efficient data sharing system, especially for dynamic cloud groups. Kallhalla et al. [3] A cryptographic storage system provides secure sharing of data on untrusted servers based on techniques that divide files into file groups and encrypt each set of files with a file block key. However, it is necessary to update and distribute the file block keys to invalidate the user, therefore, the system has a significant increase in key distribution. Other schemes to share data on untrusted servers were proposed in [4], [5]. However, the complexity of user participation and cancellation in these systems increases in line with the number of data owners and users who have been revoked. Yu et al. [6] Utilizing and aggregating technologies based on the main attribute [7], and re-encoding and slow re-encoding to achieve control of access to granular micro data without disclosing data contents. However, the one-owner method may block implementation of applications, where any member of the group can use the cloud service to store and share data files with others. Lo et al. [8] Suggest a secure source schema by taking advantage of group signatures and encryption techniques based on the encoded text attribute of the text policy [9]. Each user gets two keys after registration while using the attribute key

Encrypt encrypted data with attribute-based encryption and use the group signing key to preserve privacyTracking. However, cancellation is not supported in this system. Leo et al. [10] Multi-secure data sharing was provided by the ownersScheme, named Mona. It is said that this system can achieve fine-grained access control and invalidation of users will not be able to access data sharing again when they areRevoked. However, the schema easily suffers from an attack of collusion by the canceled user and the cloud [13]. An aborted user can use his or her own key to decrypt the encrypted data file and obtain confidential data after it is canceled by plotting with the cloud. In the file access phase,First, the deactivated user sends the request to the cloud, and the cloud responds to the corresponding encrypted data file and the cancellation list to the user who has been revoked without verification.

After that, the user who has been deactivated can calculate the decryption key with the help of the attack algorithm. Finally, this attack can result in users being denied access to the sharing data and disclosure of other secrets to legitimate members.

EXISTING SYSTEM:

Kallahalla et al. Provides a secure storage system that allows secure data sharing on unreliable servers based on techniques that divide files into file groups and encrypt each group of files with a file block key.Yu et al used key cryptographic-based encryption techniques, re-encrypting the proxy, and slow encryption to achieve control over access to accurate data without disclosing data contents.

Disadvantages of existing system:

The file block keys must be updated and distributed to override the user; therefore, the overhead system has a heavy master distribution.The complexity of the user's participation and cancellation in these plans is increasingly complicated with the number of data owners and users who have been revoked. One-way owner may block applications, as any member of the group can use the cloud service to store and share data with others.

Proposed System:

In this paper, we suggest a secure data sharing schema, which can achieve secure primary distribution and data sharing for the dynamic group.

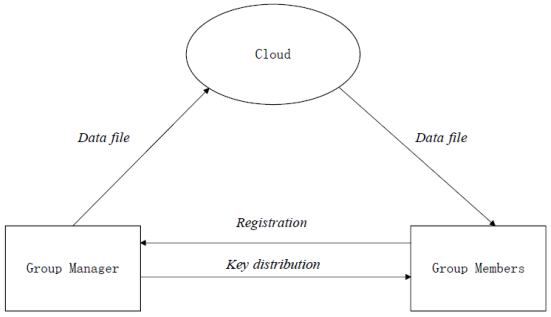
We provide a secure way to distribute keys without any secure connection channels. Users can get their own keys securely from the group manager without any of the certification authorities because of checking the public key of the user.Our plan can achieve strict access control, with the help of the user list of the group, any user in the group can use the source in the cloud and cancel users can not access the cloud again after revocation.We suggest a secure data sharing plan that can be protected from a collusion attack. Revoked users can not access the original data files as soon as they are revoked even if they conspire with the unreliable cloud. Our plan can achieve the abolition of a secure user with the help of a multi-border function.Our system is able to dynamically support dynamic groups. When a new user joins the group or the user is revoked from the group, the private keys for other users do not need to be recalculated

and updated.We provide security analysis to prove the security of our scheme.

Advantages of the proposed system:

The cost of the account is not related to the number of users revoked in the RBAC system. The reason is that regardless of how many users have been revoked, member operations to decrypt data files remain almost the same.Cost is not related to the number of canceled users. The reason for this is that the cost of the cloud account to upload the file in our plan consists of two confirmation signatures, unrelated to the number of canceled users. The reason for the small account cost of the cloud in the file upload phase of the RBAC system is that checks between contact entities are not involved in this schema.In our system, users can obtain their own keys securely from authorized authorities for groups, groups, and secure communication channels. As our plan is able to dynamically support dynamic groups, when a new user joins the group or the user is revoked from the group, the data for other users does not have to be recalculated and updated.

SYSTEM ARCHITECTURE:



conclusion

In this paper, we design a secure scheme to share data against the collusion of dynamic clusters in the cloud. In our scheme, the

Users can obtain their own keys securely from certified authorities for groups, groups, and secure communication channels. As our plan is able to dynamically support dynamic groups, when a new user joins the group or the user is revoked from the group, the data for other users does not have to be recalculated and updated. Furthermore, our plan can achieve a secure user rollout, and users who have been revoked can not access the original data files immediately They are revoked even if they conspire with the unreliable cloud**.**

AUTHOR DETAILS

Student Details

K. Pavan kumar Reddy

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 07
March 2018

Head dept. of CS&A,Besant theosophical college,madanapalli.

P no-9440750445

E mail-1.dvsrmpl@gmail.com

Guide Details