Result Analysis of Secure Anti-Collusion Data Sharing Scheme for Dynamic Groups in the Cloud

Pinky Mehra
M.Tech Scholar
Department of Cyber Security,
Kailash Narayan Patidar
College of Science and Technology, Bhopal, India

Vimal Shukla
Head of department
Department of Cyber Security,
Kailash Narayan Patidar
College of Science and Technology, Bhopal, India

Tariq Siddiqui
Asst. Professor
Department of Cyber Security,
Kailash Narayan Patidar
College of Science and Technology, Bhopal, India

ABSTRACT
The Benefited from Cloud Computing, clients can do a flourishing and moderate methodology for data sharing among gathering individuals within the cloud with the characters of low maintenance and small administration price. In Cloud Computing, cloud administration suppliers provide a reflection of boundless storeroom for customers to host data files since they're outsourced. Unfortunately, due to the frequent modification of the attachment, allocation data whereas as long as privacy-preserving is still a difficult issue, especially for an untrusted cloud owed to the collusion hit. Moreover, for existing schemes, the security of key distribution depends on the secure line, however, to have such channel could be a strong assumption and is tough for practice. Finally, our theme can succeed fine efficiency, which implies that previous users needn't to update their personal keys for matters either a replacement user joins within the group or a user is revoked from the group.

Keywords
Access power, Privacy-preserving, Key distribution, Cloud compute

1. INTRODUCTION
Cloud computing, with the characteristics of natural data sharing and low support, offers a superior usage of resources. In Cloud Computing, cloud administration suppliers provide a reflection of boundless storeroom for customers to host data files since they’re outsourced. Unfortunately, due to the frequent modification of the attachment, allocation data whereas as long as privacy-preserving is still a difficult issue, especially for an untrusted cloud owed to the collusion hit. Moreover, for existing schemes, the security of key distribution depends on the secure line, however, to have such channel could be a strong assumption and is tough for practice. Finally, our theme can succeed fine efficiency, which implies that previous users needn't to update their personal keys for matters either a replacement user joins within the group or a user is revoked from the group.

Keywords
Access power, Privacy-preserving, Key distribution, Cloud compute

2. THEORY
2.1 System Model
A cloud computing design by combining with an example that a company uses a cloud to enable its staffs within the same group or department to share files. The system model consists of 3 totally different entities: the cloud, a group manager (i.e., the company manager), and an oversized variety of group members (i.e., the staffs) as illustrated in Fig.1. Cloud is operated by CSPs and provides priced abundant storage services. However, the cloud isn’t totally sure by users since the CSPs are very possible to be outside of the cloud users’ sure domain. Like we tend to assume that the cloud server is honest however curious. That is, the cloud server won't maliciously delete or modify user information because of the protection of information auditing schemes, but can attempt to
learn the content of the stored information and also the identities of cloud users.

Group manager takes charge of system parameters generation, user registration, user revocation, and revealing the important identity of a dispute information owner. Within the given example, the group manager is acted by the administrator of the company. Therefore, we tend to assume that the group manager is absolutely sure by the opposite parties. Group members are a group of registered users that may store their private information into the cloud server and share them with others within the group. In our example, the staffs play the role of group members. Note that, the group membership is dynamically modified, because of the staff resignation and new employee participation within the company.

3. METHO

A secure data sharing theme proposes, which may achieve secure key distribution and data sharing for dynamic group. The most contributions of this scheme include:

1. This provides a secure method for key distribution without any secure communication channels. The users will securely get their private keys from group manager without any Certificate Authorities because of the verification for the general public key of the user.
2. This scheme can do fine-grained access control, with the help of the group user list, any user within the group will use the source within the cloud and revoked users cannot access the cloud again when they're revoked.
3. This secure data sharing scheme which may be protected from collusion attack. The revoked users cannot be able to get the original data files, once they're revoked even if they conspire with the untrusted cloud. This scheme can do secure user revocation with the help of polynomial perform.
4. This scheme is able to support dynamic teams with efficiency, once a new user joins within the group or a user is revoked from the group, the personal keys of the opposite users don't need to be recomputed and updated.
5. 5. This scheme provides a security analysis to prove the security of our scheme. Additionally, it conjointly performs simulations to demonstrate the efficiency of our scheme.

We can get some benefits from this scheme, they are:

1. This scheme achieves a secure key distribution and data sharing for dynamic group.
2. During this scheme the users will securely get their personal keys from group manager without any Certificate Authorities.
3. This scheme is protected from collusion attack.
4. This scheme is able to support dynamic groups with efficiency.
4. RESULT

![Graph](image)

**Fig. 4** cloud for file downloads among RBAC, Mona and our scheme

5. CONCLUSION

This scheme designs a secure anti-collusion information sharing scheme for dynamic groups within the cloud. During this scheme, the users will securely obtain their private keys from group manager without any Certificate Authorities and secure communication channels. Also, this scheme is ready to support dynamic groups with efficiency, once a new user joins within the group or a user is revoked from the group, the private keys of the other users ought not to be recomputed and updated. Moreover, this scheme can do secure user revocation; the revoked users cannot be able to get the original information files once they're revoked even if they conspire with the untrusted cloud.

6. REFERENCES


