PUBLIC INTEGRITY AUDITING FOR SHARED DYNAMIC CLOUD DATA WITH GROUP USER REVOCATION

AIM:

The aim of this project is to supports the public checking and efficient user revocation and also some nice properties, such as confidently, efficiency, count ability and traceability of secure group user revocation.

ABSTRACT:

The advent of the cloud computing makes storage out-sourcing become a rising trend, which promotes the secure remote data auditing a hot topic that appeared in the research literature. Recently some research consider the problem of secure and efficient public data integrity auditing for shared dynamic data. However, these schemes are still not secure against the collusion of cloud storage server and revoked group users during user revocation in practical cloud storage system. In this paper, we figure out the collusion attack in the exiting scheme and provide an efficient public integrity auditing scheme with secure group user revocation based on vector commitment and verifier-local revocation group signature. We design a concrete scheme based on the our scheme definition. Our scheme supports the public checking and efficient user revocation and also some nice properties, such as confidently, efficiency, count ability and traceability of secure group user revocation. Finally, the security and experimental analysis show that, compared with its relevant schemes our scheme is also secure and efficient.

INTRODUCTION:

The development of cloud computing motivates enterprises and organizations to outsource their data to third-party cloud service providers (CSPs), which will improve the storage limitation of resource con-strain local devices. Recently, some commercial cloud storage services, such as the simple storage service (S3) on-line data backup services of Amazon and some practical cloud based software Google Drive , Dropbox , Mozy , Bitcasa and Memopal , have been built for cloud application. Since the cloud servers may return an invalid result in some cases, such as server hardware/software failure, human maintenance and malicious attack , new forms of assurance of data integrity and accessibility are required to protect the security and privacy of cloud user's data.

In this paper, we further study the problem of construing public integrity auditing for shared dynamic data with group user revocation. Our contributions are three folds:

- We explore on the secure and efficient shared data integrate auditing for multi user operation for cipher text database.
- By incorporating the primitives of victor commitment, asymmetric group key agreement and group signature, we propose an efficient data auditing scheme while at the same time providing some new features, such as traceability and count ability.
- We provide the security and efficiency analysis of our scheme, and the analysis results show that our scheme is secure and efficient.

EXISTING SYSTEM:

The development of cloud computing motivates enterprises and organizations to outsource their data to third-party cloud service providers (CSPs), which will improve the storage limitation of resource con-strain local devices. Group users consist of a data owner and a number of users who are authorized to access and modify the data by the data owner The cloud storage server is semi-trusted, who provides data storage services for the group users. TPA could be any entity in the cloud, which will be able to conduct the data integrity of the shared data stored in the cloud server. In our system, the data owner could encrypt and upload its data to the remote cloud storage server. Also, he/she shares the privilege such as access and modify (compile and execute if necessary) to a number of group users. The TPA could efficiently verify the integrity of the data stored in the cloud storage server, even the data is frequently updated by the group users. The data owner is different from the other group users, he/she could securely revoke a group user when a group user is found malicious or the contract of the user is expired.