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

Pranjali wagh¹, Mayuri Khaire², Oshika Shinde³, Prof. Torana Kamble⁴

¹Computer Engineering, Bharati Vidyapeeth College of Engineering, Navi Mumbai,
²Computer Engineering, Bharati Vidyapeeth College of Engineering, Navi Mumbai,
³Computer Engineering, Bharati Vidyapeeth College of Engineering, Navi Mumbai,
⁴Professor Computer Engineering, Bharati Vidyapeeth College of Engineering, Navi Mumbai

Abstract— A cloud allows users to access application, information, and data of all sorts on an online level rather than by use of actual hardware or devices. A company offering reliable cloud technology allows or computing to be done in much more shared way, as a cloud provides a service rather than a product. User get and share their information in a way that can allow them to access and give access to the whole world or any groups of people within their cloud.

Since Cloud Computing is a newly evolving model for the delivery of software, platforms and infrastructure; it provides a new set of challenges to IT network and data security personnel. Most organizations that are considering moving their applications to the cloud have a variety of security concerns, which are in many ways, certainly warranted.

In this project, we propose a public integrity auditing scheme for cloud data sharing services characterized by multi-user modification, public auditing, high error detection probability, efficient user revocation as well as practical computational/communication auditing performance. Our scheme can resist user impersonation attack, which is not considered in existing techniques that support multi-user modification. Batch auditing of multiple tasks is also efficiently supported in our scheme.

Keywords— Cloud computing, group signature, public auditing, dynamic data, batch auditing.

I. INTRODUCTION

In past years, the rapid development of cloud storage services makes it easier than ever for cloud users to share data with each other. To ensure users’ confidence of the integrity of their shared data on cloud, a number of techniques have been proposed for data integrity auditing with focuses on various practical features, e.g. the support of dynamic data, public integrity auditing, low communication/computational audit cost, low storage overhead. However, most of these techniques consider that only the original data owner can modify the shared data, which limits these techniques to client read-only applications.

In this research paper we introduce publicly verifiable scheme, it helps in various aspects. That is data integrity can be performed not only by data owners, but also by one or more third party auditor. Conversely, the dynamic schemes which mentioned only focus on the gears where there is a data owner and only the data owner could change the data. In recent times, the growth of cloud computing, improves that some applications uses cloud service, can use as a collaboration platform. Few of the software development surroundings, one or more users in a group may need to share some of the source code, need to access, modify. At some times they may need to compile and run the shared source code at any time and place.

Purpose of this scheme is every group user can access the information from their cloud or can revoke efficiently by the group owner. In earlier scheme there is problem with collusion of cloud storage server and revoked group users during user revocation. So in propose system various concepts are used to achieve secure group user revocation. The group signature support encrypted data update
among group users and efficient group user revocation respectively. The group signature will prevent the collusion of cloud storage.

II. EXISTING SYSTEM
Considering data privacy, a traditional way to ensure it is rely on server to enforce the access control after authentication, which means any unexpected privilege escalation will expose all data.

In existing techniques that support multi-user modification. Batch auditing \([2]\) of multiple tasks. Only the data owner holds secret keys can modify the data and all other users who share data with the data owner only have read permission. If these solutions are trivially extended to support multiple writers with data integrity assurance, the data owner has to stay online, collecting modified data from other users and regenerating authentication tags for them.

Obviously, this kind of trivial extension will introduce a tremendous workload this kind of situation occurs many times, being it internationally or not, with existing cloud storage platforms.

As our design efficiently supports batch auditing, we can audit all development files at the same time to save cost. Thus, our scheme can be easily applied to existing VCSs to efficient support integrity assurance without changing their original design.

III. PROPOSE SYSTEM
Proposed scheme allows aggregation of integrity auditing operations for multiple tasks (files) through our batch integrity auditing technique, which promote our scheme in terms of auditing efficiency and data corruption detection probability.

The Third Party Auditor (TPA) refers to any party that checks the integrity of data being stored on the cloud. As our proposed scheme allows public integrity auditing, the TPA can actually be any cloud user as long as he/she has access to the public keys.

Our scheme supports the public checking and efficient user revocation and also some nice properties, such as confidently, efficiency, countability and traceability of secure group user revocation. Cloud computing, improves that some applications uses cloud service, can use as a collaboration platform.

IV. CLOUD STORAGE MODEL
There are three entities such as cloud storage server, group users and a Third Party Auditor (TPA). Group users consist of a data owner and number of users who are authorized to access and modify the information by data owner.

1) CLOUD STORAGE
Cloud storage is a model of data storage where the digital data is stored. The cloud storage providers are responsible for keeping the data available and accessible, and the physical environment protected and running people and organizations lease storage capacity from the providers to store user or application data. Cloud storage services can accessed through a co-located cloud computer service, a web service application programming interface (API) or application that utilize the API.
Figure 1. System Model

1) DATA OWNER
Data Owner Registration:
In this module an owner has to upload its files in a cloud server, he/she should register first. Then only he/she can be able to do it. For that he needs to fill the details in the registration form. These details are maintained in a database.

Owner Login:
In this module, any of the above mentioned person have to login, they should login by giving their email-id and password.

User Registration:
In this module if a user wants to access the data which is stored in a cloud, he/she should register their details first. These details are maintained in a Database.

User Login:
If the user is an authorized user, he/she can download the file by using file id which has been stored by data owner when it was uploading.

2) THIRD PARTY AUDITOR
ThirdPartyAuditor Registration:
In this module, if a third party auditor TPA (maintainer of clouds) wants to do some cloud offer, they should register first. Here we are doing like, this system allows only three cloud service providers.

ThirdPartyAuditor Login
After third party auditor gets logged in, He/ She can see how many data owners have uploaded their files into the cloud. Here we are providing three TPA for maintaining three different clouds.

V. SCHEME DESCRIPTION

1) Data Group sharing
There are multiple number of users who registered and will stored their private into cloud server and share them with others in the group. While sharing [3] some data into cloud no one directly access that file till he or she have group signature key to access shared file. Once he or she got the key then they can access file which is shared by data owner.
2) Public integrity auditing
Storage server is semi-trusted, who provides data storage services for the group users. TPA could be any entity in the cloud, which will able to conduct the data integrity of shared data stored in cloud server.

The data owner could encrypt and upload its data to the remote cloud server.
The TPA efficiently verify the integrity of the data stored in the cloud storage server, even data is frequently updated by the group users.

3) Revoked Group Users
The group signature will prevent the collusion of cloud and revoked group users, where the data owner will take part in the user revocation phase and the cloud could not revoked the data that last modified by the revoked user. An attacker outside the group may obtain some knowledge of plain text of the data.
This kind of attacker has to at least break the security of the adopted group data encryption scheme.
The cloud storage server colludes with the revoked group users, and they want to provide a illegal data without being detected.

4) Group signature
It is introduced by Chaum and Heyst. It provides anonymity for signers, where each group member has a private key that enables the user to sign messages. However, the resulting signature keeps the identity of the signer secret. Usually, there is a third party that can conduct the signature anonymity using a special trapdoor.
Some systems support revocation where group membership can be disabled without affecting the signing ability of unrevoked users.
Boneh and Shacham proposed an efficient group signature with verifier-local revocation. The scheme provides the properties of group signature such as selfless-anonymity and traceability.

VI. CONCLUSION
Proposed system to realize efficient and secure data integrity auditing for dynamic data. The proposed model consists of the public data auditing. This technique will provide better data confidentiality compare to other methodologies. The primitive of verifiable database with efficient updates is an important way to solve the problem of verifiable outsourcing of storage. We propose a scheme to realize efficient and secure data integrity auditing using group user revocation for shared dynamic cloud data.

VII. ACKNOWLEDGEMENT
It gives us great pleasure to present this paper on “Public Integrity Auditing using Group User Revocation for Shared Dynamic Cloud Data”.
We would also like to acknowledge help and guidance provided by our project guide Prof. Torana Kamble to share knowledge and provide valuable suggestions.

REFERENCES