Design the Efficiency Public Auditing Mechanism Using Identity Privacy and Traceability Concepts

D.Sharanya
M.Tech CSE Dept., Institute of Aeronautical Engineering, HYD-500043, TS, India
Dr K. Rajendra Prasad
Professor, CSE Dept., Institute of Aeronautical Engineering, HYD-500043,TS, India
Dr M. Madhu Bala
Professor, CSE Dept., Institute of Aeronautical Engineering, HYD-500043, TS, India.

Abstract: We use the cloud not only for store the data and share the data to multiple users. In storing and sharing life cycles we observe the reliability problems. Several public auditing mechanisms have been designed previously on shared data environment. Previous auditing mechanisms are design with ring signatures. Ring signature mechanism without download the complete data first verifies the signature. Signature verified then downloads the complete data. Using this procedure reduce the computation and communication cost. Here we observe the privacy accuracy is less. In this paper we design the new public auditing mechanism for enhance the privacy accuracy. Here we add the two new features. Those features are traceability and data freshness. These features improve the data privacy.

Keywords: shared data, public auditing mechanism, ring signature, traceability, and data freshness.

I. INTRODUCTION

Cloud service providers provide the access and shared services facility at a low marginal cost. Integrity and data leakage is the major problem in cloud data storage. Traditionally after retrieve the total data check the integrity. After some day’s new solution are designed. Without data utilization directly verify the signature with the help of ring signature. This solution gives the advantages with less amount of resources utilization. There is a data leakage and traceability problems.

To overcome the data leakage problem design the identity privacy tool as a new public auditing mechanism. Identity privacy tool control the fake users effectively. Next new key versions property also we add here to enhance the privacy.

II. RELATED WORK

From so many years investigation has been started to design different security tools. Tools are going to install on devices for control the hackers. Tools are works as software’s. Different common methods are ensuring to provide the cloud data storage security. Those common methods are encryption and decryption. Encryption and decryption methods provide the security in storage of cloud and transmission of data.

Different categories of cryptographic algorithms are available for providing the cloud data protection. Cryptographic algorithms are categorized into two types: symmetric cryptographic algorithms and asymmetric cryptographic algorithms. Symmetric cryptographic algorithms are used only single secrete key in encryption and decryption. Asymmetric cryptographic algorithms are used individual keys in encryption and decryption (private key and public key). Asymmetric and symmetric cryptographic algorithms does not providing the full fledged protection support. We have to use the algorithms for generation of passwords. Use password procedure for authentication purpose in different number of real time applications. Next in transmission of messages also we want security that’s why again we design the token approach. Using password and token approach store the encryption data in cloud as a secure. Some other methods are available to control the malicious insiders and outsiders. After store the encrypted data in cloud there is no reviewing procedures.

As a next concept we discuss service level agreement procedures for review the stored encrypted data. Use the service level agreement procedures improve the availability of integrity data in cloud. This is one of the important steps to improve the data security in cloud data storage environment. Improve the security for our data we should follow the below steps

1. Encryption and decryption operations data should not be store in single location.
2. Independent audit techniques improve the security levels.
3. Service providers design the more number of laws for reasonable security services implementation process.
4. Using backup and signature verification methods provide the desirable and reliable solutions.

Different cloud service providers are available to access and share the resources with less cost. Whenever access and share the resources first we should maintain the cloud storage as integrity data. Cloud is not contains the sufficient integrity data user’s are not get the correctness data. In previous
architectures we observe the many issues like hardware, software failures, data corruptness and human errors.

Downloading or store the files in cloud storage we observe the integrity issues and more resource utilization. Before downloading the complete file we check the signature of each and every block. All blocks of signatures are verified then we download the integrity file of information. This way provides effective services with reduce resources and cost. In this present software’s some features are missing like traceability and data freshness. We observe the some privacy issues.

III. PROBLEM STATEMENT

We design the new system model with different components like data owner, cloud server, group of users. Here two types of users are involved here. Those types of users are original user and group of users. Every user has a facility to access and modify the shared data in cloud server. Data owner store the files in cloud server. Before store the files in cloud server. Cloud owner provide the public key to the data owner and group users. Original user generates the ring signature using the private keys information. This ring signature is very useful for auditing of the data. Ring signature tracks the leakage of blocks information.

To overcome the leakage of blocks content now design the new mechanism with latest features. Those features are
1. Public auditing
2. Correctness
3. Traceability
4. Identity Privacy
5. Data Freshness

IV. SYSTEM MODEL

In new system model we propose the traceability and data freshness. Traceability property tracks the fake users. Any user can perform any operation user must be authentication user. Authentication user verification decision depends on log files. Log files contain registered users metadata. First users entered data is not match directly we are not deciding like fake user. Next user provides the security question answer. Finally security answer is wrong then we detect as a fake user.

Data freshness property provides the update key value information based on time interval. This property controls the more data leakages.

V. ALGORITHM

Pseudo code Traceability and Data Freshness:
Input: Registration information, Query, Files, key generation
Output: Traceability, Data Freshness
Step1: original user enter the details
Step2: check in log files
Step3: match in log files
Else if
   Allow to access the users
Else
   Detect as unauthorized user
Else
   Check with security questions
   Allow as a authentication user
Else
   Fake user
step4: update the keys based on time interval
step5: user submit the key to access the information
Enter update key
Check the key
Allow to download
Else
Reject the request
VI. EXPERIMENTAL RESULTS AND PERFORMANCE GRAPH

We conduct the experiments calculate the privacy responsibility levels. Privacy increases in terms of enhanced traceability and data leakage detection. Numbers of verifications are increases and data leakages are decreases.

![Performance Graph](image)

Fig 2: Performance Graph

Fig 2: graph represents the data leakage, traceability and auditing results. Compare to existing in proposed system produce the better results because of new features.

VII. CONCLUSION AND FUTURE WORK

In this paper we design the enhanced privacy and efficient public auditing mechanism with some extra features. Those features are traceability and data freshness. Data privacy in the cloud storage is improved using the new public auditing mechanism. Compare to existing system, proposed system is more efficient. Data freshness provides the efficient solution in access the data.

In future we extend the privacy mechanism using backup and data replication concept.

REFERENCES


Donthri Sharanya MTech computer science Engineering from Institute of Aeronautical Engineering,HYD-500043 BTech Computer Science Engineering from JNTUH. Her interested subjects include Data mining Information security big data.

Dr K. Rajendra Prasad Ph.D Computer Science Engineering M.Tech Computer Science Engineering, Professor is working in Institute of Aeronautical Engineering has guided many UG & PG studied. His research areas include Mining Techniques, Network Security Image Retrieval System.

Dr M. Madhu Bala Ph.D Computer Science Engineering M.Tech Computer Science Engineering, she is working as professor in Institute of Aeronautical Engineering has guided many UG & PG studied. Her research areas include Mining Techniques, Network Security Image Retrieval System.