Regeneration of Code Based Cloud Storage

[1] Namita S. Ranaware, [2] Rupali Dalvi

Dept. of Computer Engineering
MMCOE,
Pune, Maharashtra

Abstract - Cloud Computing is largely used utility for computing, where users can store their data into the cloud and access data from cloud as when they required so user can enjoy quality services from a computing resources. By data outsourcing, users can get free from the burden of data storage and data maintenance. Enabling public auditing for cloud data storage security is of critical importance so that users can restore to an external audit party to check the integrity of outsourced data when needed. To maintain this data efficiently, there is a necessity of data recovery services. First it help the users to collect information in the form of multimedia form from any remote location in the absence of network connectivity and second to recovery the files on data loss or if the server gets failed due to any reason.

***Keywords* - Cloud Storage, Privacy Preserving, Authenticator Regeneration, Regenerating Code.**

1. Introduction

Cloud storage is now gaining popularity because it offers a flexible on-demand data storage service with benefits. The relief from burden for universal data access at any location, storage management, and avoidance of expenditure on software, hardware, and personal maintenances, etc.[1]

To introduce third party auditor(TPA), the following two requirements have to met:

1) TPA should be able to audit the cloud data storage without the local copy of data from user of data, and no additional burden to stay on-line to the cloud user;
2) The third party auditing process should bring in no new vulnerabilities towards user data privacy[5]

1.1 Cloud Storage Server

Cloud storage server find outs the misbehaving server and threats and also protects the user data from attacks of untrusted third party. Cloud Storage Server is main storage server, it contents cloud exchanger and cloud coordinator. Cloud Data are retrieved from the storage devices on request of end user. In Data Storage architecture, the end user of system can also decide which data should available to access and share for the other users in cloud. Cloud service provides the services to user of cloud in very securely. MD5 algorithm improves security of data during storage and retrieval of data in cloud. Remote data integrity checking is used to maintain the data from threats. It manages the retrieval processes and effective storage, that ensures data security from untrusted access.

1.2 Data Partitioning Techniques To Improve Cloud Storage

The Data Partitioning Technique provide high performance, reduced cost and unlimited data storage space in cloud [5]. It also ensures resilient against threads, attacks and misbehaving server by using encryption techniques. To ensure security and data storage efficiency on cloud, cloud Data partitioning and Integrity checking is designed effectively.

1.3 Regenerating Code Based Cloud Storage

We focus on the integrity verification problem to regeneration of code based on cloud storage are designed for private audit, only data owner is able to verify the integrity of users data and repair the dead servers. Earlier, large amount of data is generated in electronic format, to provide data on users request there is necessity of data recovery services.

These services provide to introduce seed block algorithm which we used for remote data backup. There are two objective of this algorithm. The first is to gather information from any location and the second is to recovery of the files which might be delete or that can be lost because of cloud destroy[2]. This algorithm also reduce the time require for recovery process, concerns about the simplicity of backup and recovery process. Seed Block Algorithm uses exclusive OR(XOR) operation for computation.

2. Literature Survey

[1] Boyang Wang, Li, and Hui Li, "Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud", IEEE TRANSACTIONS ON CLOUD COMPUTING, VOL. 2, NO. 1,JANUARYMARCH 2014.

This paper uses public auditing scheme for the regenerating-code-based cloud storage system, where the data owners need to communicate TPA for their data validity checking[1]. To protect trusted third party the data privacy against the , system randomize the coefficients in the beginning rather than applying the blind technique during the auditing process. The data owner cannot stay always online[3]. This scheme is provable secure, and the performance evaluation shows that scheme is highly efficient.

[2] C. Selvakumar,G. Jeeva Rathanam,M. R. Sumalatha, "PDDS - Improving Cloud Data Storage Security Using Data Partitioning Technique", 3rd IEEE International Advance Computing Conference (IACC), 2013.

In this paper privacy-preserving mechanism that supports public auditing on shared data stored in the cloud. This mechanism is able to perform multiple auditing tasks simultaneously instead of verifying them one by one. This mechanism utilize ring signatures , so that a public verifier can check data integrity without retrieving the entire data. But the drawback of this system is that it just find out that data is lost/corrupt or not. It will not regenerate the corrupted data[4].

Advantages- Able to perform multiple auditing tasks simultaneously.
Disadvantages- It just find out that data is lost/corrupt or Not.

[3] Pritee Parwekar, Mayuri Saxena, Prakash Kumar, Sakshi Saxena, "Public Auditing: Cloud Data Storage", IEEE TRANSACTIONS , VOL. 24, NO. 4, 2013
Using dynamic data operation data is stored on the cloud , which makes the user to make a copy of data for further updating and verification of the data on loss. In this paper the partitioning method is proposed for the data security which avoids to make copy of data at the user side by using partitioning method. This method ensures high cloud storage integrity, easy identification of misbehaving server, enhanced error localization. But the drawback of this system only finds out that is there is any misbehaving is happened or not. if happened is will not recover the data[2].

Advantages- Error localization And easy identification of misbehaving server.
Disadvantages- This system only finds out that is there is any misbehaving is happened or not.

[4] Shivananda V. Seeri, J. D. Pujari and P. S. Hiremath, "Seed Block Algorithm: A Remote Smart Data Back-up Technique for Cloud Computing", IEEE Volume 4, Issue 1, April 2013

Parity cloud service is comparatively reliable from among all technique. simple, easy to use and more convenient for data recovery totally based on parity recovery service. It can recover data with very high probability. For data recovery, it generates a virtual disk in user system for data backup, make parity groups across virtual disk, and store parity data of parity group in cloud. It uses the Exclusive OR( ) for creating Parity information[4]. But drawback is it unable to control the implementation complexities[2].

Advantages- Easy to use and more convenient for data recovery.
Disadvantages- Implementation complexities.

[5] Kakad Umesh , Kankhar Mahesh ,Mysore Ajay , Nitin Rathee, "BACKUP AND RECOVERY SYSTEM USING SEED BLOCK ALGORITHM", International Journal of Advanced Research in Computer Engineering Technology (IJARCET) Volume 4 Issue 1,January 2015

High Speed Data Rate Transfer has come out an efficient technique for the movable clients such as laptop, smart-phones etc. nevertheless it fails to manage the low cost for the implementation of the recovery and also unable to control the data duplication[7].

Advantages- Efficient technique for the movable clients.
Disadvantages- Costly, Increased redundancy

3. Comparative Study

Table 1: Comparative Study

Sr. No	Title	Author	Method
1.	Oruta: Privacy Preserving Public Auditing for shared data in cloud, IEEE, 2014.	Boyang Wang, Baochun Li,Hui Li	public auditing.
2.	PDDS: Improved cloud Data storage security using Data partitioning technique, IEEE 2012,	C. Selvakumar, G. Jeeva Rathanam ,M.R. Sumalatha	The user need to make a copy for further updating and verification of the data

3.	PCS(Parity cloud storage), international joint conference of IEEE,2011	Ruchira. H. Titare, Prof. Pravin Kulkurkari	For data recovery,it generates a virtual disk in user system for data backup
4.	HSDRT(High speed Data rate transfer), fifth international conference on system network communication, 2012,	Tanay Kulkarni, Krupali Dhaygude, Sumit Memane, Onkar Nene	This System will transfer data with high rate of transfer.

4. Experimental Setup and Evaluation

To create the multimedia data regeneration system we will connect two cloud servers in network and one proxy server for purpose of security and recovery of data. TPA will act as trusted party and partition data to different cloud servers for recovery.

Data owner of the system will sign up/ sign in to upload a multimedia file. The data owner will upload a file and generate a private key to encrypt file and sends encrypted file to the TPA(Third Party Auditor). Then TPA will apply partitioning algorithm on encrypted file, generate digital signature of each partition and upload partitions on different servers. After that TPA will send metadata to proxy server and audit the servers after some specific time interval. As the attacker deletes file from server TPA notifies proxy about deleted file and proxy will regenerate the deleted file with the help of regeneration algorithm.

The proposed system result will be regenerate multimedia data with the help of regeneration algorithm and cloud server. By comparing the result of existing system with the result of proposed system, proposed system will regenerate the multimedia data which is lost which existing system will only find out that data is lost or not.

5. Conclusion

In this paper we have described various techniques available in literature for multimedia data regeneration techniques. Number of approaches proposed for solution to the regeneration of large amount of multimedia data. This research presents a novel idea of regenerating data to provide a security and availability of the data. By using this method, the problem of data unavailability will be solved without using public auditing technique.

6. Future Scope

In future we can provide a more security to data to avoid data loss . And also instead of doing two partitions of data we can do more partitions.

References

[1] Cong Wang, Qian Wang, Kui Ren, and Wenjing Lou, “Privacy-Preserving Public Auditing for Regenerating-Code-Based Cloud Storage”, IEEE Transactions on Information Forensics and Security,2015

[2] Kailas Pophale, Priyanka Patil,Rahul Shelake,Swapnil Sapkal,“Seed Block Algorithm: Remote Smart Data-Backup Technique for Cloud Computing”, International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 3, March 2015

[3] Boyang Wang, Li, and Hui Li, “Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud”, IEEE TRANSACTIONS ON CLOUD COMPUTING, VOL. 2, NO. 1,JANUARYMARCH 2014.

[4] C. Selvakumar,G. Jeeva Rathanam,M. R. Sumalatha, “PDDS - Improving Cloud Data Storage Security Using Data Partitioning Technique”, 3rd IEEE International Advance Computing Conference (IACC), 2013.

[5] Pritee Parwekar, Mayuri Saxena, Prakash Kumar, Sakshi Saxena, “Public Auditing: Cloud Data Storage”, IEEE TRANSACTIONS , VOL. 24, NO. 4, 2013

[6] Kakad Umesh , Kankhar Mahesh ,Mysore Ajay , Nitin Rathee, “BACKUP AND RECOVERY SYSTEM USING SEED BLOCK ALGORITHM”, International Journal of Advanced Research in Computer Engineering Technology (IJARCET) Volume 4 Issue 1,January 2015

[7] Shivananda V. Seeri, J. D. Pujari and P. S. Hiremath, “Seed Block Algorithm: A Remote Smart Data Back-up Technique for Cloud Computing”, IEEE Volume 4, Issue 1, April 2013

Author Profile:

Ranaware Namita S. received her B.E degree in computer engineering from Savitribai Phule Pune University in 2014.She is currently pursuing M.E degree at computer engineering from Marathwada Mitra Mandal’s College Of Engineering,pune.

Mrs. R. Dalvi has completed M.E. in Computer Engineering from Pune university. She is currently working as Assistant Professor in the Department of Computer Engineering at MarathwadaMitra Mandals College of Engineering, Pune.