International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue14
November 2017

User Data Recovery and Secure Data Distribution in the Cloud

Anuj Rapaka
Assistant Professor, Department of CSE, Shri Vishnu Engineering College for Women (A),
Vishnupur, Bhimavaram, West Godavari District, Andhra Pradesh.
anujrpk@gmail.com

Abstract: *Cloud storage provides online storage where data file is stored in form of virtualized pool that is usually organized by third parties. In cloud computing, data generated in electronic form are huge in amount. To maintain this data efficiently, there is a necessity of reliable data recovery services. When the data file is stored in remote server, we need to provide the security to maintain the integrity of the data file. With cloud data services, it is commonplace for data file to be not only stored in the cloud, but also shared across different users. Because of this, the integrity of cloud data is subject to uncertainty due to the hardware/software failures and data user errors. In this article, we propose a smart remote data backup technique using encryption and compression techniques. The objective of proposed techniques is twofold; first it help the users to collect and recover the data files in case of the data file deletion or if the cloud gets destroyed due to any reason and second is to preserve the privacy of any user during data distribution in cloud. We are using admin panel to preserve the privacy of the user. We are also providing encryption technique to provide security to the user's data file. The time related issues are also being solved by proposed techniques such that it will take minimum time for transmitting the data file to remote cloud as data file size is reduced by using the data compression technique.*

Keywords: data recovery, remote storage, encryption, Compression.

1. INTRODUCTION

The data files or information concerning user's which is stored in any devices is lost due to hardware problem like if the system gets physically crashed or data gets corrupted then there is no other source to recover it. It is very complex job to manage various user data since work is done manually. There are lots of chances that the errors can occur in maintaining the various users and also there is huge data storage problem in centralized storage system.

Today, Cloud Computing is itself a huge technology which is surpassing all the previous technology of computing of this competitive and challenging IT world. Cloud storage provides the online storage where data stored in form of virtualized pool that is usually hosted by third parties. The cloud computing has rapidly grown in recent years due to the advantages of greater flexibility and availability of computing resources at lower cost. Cloud service providers offer users efficient and scalable data storage services with a much lower marginal cost than

traditional approaches. Cloud computing gives flexibility to the user, when users put their data in the cloud, they need not manage the information stored in cloud storage. Cloud computing lets you access all your application and document from anywhere in the world.

Cloud service provider operates huge data on data centre and according to the requirements of the customer these data centre virtualized the resources and expose them as the storage pools that help user to store data files or data objects. Data sharing becomes a standard feature in most cloud storage offerings, including iCloud and Google Drive [2]. As number of user shares the storage and other resources, it is possible that other customers can access user data. Either the human error, faulty equipment's, network connectivity, a bug or any criminal intent may put our cloud storage on the risk and danger.

The integrity of data in cloud storage, however, is subject to uncertainty as data stored in the cloud can easily be lost or corrupted due to the unavoidable hardware/software failures and human errors. To make this matter even worse, cloud service providers may be reluctant to inform users about these data errors in order to maintain the reputation of their services and avoid losing profits. The traditional approach for checking data correctness is to retrieve the entire data from the cloud and then verify data integrity by checking the correctness of signatures of the entire data. Though this conventional approach is able to successfully check the correctness of cloud data, the efficiency of using this traditional approach on cloud data is in doubt. The main reason is that the size of cloud data is huge in general and downloading the entire cloud data to verify data integrity will cost or even waste user's amounts of computation and communication resources.

To overcome these issues, we propose a new technique in which the data is stored in the remote cloud. If the main cloud gets destroyed or data is lost then the remote cloud will give the back-up of data to the client. The admin panel will provide a secure ID to each client so in case of data distribution to other clients this ID will preserves the privacy of the clients.

2. RELATED WORK

In literature, we study most of the recent back-up and recovery techniques that have been developed in cloud computing domain. SBA technique help the users to collect information from any remote location in the absence of network connectivity and second to recover the data files in case of the data file deletion or if the cloud gets destroyed due to any reason. The time related issues are also being solved by proposed Seed Block Algorithm(SBA) [1].

Privacy-Preserving Public Auditing for Shared Data in the Cloud is a novel privacy-preserving mechanism that supports public auditing on shared data stored in the cloud. In this mechanism ring signatures are used to compute verification metadata needed to audit the correctness of shared data. The Parity Cloud Service (PCS) technique provides a privacy-protected personal data recovery service.

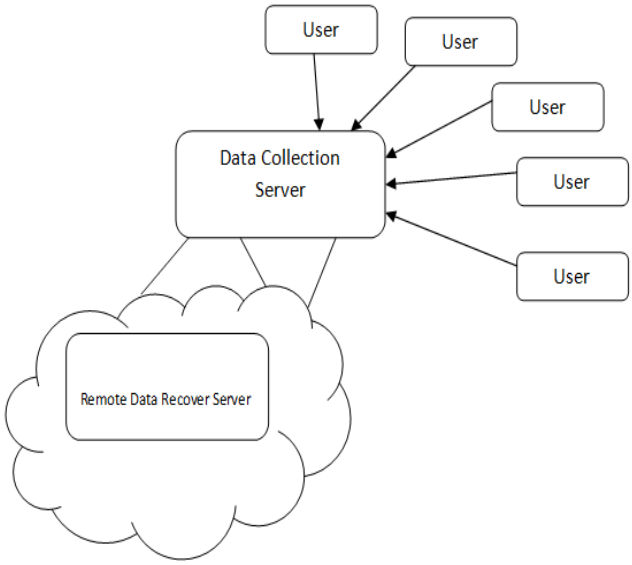

Fig:- Remote Data Recovery Server and its Architecture

The objective of Remote Data Collection Server: Health Care is to provide auto response server, better solutions for data backup and restore using cloud. It can collect data and send to a centralized repository in a platform independent format without any network consideration [4].

All these techniques tried to cover different issues maintaining the cost of implementation but it creates the huge amount of data and requires more storage as the size of data is not reduced. Also there is lack of privacy and security in these techniques.

3. SEED BLOCK ALGORITHM

Initialization:

Data Collection Server **DC**;

Remote Data Recover Server **RD**;

Users of Data Collection Server: $\mathbf{U_i}$;

Files: $\mathbf{a_1}$;

Random Number: r;

Seed Block: $\mathbf{S_i}$

User's ID: **User_ID**

Input: $\mathbf{a_1}$ Created by $\mathbf{U_i}$; **r** is generated at **RD;**

Output: Recovered file $\mathbf{a_1}$ after deletion $\mathbf{U_i}$ at

Given: Authenticated Users Data server allow uploading, downloading and do modification on its own the file only

Step 1: Generate a random number.

Intr = rand();

Step 2: create a seed block $\mathbf{S_i}$ for each $\mathbf{C_i}$ and Store $\mathbf{S_i}$ at **RD**

$\mathbf{S_i}$ **= rUser_ID**

(Repeat step 2 for all users)

Step 3: if $\mathbf{U_i}$**/Admin** creates/modifies **a** and stores $\mathbf{a_1}$ at **DC**

then a^1_1 create as $a_1 = a^1_1 S_i$

Step 4: Store a^1 at **RD.**

Step 5: If Server crashes a_1 deleted from **DC,**

then, we do EXOR to retrieve the original a_1 as:

$a_1 = a^1_1 S_i$

Step 6: Return a_1 to U_i

Step 7: STOP.

4. PROBLEM DEFINITION

In the cloud, huge amount of the data are stored but if one of the server is crashed or slows down then the private data of the user will loss. This paper will explain the process of taking the back-up of user's data in encrypted and compressed manner. As data is shared in the cloud so to provide the privacy to the user we are providing the admin panel to authenticate the user.

5. OBJECTIVE

The objective of proposed techniques is

- To help the users to collect and recover the files in case of the file deletion or if the cloud gets destroyed due to any reason
- To preserve the privacy of any user during data distribution in cloud. We are using admin panel to preserve the privacy of the user.

We are also providing encryption technique to provide security to the user's data. The time related issues are also being solved by proposed techniques such that it will take minimum time for transmitting the file to remote cloud as file size is reduced by using the compression technique.

To achieve the objective of this project, we have proposed following techniques:

-While creating the back-up of the user's data, we are going to encrypt the data by using advanced encryption techniques.

-Then we compress this encrypted file by using lossless compression technique and the store this compressed file to a remote data back-up cloud.

-For privacy preserving we are introducing an admin panel that manage and authenticate the user credentials and provide signature. The user credentials are also encrypted.

6. CONCLUSION

This review paper proposes a technique to perform a smart remote data backup using encryption and compression techniques. It also preserves the privacy of the user in case of data distribution in the cloud by providing the admin panel.

7. REFERENCES

[1] Ms. Kruti Sharma, Prof. Kavita R Singh, 2013, "Seed Block Algorithm: A Remote Smart Data Back-up Technique for Cloud Computing", 2013 IEEE international conference on

communication system and network technology, 6-8 April 2013, ISBN 978-1-4673-5603-9

[2] Boyang Wang, Baochun Li, Hui Li have presented a new technology "Oruta: Privacy-Preserving Public Auditing for Shared Data in Cloud", IEEE transactions on cloud computing, vol. 2, no. 1, january-march 2014.

[3] Chi-won Song, Sungmin Park, Dong-wook Kim, Sooyong Kang, 2011, "Parity Cloud Service: A Privacy- Protected Personal Data Recovery Service," International Joint Conference of IEEE TrustCom-11/IEEE ICESS-11/FCST-1

[4] Kalyani Bangale, Nivedita Gupta, Swati Singh Parihar, "Remote Data Collection Server : E-Health Care" International Journal of Innovative Research in Computer and Communication Engineering, An ISO 3297: 2007 Certified Organization, Vol. 2, Issue 2, February 2014.

[5] S.Ezhil Arasu, B.Gowri, S.Ananthi presented "Privacy-Preserving Public Auditing In Cloud Using HMAC Algorithm" International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-2, Issue-1, March 2013.

[6] Giuseppe Pirr´o, Paolo Trunfio , Domenico Talia, Paolo Missier and Carole Goble, 2010, "ERGOT: A Semantic-based System for Service Discovery in Distributed Infrastructures," 10th IEEE/ACM International Conference on Cluster, Cloud and Grid Computing.

[7] Kruti Sharma, Kavita R Singh, "Online Data Back-up and Disaster Recovery Techniques in Cloud Computing: A Review" ISSN: 2277-3754 ISO 9001:2008 Certified International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 5, November 2012

[8] Lili Sun, Jianwei An, Yang Yang, Ming Zeng, 2011, "Recovery Strategies for Service Composition in Dynamic Network," International Conference on Cloud and Service Computing.

[9] D. Srinivas, "Privacy-Preserving Public Auditing In Cloud Storage Security", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 (6) , 2011, 2691-2693.

[10] Tejashree Paigude, Prof. T. A. Chavan, "A survey on Privacy Preserving Public Auditing for Data Storage Security", International Journal of Computer Trends and Technology- volume4 Issue3-2013