International Journal of Innovative Research in Computerand Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488 |

||Volume 8, Issue 6, June 2020||

Private Information Retrieval and Security in Cloud Storage Systems

Pallavi Karjol[1], Pallavi V R[2], Rohini T[3], Shravani J[4], Rashmi T V[5]

B. E Student, Dept. Of CSE, SIT, Tumkur, Karnataka, India. [1]

B. E Student, Dept. Of CSE, SIT, Tumkur, Karnataka, India[2]

B. E Student, Dept. Of CSE, SIT, Tumkur, Karnataka, India[3]

B. E Student, Dept. Of CSE, SIT, Tumkur, Karnataka, India[4]

Assistant Professor, Dept. Of CSE, SIT, Tumkur, Karnataka, India[5]

ABSTRACT: Preserving privacy while retrieving data from cloud storage is very important. The proposed solution provides security and privacy for cloud data storage systems that ensure the requested information is securely accessed by a user without knowing to the other servers. Uploaded content will be distributed among the different servers as encrypted data. This ensures that the data leak will be of no use for the third party.This paper focuses primarily on the Private Information Retrieval problem in distributed storage systems. Users must be able to download content from a pool of distributed servers in such a way that the servers cannot determine which content the user is requesting. The goal here is to provide user data with privacy.

KEYWORDS: Privacy, Security, cloud storage

I. INTRODUCTION

This section includes a brief introduction about cloud storage and importance of preserving privacy and security while retrieving data from cloud storage.

In today's world everything is being connected with cloud. Cloud allows users to store, manage and even access their data. The cloud systems are the very popular platform for storage. They provide many services to cloud users such as Platform as a service (PaaS), Software as a Service (SaaS), Infrastructure as a Service(IaaS) etc. The main issue concerned with cloud systems is security. The stored data in the cloud has to be protected and it should be unavailable to the unauthorized users. One of the main concerns of service providers is thus to provide protection for the data stored in the cloud. Most cloud service providers use the encryption algorithm to encrypt the data present on the servers.

In this approach, all contents stored over the network is distributed among the servers with Random Linear Fountain (RLF) codes. A number of servers are working together to form a Repair Group to retrieve a content. Secrecy and privacy through encryption and decryption algorithms in distributed storage systems. If the user wants to download the content from a pool of distributed servers in such a way that the servers cannot determine which content the user is requesting. This is primarily known as Private Information Retrieval (PIR) problem. To request data from the servers, users can use the random queries to address the PIR problem in the distributed storage systems and retrieving any desired content without knowing what content the user is requesting from the other servers. It is an important feature of the proposed technique which offers security for the user data against many other servers.

II. RELATED WORK

In this paper, Random Linear Fountain (RLF) codes [1][2] are used to encode the contents within the servers in the network. The codes which provides data reliability, data availability and also perform node repair efficiently are called Regenerating codes [2].

They have considered threat model where the auditor gain access to the data. Another aspect can be is handling of node failures. If it fails, a new empty node has to replace the storage node and it can be used to obtain the data stored by the failed node. To achieve this, the entire message from the network has to be downloaded and the desired content has to be extracted from that node. They provide explicit, secretive constructions of regenerating codes.

A hybrid PIR scheme [3] which is mainly proposed based on secret sharing. This provides the security upto a certain number of servers. Initially they presented a protocol which is called Byzantine-robust PIR protocol, provides privacy protection against coalitions upto all responding servers. They have extended their protocol to provide protection to the

queries, if any collusion occurs in limited number of servers. Protection is also provided against collusions to the contents of the database.

PIR algorithm has been proposed against the colluding server which is robust and for private information retrieval they presented fault tolerant scheme [4]. This scheme ensures the service provision in the presence of server failures and protects the users privacy. They introduced error-detection algorithm used to detect corrupted results from the servers. This scheme tolerates the failures of the servers very efficiently and any information being leaked to attackers is prevented.

To solve PIR problem shannon used a technique called shannon cipher [5]. The number of keys should be equal to the number of messages according to this technique. The problem here, if there is any increase in number of messages, key number also increases. A huge number of keys has to be stored by each user which is not possible in practical.

III. SYSTEM DESIGN

A. System Architecture

Figure 1 represents the control between cloud servers, owner and client in a cloud storage system and Figure 2 represents the system architecture. When the file is uploaded, it is divided and stored in different servers. Among these, one server acts as coordinating server which will contains the information of all the other servers and acts as catalog which stores metadata of all the servers and the other servers doesn't have any connection or link between each other and cannot have accessibility to know what is stored in each other servers.

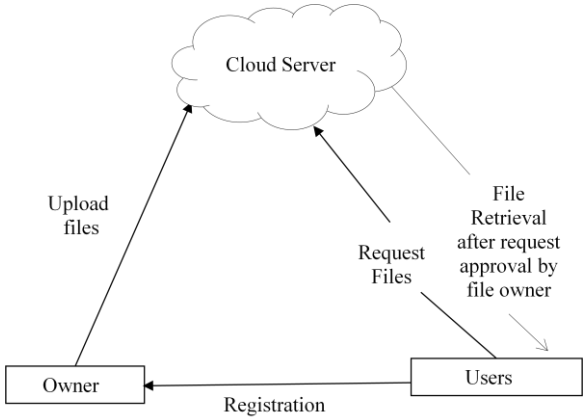

Figure 1: System Architecture depicting control flow

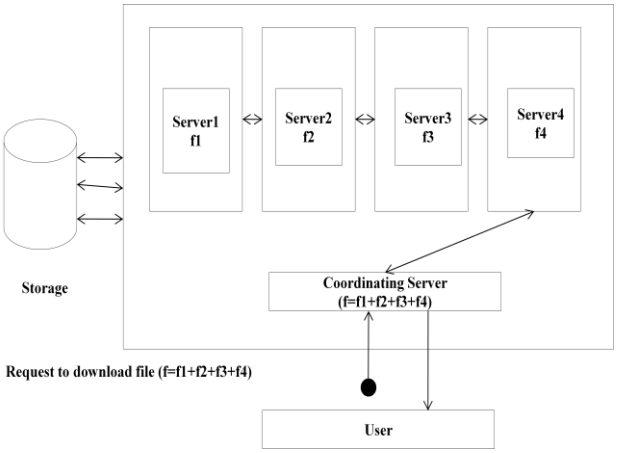

Figure 2: Architecture depicting co-ordination between servers

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488 |

||Volume 8, Issue 6, June 2020||

B. Methodology

The system provides an interface for user register for first time using several inputs such as username, mobile number and password etc. Once the user registers, username and password can be used for login. Registered user can login to the application and use the services using their credentials (username and password). Then user can upload files into cloud. Files uploaded by the user are encrypted using RSA algorithm and uploaded into cloud server. Files are divided into parts and the same are encrypted and stored in different servers. If user needs file they can download the file. Encrypted parts of that file from the servers are aggregated and decrypted before user receives his requested file. An user can request a file uploaded by another user by sending the owner a request. Once the owner accepts this request, requested user will be sent an OTP which is used as authentication for downloading the requested file.

C. Modules

1. User registration : This module provides an interface for user registering themselves for first time using several inputs such as username, mobile number and password etc. Once the user register himself, username and password can be used for login next time. Input fields while registration of the user are validated so that only valid information is allowed.
2. Login Module : Registered user can login to the application and use the services using his credentials (username and password). This module verifies that user credentials are already authenticated.
3. File Upload : User can upload files into cloud using this interface. Files uploaded by the user are encrypted using RSA algorithm and uploaded into cloud server. Files are divided into parts and the same are encrypted and stored in different servers.
4. File Download : User can download his files using this interface. Encrypted parts of that file from the servers are aggregated and decrypted before user receives his requested file.
5. File Request : An user can request a file uploaded by another user by sending the owner a request. Once the owner accepts this request, requested user will be sent an OTP which is used as authentication for downloading the requested file. Downloading procedure will be same as before.

IV. RESULTS AND SCREENSHOTS

The proposed solution provides security and privacy for distributed cloud storage systems.

Figure 3: User Interface for new user registration by clicking the Register button on Home Page

Figure 4: User Interface for login by clicking Login button on Home Page

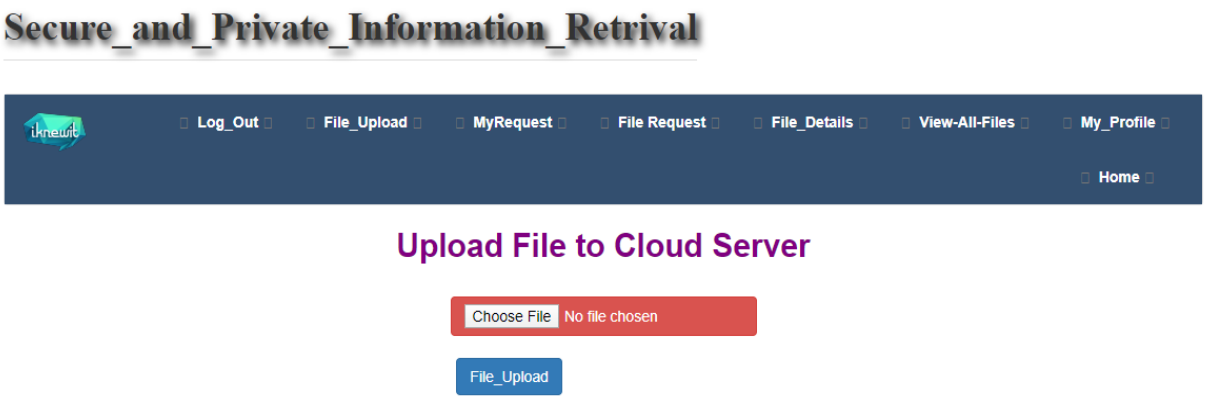

Figure 5: File uploading service on clicking File Upload option with various input fields

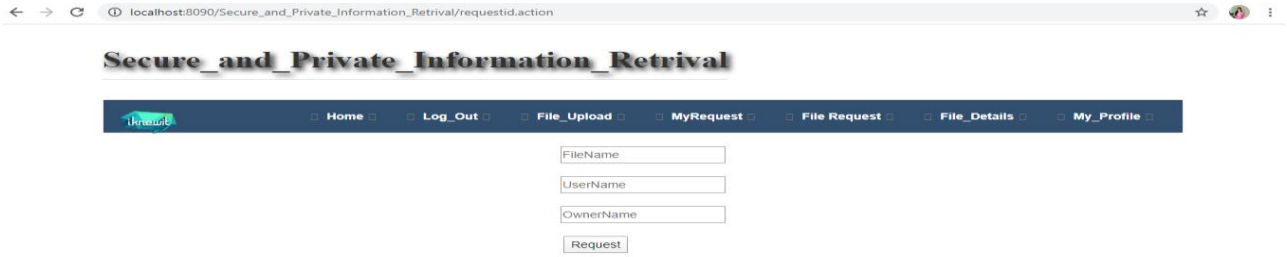

Figure 6: User Interface for requesting a file on clicking on Request option against any file.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488 |

||Volume 8, Issue 6, June 2020||

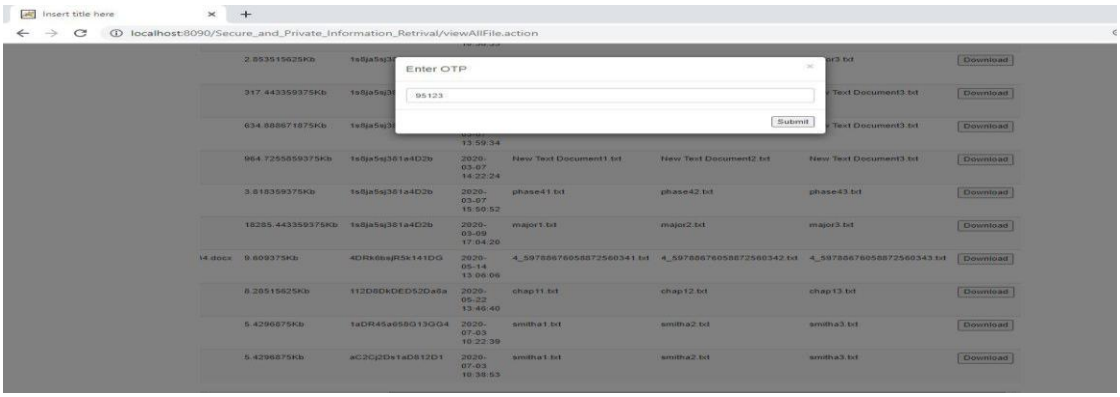

Figure 7: Asking for OTP whenever file owner accepts download request of user

.

V. CONCLUSION

The proposed solution provides security and privacy for distributed cloud storage systems. The technique used here is robust against other servers and it achieves secrecy for distributed storage systems.

REFERENCES

[1] Mohsen Karimzadeh Kiskani and Hamid R. Sadjadpour, “Secure And Private Information Retrieval (SAPIR) in Cloud Storage Systems”, IEEE 2018.
[2] N B Shah, K V Rashmi, and P Vijay Kumar, “Information theoretically secure regenerating codes for distributed storage”, 2011.
[3] y Ian Goldberg, “Improving the robustness of private information retrieval”, 2007.
[4] E Y Yang, Jie Xu, and Keith K Bennett, “Private information retrieval in the presence of malicious failures”, Proceedings of the 26th International Computer Software and Applications Conference on Prolonging Software Life: Development and Redevelopment, August 2002.
[5] C.E.Shannon, “Communication Theory of Secrecy Systems”, Bell system technical journal, 1949.
[6] David JC MacKay. Fountain codes. IEE Proceedings-Communications, 152(6):1062–1068, 2005.
[7] Dr. Rajamohan Parthasarathy P, P , Ms. Haw Wai Yee P, P, Mr. Seow Soon Loong P, Dr. Leelavathi Rajamanickam P, P, Ms. Preethy Ayyappan P, “Implementation of RSA Algorithm to Secure Data in Cloud Computing”, - International Journal of Innovative Science, Engineering & Technology, Vol. 6 Issue 4, April 2019 ISSN (Online) 2348 – 7968.
[8] Santosh Kumar Singh , Dr. P.K. Manjhi , Dr. R.K. Tiwari , “Data Security using RSA Algorithm in Cloud Computing”, International Journal of Advanced Research in Computer and Communication Engineering ISO 3297:2007 Certified Vol. 5, Issue 8, August 2016.
[9] Sheren A. El-Booz , Gamal Attiya and Nawal El-Fishawy, “A secure cloud storage system combining time-based one-time password and automatic blocker protocol”, El-Booz et al. EURASIP Journal on Information Security (2016) 2016:13.
[10] Ankita Patil, Kiran Zambare, Preeti Yadav, Pankaj Wasulkar Nisha Kimmatkar, “Integration Of Encryption Of File And One Time Password For Secure File Accesson Cloud”, International Journal of Advances In Computer Science and Cloud Computing, ISSN: 2321-4058 Volume- 3, Issue- 1, May-2015.
[11] Prof. Basavaraj M. Hunshal, Praveen D. Madagudi, Chetankumar S. Bidari, Manjunath G. Hubballi, Trimurthy .S.Panchal, “Security Cloud using Text File Splitting and OTP”, 2017 IJESC.