ISSN: 2277-9655
Impact Factor: 1.852

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

# Private Information Retrieval from Cloud in a Distributed Location

**Ms. Divya Pradha.N[*1], Mr.G.R.Anantha Raman[2]**
[*1] PG Scholar, Department of CSE, Adhiyamaan College of Engineering, Hosur, India
[2] Assistant Profesor, Department of CSE, Adhiyamaan College of Engineering, Hosur, India
jesusdivyapradha@gmail.com

## Abstract

Cloud computing a big buzzword now-a-days and IT Industry talks about it a lot and they started to move to Cloud. Cloud is mainly for Storage, Elasticity, Sharing, and Fast Access. Mainly for storage purpose Private Cloud (pCloud) is preferable to store secure information. In this paper we work on storage of information securely and retrieval of data efficiently. Our main objective is how efficiently we reduce time in retrieving of data in storing secure information. We have implemented a proxy re-encryption and data striping technique for storage and retrieving purpose. The results are been taken placed by using .NET technology and output is shown in graph analysis.

**Keywords**: Private Cloud, Proxy re-encryption, Data Striping, .NET

## Introduction

This paper proposes a secured threshold proxy re-encryption server and integrates it with a decentralized erasure code such that a secure distributed storage system is formulated for processing big data. Using a striping technique, we distribute the database to a number of cooperative peers, and leverage their computational resources to process cPIR queries in parallel. In this method multiple users can interact with the storage system. Users can upload their data in to the distributed storage system. The distributed storage system not only supports secure and robust data storage and retrieval, but also lets a user forward his data in the storage servers to another user without retrieving the data back. This makes the ownership data unused and secured during the time of retrieval. The maintechnical contribution is that the proxy re-encryption scheme supports encoding operations along with a key over encrypted messages, as well as forwarding operations over encoded and encrypted messages. The content in the database will be in the encrypted format by striping the data in to various databases. So that even intruder can't able to access the big data even they access the database. The encrypted data will become unused even the data obtained by the intruder. This makes the system so stronger. This paper deals with fully integrates encrypting, encoding, and forwarding. The application can be shown in both cloud servers as well as in local host as per the environment. The storage and robustness are more flexible with the users. So that user will authorize the sender request to generate the key. Using the authorized one time key sender can access the encrypted file in decrypted format at once. The key will become invalid after one use. This is method is implemented for secured data forwarding. During data forwarding a proxy server will be created virtually to access the encrypted data from the sender side. The original data from the cloud server will be transmitted to the proxy virtually. This makes less traffic and the original big data content will not get affected during the time of data transaction. After the transaction the proxy server will be deleted along with the data. So that data will be safe always in the cloud storage servers.

In this paper we are carrying out work by taking college department concept in real time based application. We can also develop for organization, hospitals, library, working areas etc.,

## Literature Survey

The main objective of the survey paper is to develop a Computational Private Information Retrieval (cPIR) protocols on cloud architecture using erasure code for secured data forwarding. These protocols are too costly in practice because they invoke complex arithmetic operations for every bit of the database. Basically cloud storage architecture will have a collection of storage servers with higher end configuration which will provides

ISSN: 2277-9655
Impact Factor: 1.852

long-term storage services over the Internet and also for the cloud storage system. Here storing and retrieving the data in a third party's cloud system and public auditing scheme causes serious problems and conflict over data confidentiality during the data transactions. Whenever third party big data storage will involved with the cloud server this conflict will occur naturally. Even thou there are various methods are available to overcome this problem like cryptography, key encryption and etc. But general encryption schemes protect data confidentiality during the transaction, but along with this process the main drawback will, it limits the functionality of the storage system. This is because; a few operations only supported over encrypted data. These methods will cause failure. In order to constructing a secure storage system that supports multiple functions is challenging when the storage system is distributed and has no central authority. In our paper we are not using any central authority but going to retrieve block of information in secure and efficient response time.

## Modules

Since we are taken college department based application in our first module we need to create a users. We separate our user into two. One is Owner (student) and Master (staff). We divide our module as

1. Ownership
2. Data Striping
3. Proxy re-encryption
4. Analysis.

**Ownership**

The public cloud environment is the IaaS/PaaS Infrastructure or Platform as a Service that we rent from Linux (IaaS) or Microsoft (PaaS). Both are enabled for web hosting. Then, your SaaS stack will run under your Internet environment most likely in a virtualized one on your own equipment which would make it private. In this paper we specialize in private cloud technology. Here we execute in a cloud environment. If strict security requirements go public or hybrid and if not, try the public or community cloud environment. So that here we are implementing a web services for the output purpose as well as the environment will be shown in actual while hosting the application. So finally SaaS can be fully utilized in cloud environment as IaaS/PaaS. Thus we formed cloud environment

This is the initial module of this paper. Data ownership refers to both the possession of and responsibility for information. Ownership implies power as well as control. The control of information includes not just the ability to access, create, modify, package, derive benefit from, sell or remove data. Data ownership is the act of having legal rights and complete control over a single piece or set of data elements. It defines and provides information about the rightful owner of data assets and the acquisition, use and distribution policy implemented by the data owner. Here Data owners can create a login and they can upload their own files in the cloud Storage.

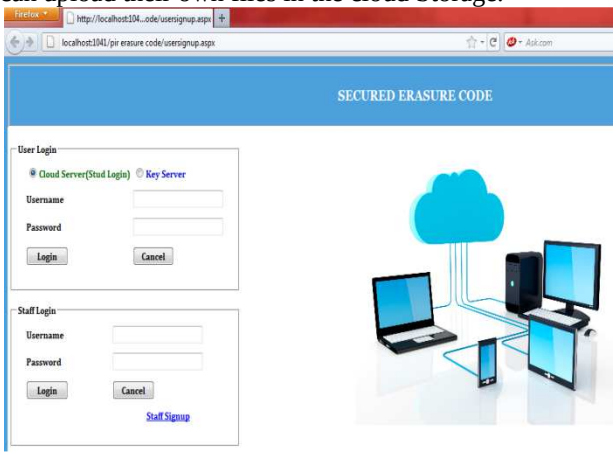


**Fig 1: user's creation**

In this the master need to login in first and create a owners access permission login and distribute the login information to the owners. Owners can access their cloud storage to upload the assignments (data) to the master only after they get login information from their masters. When assignments (data) are been uploaded by owner to cloud space the master can view their assignments (data) only their department basis. But access is denied for the other owners in same or different departments to view others data. To gain access each owner must get access permission key.

**Data Striping**

Data Striping technique one of the advance technique in cloud is like splitting data in to different database also known as distributed database. Here we are considering a single document file or presentation file is been split into different locations so that even a intruder cannot find in which location the other part of pages is located. When a owner upload their document the files is split before splitting they are been encrypted for security. Now the files are encrypted as also they are been located in different location in cloud database where high security is reached.

ISSN: 2277-9655
Impact Factor: 1.852

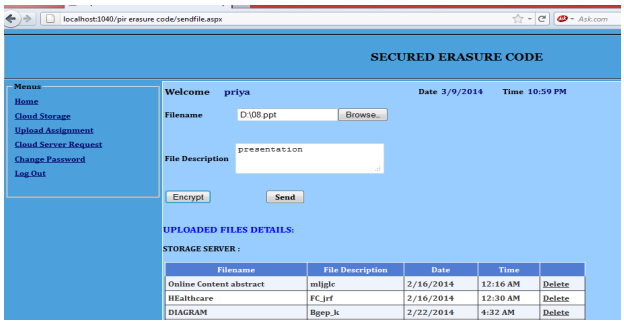


**Fig 2: Files upload**

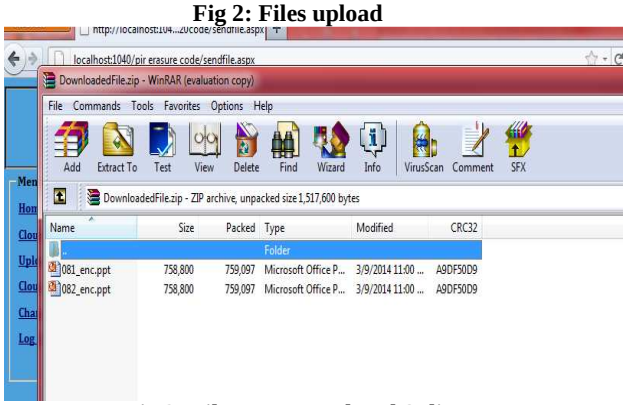


**Fig 3: Files Encrypted and Split**

## Proxy re-Encryption

Here the construction of the cloud will be more secured in peer to peer network. The encryption methods are follows in the next module. The two biggest concerns about cloud storage are reliability and security. Basically, a cloud storage system can be considered to be a network of distributed data centers which typically uses cloud computing technologies like virtualization, and offers some kind of interface for storing data. To increase the availability of the data, it may be redundantly stored at different locations. In general, all of this is not visible to the user mostly data will be in the encrypted format. Many cloud storage providers are active on the market, offering various kinds of services to their customers. But here we are using a personalized cloud store server for both big data and secured erasure code. The storage server will be unique which has been distributed into much system for easy access of data. It contains only the encrypted data of the data owners.

It is one of the advanced encryption model which works on both real system and virtual systems. This works more efficient on cloud systems. Proxy re-encryption schemes are cryptosystems which allow third-parties (proxies) to alter a cipher text which has been encrypted for one party, so that it may be decrypted by another. Proxy re-encryption schemes are similar to traditional symmetric or asymmetric encryption schemes. It allows a message recipient (key holder) to generate a re-encryption key based on his secret key and the key of the delegated user. This re-encryption key is used by the proxy as input to the re-encryption function, which is executed by the proxy to translate cipher texts to the delegated user's key. Asymmetric proxy re-encryption schemes come in bi-directional and uni directional varieties. Proxy re-encryption schemes allow for a cipher text to be re-encrypted an unlimited number of times. Proxy re-encryption should not be confused with proxy signatures, which is a separate construction with a different purpose.

In this when the user need to access the data to reduce the time to get access permission proxy key the users are divided into three types: Genral User, Recommended user, Most Recommended user.

***Genral User:***

Genral user is new user. When this type of user access data directly it is denied and permission should be granted from authorized user

***Recommended User***

This type of user can access the data directly by getting key from the user without any request. But key should directly get from authorized user they comes to this type of user when they access data minimum 10 times.

**Highly Recommended User**

Highly recommended user will be always alive who will have highest priority since they always stay alive. For this type of user cloud will automatically give permission to access.

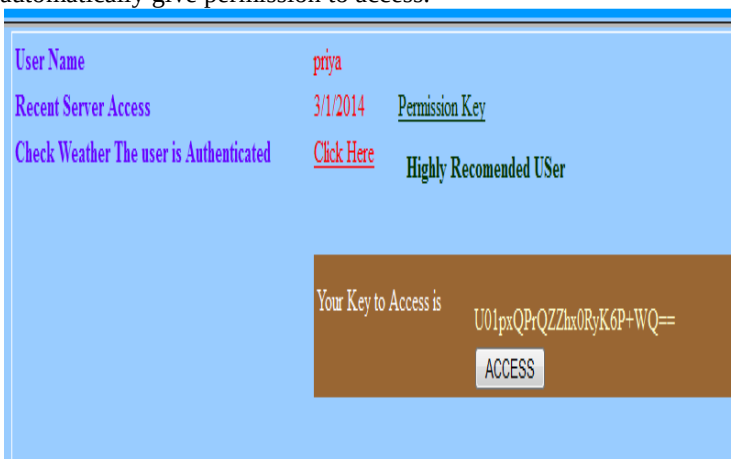


**Fig 4: Accessing the File by Permission**

## Analysis

The files then are downloaded by using downloading link. The result of the data retrieving is been shown below. In this we are calculating time between key generated to view the file i.e. request time and the time when the user responded. We have taken results for highly recommended user since they stay alive. Here the calculation is done comparing

ISSN: 2277-9655
Impact Factor: 1.852

CPU processor speed and time in seconds. It takes only limited time limit to retrieve when we see bar graph.

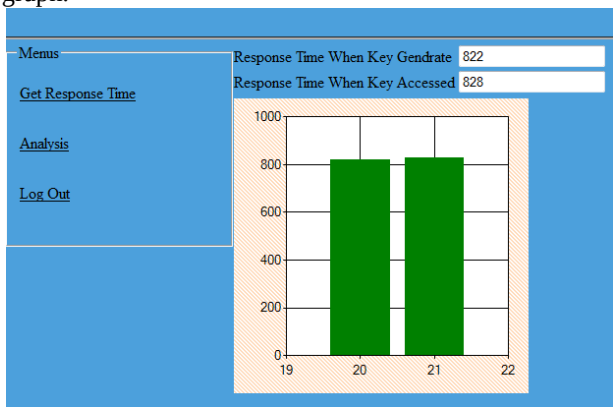


**Fig 5: Response Time**

## Conclusion

Private Information Retrieval is one of the important parts in Cloud. In this paper we have discussed about retrieval of private information from the cloud. We securely store the block of data by encryption and stripping technique and retrieve the data without delaying in response. To reduce the waiting time from authorized user we also discuss the idea about three users. While we implement this in organization then we need to consider about making much more key stronger. Since we going to keep this data in cloud, cloud will manage the data's. By distributed database data will be robust and safe.

## *Reference*

[1] *Stavros Papadopoulos, Spiridon Bakiras, and Dimitris Papadias, "pCloud: a distributed system for practical PIR" in IEEE transactions on dependable and secure computing, vol. 9, no.1, 2012.*

[2] *Hsiao-Ying Lin, Wen-Guey Tzeng, "A Secure Erasure Code-Based Cloud Storage System with Secure Data Forwarding" in IEEE Transactions on parallel and distributed systems, vol.23, no. 6, june 2012*

[3] *Alex Huth and James Cebula, "Basics of Cloud Computing" in the Carnegie Mellon University. Produced for US-CERT, a government organization, 2011*

[4] *Andris Ambainis "Upper bound on the communication complexity of private information retrieval" in* Proc. International Colloquium on Automata, Languages, and Programming (ICALP '97), *1997.*

[5] *Benny Chor, Oded Goldreich, Eyal Kushilevitz and Madhu Sudan "Private Information Retrieval" in,* Proc. Symp. Foundations of Computer Science (FOCS '98), *1998.*

[6] *Boris Tomas and Bojan Vuksic "Peer to Peer Distributed Storage and Computing Cloud System" in, International conference on Information Technology Inferences, 2012*

[7] *Christian Cachin, Silvio Micaliy and Markus Stadler "Computationally Private Information Retrieval with Polylogarithmic Communication" in the* Proc. International Conference Theory and Application of Cryptographic Techniques (EUROCRYPT '99), *1999.*

[8] *David A Patterson, Garth Gibson, and Randy H Katz, "A Case for Redundant Arrays of Inexpensive Disks (RAID)" published by in* Proc. ACM SIGMOD '88, *1988.*

[9] *G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.L. Tan, "Private Queries in Location Based Services: Anonymizers Are Not Necessary,"* Proc. ACM SIGMOD '08, *2008.*

[10] *Ion Stoica, Robert Morris, David Karger, M. Frans Kaashoek and Hari Balakrishnan "Chord: A Scalable Peer to peer Lookup Service fo Internet Applications" in* Proc. ACM SIGCOMM '01, *2001.*

[11] *Kuyoro S.O., Ibikunle F & Awodele O, "Cloud Computing Security issues and Challenges" in the International Journal of Computer Networks (IJCN), 2011.*

[12] *L. Sassaman, B. Cohen, and N. Mathewson, "The Pynchon Gate: A Secure Method of Pseudonymous Mail Retrieval,"* Proc. Workshop Privacy in the Electronic Soc. (WPES'05), *2005.*

[13] *Qin Liu, Chiu C.Tanb, Jie Wub, Guojun Wang "Cooperative private searching in clouds" published By in, Journal of Parallel Distributed and Computing, 2012.*