**Australian Journal of Basic and Applied Sciences**, 9(11) May 2015, Pages: 727-730

ISSN:1991-8178

**Australian Journal of Basic and Applied Sciences**

Journal home page: www.ajbasweb.com

# A Method for Secure Storage and Sharing of File for Space Reduction in Cloud

Saranya R., Uma Priyadarsini P.S. and Silviya Nancy J.

*Department of Computer Science and Engineering, Saveetha School of Engineering, Saveetha University, Chennai - 602105, India.*

**ARTICLE INFO**

***Article history:***
*Received 12 March 2015*
*Accepted 28 April 2015*
*Available online 1 June 2015*

***Keywords:***
*cloud storage, access control, fuzzy authorization (FA), secure cloud storage.*

**ABSTRACT**

Cloud storage is widely used for storing large data from various users at different place, but cloud storage provider has a lot of issues like data missing, security, access control and confidentiality. To overcome these issues, fuzzy authorization scheme in cloud storage is adopted. In this technique to enable an application registered with one cloud account to access data files in own cloud account. The new proposed system permits the fuzzy authorization to improve the scalability and flexibility of data file sharing by taking benefit of the one to one correspondence between Linear Secret Sharing System. The security of the fuzzy authorization is shown under the Diffie-Hellman statement. In this system user can register the profile detail in their own cloud, in this cloud having the application for pdf merging, taking files from different storage area of files with OTP authenticated to a third party account. After accessing the third party file then merging the pdf file of own cloud to third party file into one file of pdf and stored into own cloud space with base64 encrypted form. In this proposal, the authorization can realize fuzzy logic between heterogeneous clouds with security and effectiveness.

**© 2015 AENSI Publisher All rights reserved**.

**To Cite This Article:** Saranya R., Uma Priyadarsini P.S. and Silviya Nancy J.., A Method for Secure Storage and Sharing of File for Space Reduction in Cloud. ***Aust. J. Basic & Appl. Sci.,*** *9(11): 727-730, 2015*

## INTRODUCTION

Now a day's cloud storage is used for storing data of user such as photos, videos, files, music, and contact list, etc. All these data stored in cloud storage within the account. Many users are storing their data in Google Drive, Dropbox, icloud, JustCloud etc., due to less memory space of their physical devices. But this has many issues of security, confidentiality, integrity, access control of data and trust between user and storage providers. So, we implement an idea of using a fuzzy authorization technique which permits to improve the scalability and flexibility of data file sharing by taking benefit of the one to one correspondence between Linear Secret Sharing System. In this paper, we are showing the pdf merged access control, data owner his/her data pdf files stored in cloud storage like a Google Drive, Dropbox storage which is top cloud storage providers. After upload the files in cloud storage, owners have to merge pdf files with help of PDFMerge application. This application has been already there in own cloud than files taking from third party accounts with OTP access control of user accounts. The final output of merged PDF files encrypted base64 form and stored in own cloud.

Current issues of cloud storage including the owner of the file and trust between them is more challenging. Another issue is that more than one access token or secret key is required for access control of files. Let us assume one person have hundreds of pdf file there in cloud storage than person want to merge his file, first person want to download his file in cloud storage then after merged the pdf with application provider (Available:http://www.pdfmerge.com). At file need a secret key for accessing the pdf than only merged the pdf. That is a very difficult scenario. To makeover it, we are using fuzzy authorization in cloud storage. In our system secret key create only one user not every pdf file so here access control is reduced compared to last system. The user profile is encrypted in ABE (attribute base encryption) form, every attribute of user are encrypted like as user name, city, address, phone number be encrypted to become into CP-ABE (cipher text Policy attributes base encryption). If their own cloud wants to access the third party user's account firstly decrypts the CP-ABE (Bethencourt, J., 2007) of user profile then access the third party account and after merge the pdf files in easier way.

Cloud storage of fuzzy authorization is more secure file sharing with high flexibility, confidentiality and scalability by modifying CP-ABE (Yong Cheng, ). The term of fuzzy is attribute discrepancy tolerance of authorization or secret key

**Corresponding Author:** Saranya R., Department of Computer Science and Engineering, Saveetha School of Engineering, Saveetha University, Chennai, India.
Tel: +91 9487752343; E-mail: saranya22061989@gmail.com

related to set one attribute to another set done with proper adjustment of two set of attribute.

***Common issues in cloud storage access:***

Cloud-based system incorporates much natural vulnerability; however, they require not keep a business client from exploiting its economies and adaptabilities. Here are the five most essential approaches to address information security in cloud-based capacity bases.

***Data loss:***

When disk drives of cloud storage providers are dying or corrupt then there is a loss. If some condition data owner has it backup files but encrypted file be store in cloud storage than it will be difficult to recover data due loss of data corrupt at data centre of cloud storage. And sometime data loss could occur purposely in the event of a malicious attack (http://www.informationweek.com/cloud/infrastructure-as-a-service).

***Key Management****:*

1) General issues:
a) Keys are stolen
b) Keys are vulnerable to attacks.
2) Availability
3) Management of all keys
a) Single point of failure
b) To handle lots of keys for need scale linearly.[5]

***Snooping****:*

Documents can be defenceless in the cloud; however there are additionally dangers amidst of information transmission. Entirely talking, scrambled records don't have to be sent over a safe line – this adds up to twofold encryption. Anyway, it is best to expect the most exceedingly bad and prepare for any measure of snooping by just sending and recovering information over a protected line. This forestalls against somebody seeing cloud metadata. Information and metadata ought to be totally misty on the wire and in the cloud. Nothing – no filenames, timestamps – ought to be decipherable once it leaves your pr.

***Credentials****:*

Indeed, even scrambled information can be powerless if your documents are pooled in with those of another client. Access to a given pool of capacity is in view of accreditations, and on the off chance that you are lumped together with another arrangement of clients and offer the same certifications, there is a hazard that one of them could get those qualifications and access your information. They would not have the capacity to interpret it, accepting it is encoded; however they could erase the records. By securing your own particular exceptional accreditations, in any case, your records will be divided. Nobody else will have the capacity to log into your record and erase your information.

***Performance:***

A solid security procedure is a need; however it ought to not truly affect execution. Encryption of information being sent to the cloud, and decoding of records got back to from the cloud, ought to happen with almost no effect on the client experience. In a perfect world, it would happen without the client perceiving a thing (http://www.nasuni.com/blog).

***Existing Model System:***

In this system have three models. These models are user registration, upload file in cloud storage and last is merging files with application service providers. First user registration his/her profile data in cloud storage account and upload his /her files is uploading in cloud storage. Than after download his file for merging the file, the pdf file merger is used by online of application provider. This pdf merger merged the pdf file and stored into the cloud storage.

*Issues in Existing System:*

The important issue is that more than one access token or secret key is required for access control of files. Let us assume one person have hundreds of pdf file there in cloud storage than person want to merge his file, first person want to download his file in cloud storage then after merged the pdf with application provider. At file need a secret key for accessing the pdf than only merged the pdf. That is very difficult to person than only we are using fuzzy authorization in cloud storage, in our system secret key create only one users not every pdf file so here access control be reduced compared to last system.

***Proposed system model:***

***Registration & File Upload:***

In this phase the users register and upload their file into cloud. For registration user has to fill all their personal details. Without user register into cloud they can't upload their files. Here we are using two types of cloud one is for cloud storage and other is for cloud storage, application provider. Once user registered their details into the cloud he/she can upload the file. Here PDF files are only uploaded into the cloud.

***Profile View & PDF File Merge in Same Cloud:***

In this phase user can view own profile and merging their uploaded PDF files. In that user account, cloud will show the user details and file which he/she uploaded. After viewing the account user will merge the files in the cloud. For merging file user select PDF files which the user has uploaded. Merged file can be displayed into the user page. Here merging and display PDF files are all done in single cloud.

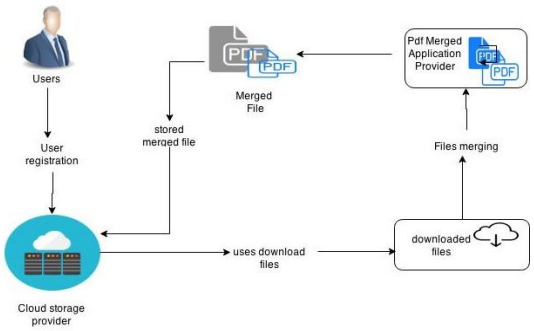


**Fig. 1:** Existing model.

***Merge in Different Cloud without Third-Party:***

Here merging PDF files are done based on different cloud files. So far we are done merging only in a single cloud. But here user merge file from other cloud. For merging other cloud file, users enter into the cloud. Once particular user entered, cloud will generate OTP for that user. After he/she entered the OTP into the cloud, cloud verifies the OTP. If it is verified, cloud will list out the PDF files that he/she uploads. After user getting the list they can merge files.

Owner of data encrypts the data with random symmetric key KE and it convert into CP-ABE form. Data owner can hide CP-ABE text into his application cloud. There is no need to storage in cloud storage.

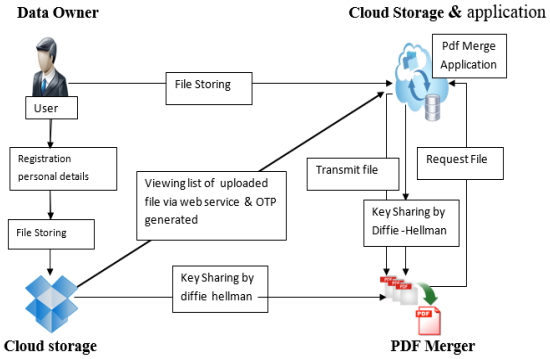


**Fig. 2:** Proposed System Model.

***Benefits of the System:***

***The following benefits are:***

a) No need trust between them users and application service providers.

b) When the file is modified and re-encrypted than FA automatically withdraw the right access of files.

c) FA can access the files of owner with different cloud storage.

d) Analysis of security show that FA provides more security, integrity, secures access control and confidentiality of outsourced data.

e) It provides more efficiency of cloud storage data.

***Conclusion:***

FA transmits flexible file sharing between an owner who stores his/her data file in one cloud storage party and other cloud which have own application of merged pdf. These files shared through Diffie-Hellman assumption, for accessing the files of the cloud storage party by matching his/her public and private key than only file is merged otherwise files not accessed. FA provides a security of data, confidentiality, secure access control and integrity.

## REFERENCES

Shasha Zhu and Guang Gong, 2014. "Fuzzy Authorization for Cloud Storage" in Ieee Transactions On Cloud Computing, 2-4.

[Online].Available:http://www.pdfmerge.com/

Bethencourt, J., A. Sahai and B. Waters, 2007. "Ciphertext-policy attribute- based encryption," in Proc. IEEE Symp. Security Privacy, 321–334.

Worst Cloud Security Threats http://www.informationweek.com/cloud/infrastructure-as-a-service.

"cloud security the challenges with key management-in-the- cloud-and-everywhere-else" https://www.joyent.com/blog/"

The Nasuni cloud storage blog"http://www.nasuni.com/blog.

Yong Cheng, Jiangchun Ren, Zhiying Wang, Songzhu Mei, "Re-encryption Optimization in CP-ABE Based Cryptographic Cloud Storage"

Sushmita Ruj, Milos Stojmenovic, Amiya Nayak "Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds"

Wang, C., S.S. Chow, Q. Wang, K. Ren and W. Lou, 2013. "Privacy-preserving public auditing for secure cloud storage," IEEE Transaction on Computers, 62(2): 362–375.

Zhu, Y., H.Wang, Z. Hu, G.J. Ahn, H. Hu and S.S. Yau, "Dynamic audit services for outsourced storages in clouds,"