ISSN: 0975-766X
CODEN: IJPTFI
Research Article

Available Online through
www.ijptonline.com

GROUP KEY MANAGEMENT SECURITY CONTROL IN CLOUD

Diwakar kumar[1], Ramya.G.Franklin[2]
Department-MCA, Faculty of Computing, Sathyabama University, Chennai-600119,Tamilnadu, India.
Email: diwakarkumar0038@gmail.com

Received on 23-02-2016 *Accepted on 17-03-2016*

Abstract

The user of cloud service could easily store the data in cloud storage by using remote services and can access the high quality demanded services and application by sharing the configuration of computing resources pool without making any burden of maintenance for local storage of data. However the user doesn't have longer possession of physical data outsourced link within the protection of data integrity in cloud system over a formidable issues, and the resources of constrained computing.

An enhanced and better technique has been proposed over the enforcement delegation by controlling the fine grained access over the cloud for minimizing the issues in side of data owner's process, while data owner is assuring the confidentiality of data through cloud services. The paper has proposed two layers cryptography technique which addressing the requirements for the encryption and decryption processes. The paper is presenting the enhancement with flexible and effective technique by explicating the support of data for ensuring the user's correctness in cloud. Particularly, it considers the task to allow threshold based proxy re-encryption technique for client of cloud to verifying the integrity of data in cloud storage. The proposed technique has avoided the technique to use additional cloud storage functionality.

Keywords: OTP (One Time Password), Multi-Cloud, Data Splitting, Group Key Management, Cloud Storage.

1. Introduction

The cloud technology adoption is for representing the major concern of storage environment for privacy and security. The confidentiality of user's data is needed to get protected by the user privacy. The traditional approach of encryption is not more sufficient for assuring the record confidentiality from server of cloud [1]. Recently, there are most of the organization is performing the ACPs (Access Control Policies) which means to express the user property terms by identity attribute [2].

Fine Grained Access Control: The ability of Fine Grained Access Control has ability to resolve the issues over attributes and accessing of individual data. The Fine Grained Access Control is allowing implementing the accessing selection over policy specification based on the content. The system is making a different access yielding access for the users set and allowing the specification over the rights of users [3].

Delegation

The technique of delegation is transmitting the accessibility of user’s right. The delegation might get occur in two individual forms. Those are mentioned below:

1. User delegation
2. Administrative delegation.

The administrative delegation is allowing the administrative to allocate the right of access for users and required a process of user accessing for capability of the access right [4]. Furthermore, the delegation administration is often operating a durable and long-lived delegation operation temporarily and tends to purpose specifically [5]. The flexible process of the delegation is accessing the delegation models which identify the three consecutive cases while the delegation process is necessary. Firstly, id any individual is being absent from their job and carry out some job. Secondly, the delegation process allows decentralizing the authority operations [6]. The study over the data security process is preserving the environment delegation in which the policy is providing the policies over the data [7]. The broadcasting of the encryption scheme is allowing the sender to designate the cipher text in the group which could decrypt the data content within decryption key. So, nobody from out of the group will be able to read the content or data [8].

To enhance the services over the cloud system, these papers presents the erasure correcting code for distribution process of the data into several storage files, where uploaded data is being split into three parts and stored in the three different storage space, and provide data dependability and redundancies.

The proposed system is providing the communication and storage facility as well, the Homomorphic token is being utilized within the distributed verification process for the data of erasure data, and this proposed scheme achieves the data error localization and storage correction.

1.2 Related Work

The author [9] has proposed a technique that been used widely for the real world application security. However the cryptography has been applied over the dynamics data of cloud for the performance problems. The policy based dissemination content is being and described as another approach that being introduced in the year of 2010.

The authors [10] have introduced the delegated control of accessing for dissemination security over the documents of XML. The cryptography technique has been used for security of data while it publishing. The cloud accessing control is being explored with similar research concept by different author [12].

The authors [11] have proposed a technique for broadcasting the encryption mechanism that being applied on the service of broadcasting. The concepts over oblivious certificate could be used for data security. Similarly, the security mechanism within fashion attribute is providing the grouping management of key attribute.

The authors [13] have presented the delegation over public cloud for privacy preserving which afford the efficient key management in grouped scheme for supporting the ACPs. This functionality is assuring the data confidentiality for privacy preserving for cloud users when it delegating the privacy preservation for cloud users by enforcement accessing control over the cloud system. They had proposed two layer of encryption is being performed by the data owner and second encryption is done by the cloud.

The authors [14] have proposed a security mechanism as group key management towards attribute. The accessing control system is permitting the fine grained attribute based system for several users group that being identified within attribute set. The collaborative application is being protected which could be providing the attribute based system flexibility for maintaining the distribution keys. The system is supporting the monotonic accessing control policy by using the attributes set, while changing the groups, operation over rekeying which is not affecting the secret information for members group or preventing the need of schemes for establishment of expensive channel for communication.

The authors [15] have presented a novel concept over the de-duplication scheme of client-side for sharing and storing the outsourced data with public cloud towards privacy and security over the public cloud environment. The originality of their proposal is having twofold. The first part is ensuring the better confidentiality over unauthorized users. Second, the integration of accessing privileges for metadata file, where unauthorized user could decode the encrypted file within private keys.

3. Materials and Methods

3.1 Overview

The proposed architecture and technique is providing the data splitting over storing into the cloud. There are two layer enforcement is there for helping the data uploading and reducing the load of data while storing the data on cloud. The proposed concept is providing a better idea for several updating process, data modification and locations. The system is going through the comparison of additional phase from existing system. It also providing the several function on the basis of data splitting or data decomposition from various cloud stores which being finally retrieved within decryption keys.

3.2 Overall Architecture

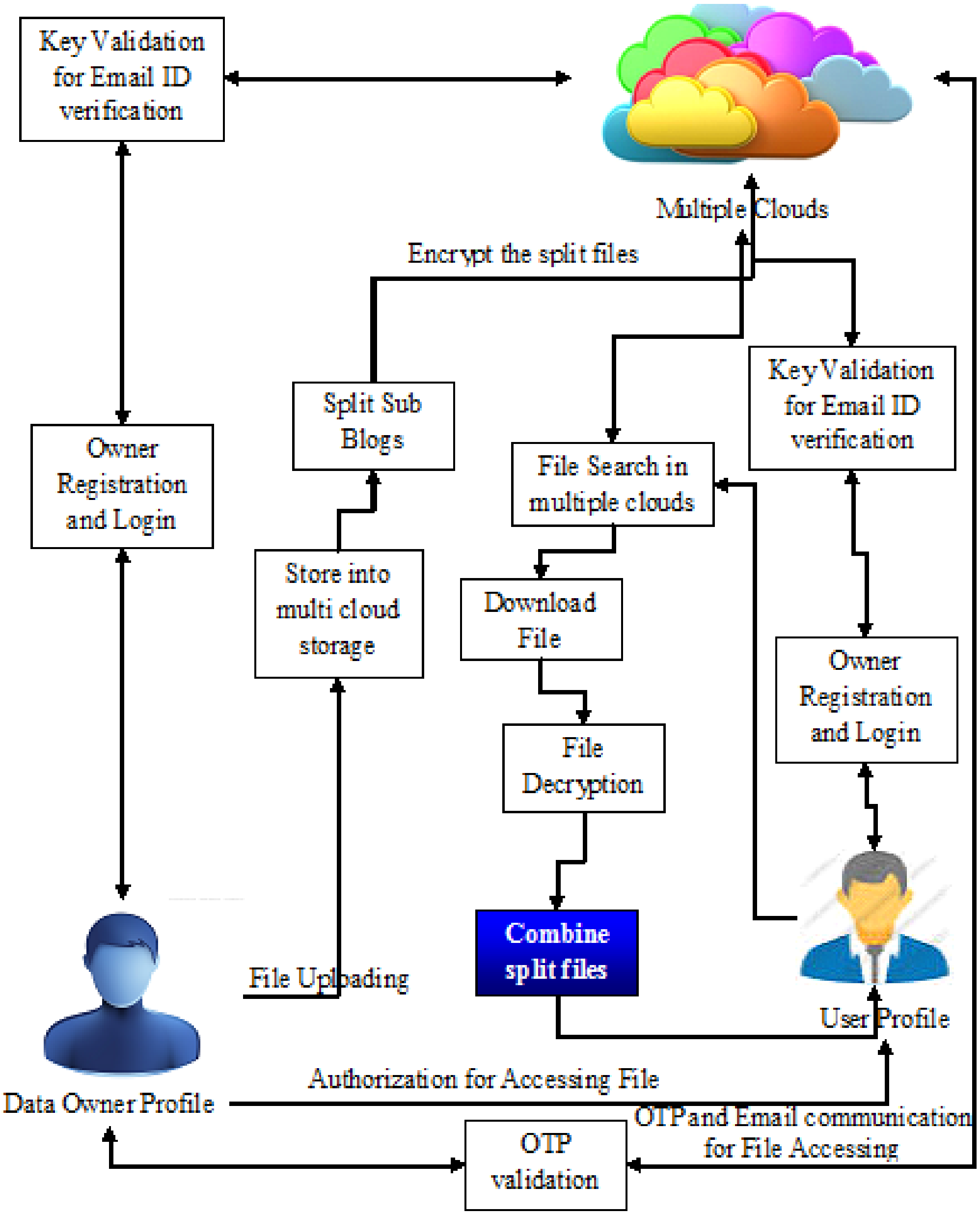

Key Validation for Email ID verification
Multiple Clouds
Encrypt the split files
Split Sub Blogs
Key Validation for Email ID verification
File Search in multiple clouds
Owner Registration and Login
Store into multi cloud storage
Download File
Owner Registration and Login
File Decryption
Combine split files
File Uploading
User Profile
Data Owner Profile
Authorization for Accessing File
OTP and Email communication for File Accessing
OTP validation

Figure-1: Overall Architecture.

3.3 Data Encryption and Uploading

The process of encryption and data uploading is based on the ACPs of data owner for hiding the content or data and then uploading to cloud by splitting within shared information publicly. The information is being shared publicly by using key gen technique, where it generating the secret key the secret key is allowing the user or ACPs to access the sensitive data or information by consideration of data owner.

3.4 Token Registration

The users are registering their identity for getting the secret key for decrypting the content or data. The identity tokens are allowing the user to register the key and accessing the data.

The user registration is identifying the related owner within the tokens and making a registration in cloud with different tokens for privacy manner.

3.5 Cloud Storage

The model of cloud storage is the enterprise storage over network, which storing the data in the storage of virtual pool the commonly being hosted by agents or third party. The companies of cloud services host or operate the large centers of data, where people requires their content to get lease or buy the hosted content or data based storage.

The operators of data center are processing the virtual resources accordance of customer requirement and exposing the pools of storage. The safety of the files depends upon the hosting companies, and on the applications that leverage the cloud storage.

3.6 Data Downloading and Decryption

The users are downloading the encrypted data from cloud storage and decrypting two times. Initially, the decryption is being done on the cloud server side and seconds it done on the user side. The cloud server is generating the tuple for public information is being used over the drive for OLE key and data owner have to generate the public tuple information by deriving the ILE key within GKM keygen technique.

3.7 Group Key Management

The approaches of the selective ABAC within fine-grained services is for identifying the dataset items for that accessing policy to control the encryption and it applies the same encryption key. The data within the encryption could get uploaded over the cloud and every user be getting the secret keys set for accessing the data and the user will be accessing each data or content based on the organized policies. The Group Key Management (GKM) is approaching the two major requirements:

a) The data confidentiality protection over cloud and from cloud.

b) The accessing policy over control for fine-grained is enforcing the data users.

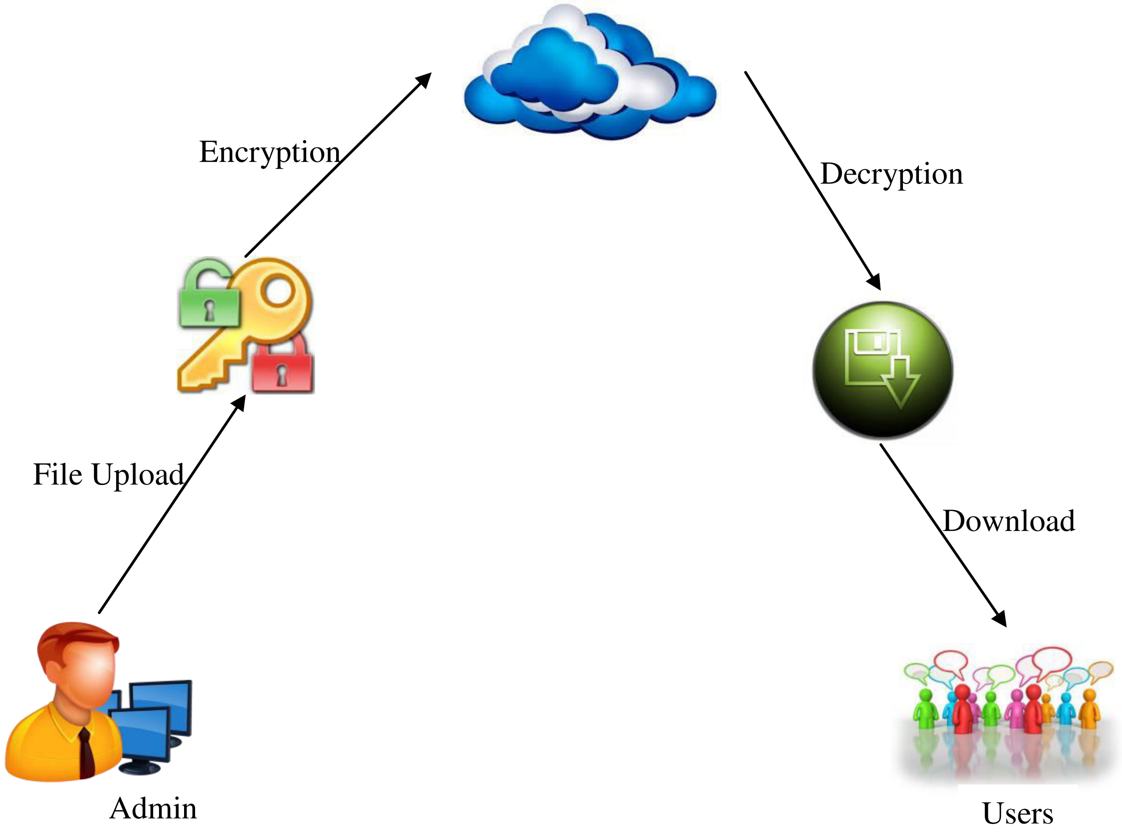


Figure 2: Group Key Management Architecture.

3.8 Encryption Broadcasting

The process of broadcast encryption is introducing the solution of issues that encrypting the content or message and broadcasting to the system user subset. The users subset could be get change dynamically. The broadcasting scheme of the encryption is consisting the message encryption by authentication of separate users and broadcast the entire encrypted message. There are better scheme for encryption broadcasting which reducing the parameters:

- The server processing time for message encryption is towards the authorized users.
- The decryption processing time for authenticated users.
- Broadcasting the message size.
- The size of storage at both authenticated users and server.

3.9 Algorithm

The process of keygen algorithm is producing the cryptography keys for encrypting the data or content and decrypting the content or data as well.

RSA Algorithm

1. Pick two large prime numbers p and q. These are secret.

2. Calculate n = pq

3. Pick another number e such that e and (p-1)(q-1) are relatively prime.

4. The numbers n and e make up your public key. Publish them!

5. Calculate d such that ed = 1 mod (p-1)(q-1) {i.e. d = e^{-1} mod (p-1)(q-1) }

6. The number d is your private key..

Encrypt message m via c = m^e mod n

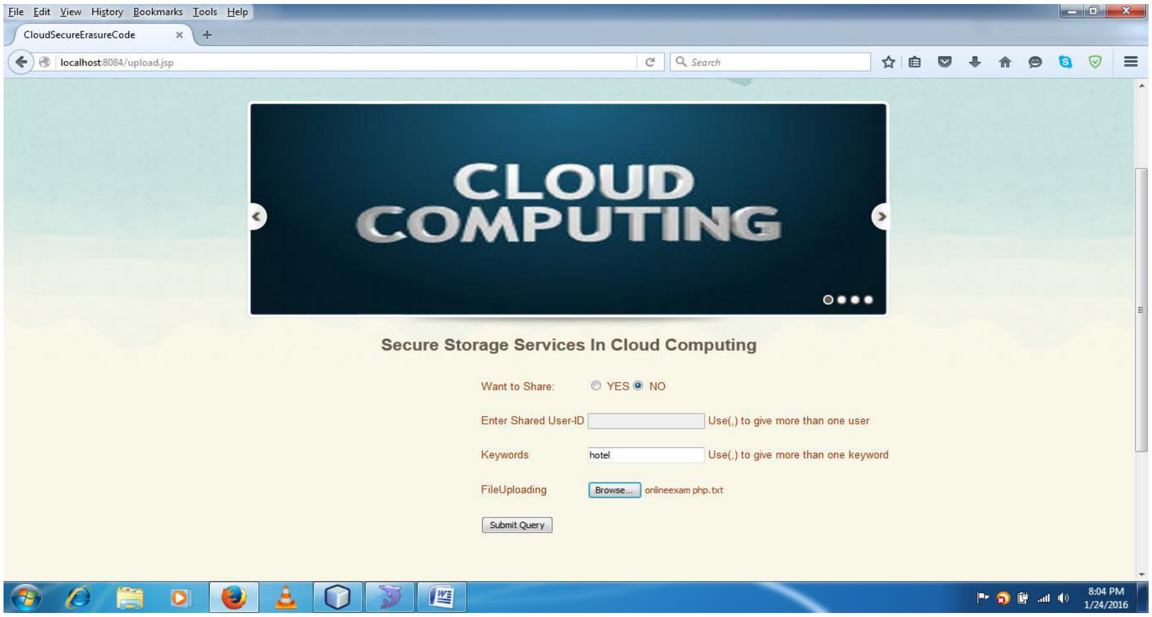
Decrypt the cipher text c via m = c^d mod n

4. Result and Discussion

4.1 System Setup

The proposed system implements with following system configuration such as Intel(R) Pentium (R) processor, G2020 CPU with 2.90 GHz clock speed, Windows 7 Professional operating system and 4 GB RAM

Data Uploading Process


File Edit View History Bookmarks Tools Help
CloudSecureErasureCode
localhost:8084/upload.jsp
Search
CLOUD COMPUTING
8:04 PM
1/24/2016

Secure Storage Services In Cloud Computing

Want to Share: ○ YES ● NO

Enter Shared User-ID Use(,) to give more than one user

Keywords hotel Use(,) to give more than one keyword

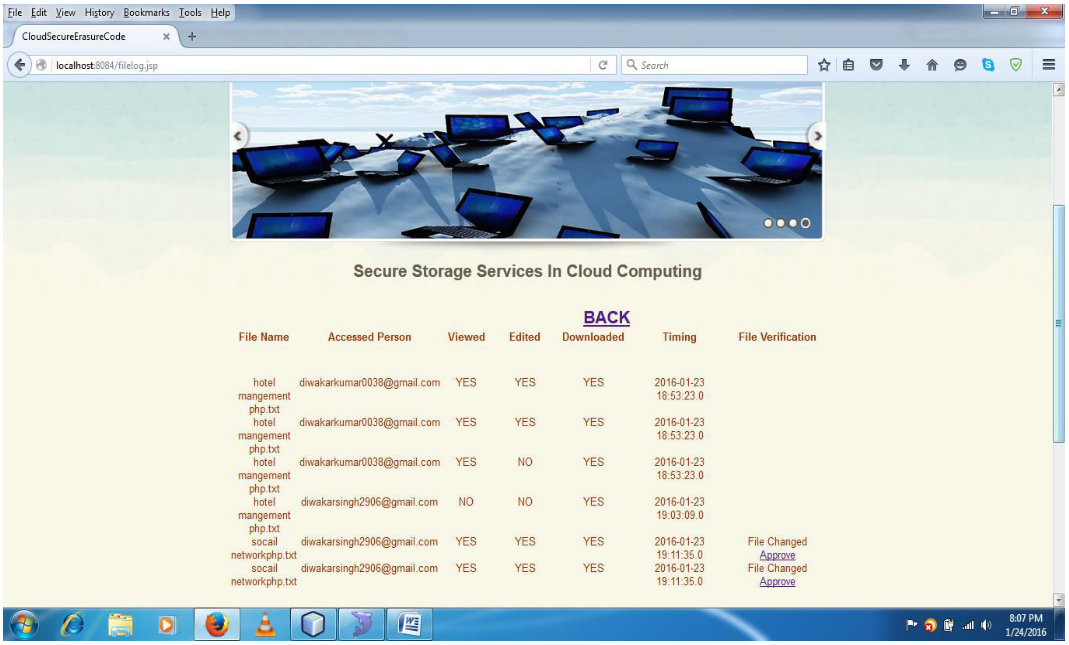
FileUploading Browse... onlineexam php.txt

Submit Query

Figure 3: Data Uploading.

The above mentioned figure 3 is presenting the data uploading process over the cloud storage, where user or data owner is setting the privilege for their uploaded data like sharing option or authentication for share the file with any specific user.

Uploaded Data Modification


File Edit View History Bookmarks Tools Help
CloudSecureErasureCode
localhost:8084/filelog.jsp
Search
8:07 PM
1/24/2016

Secure Storage Services In Cloud Computing

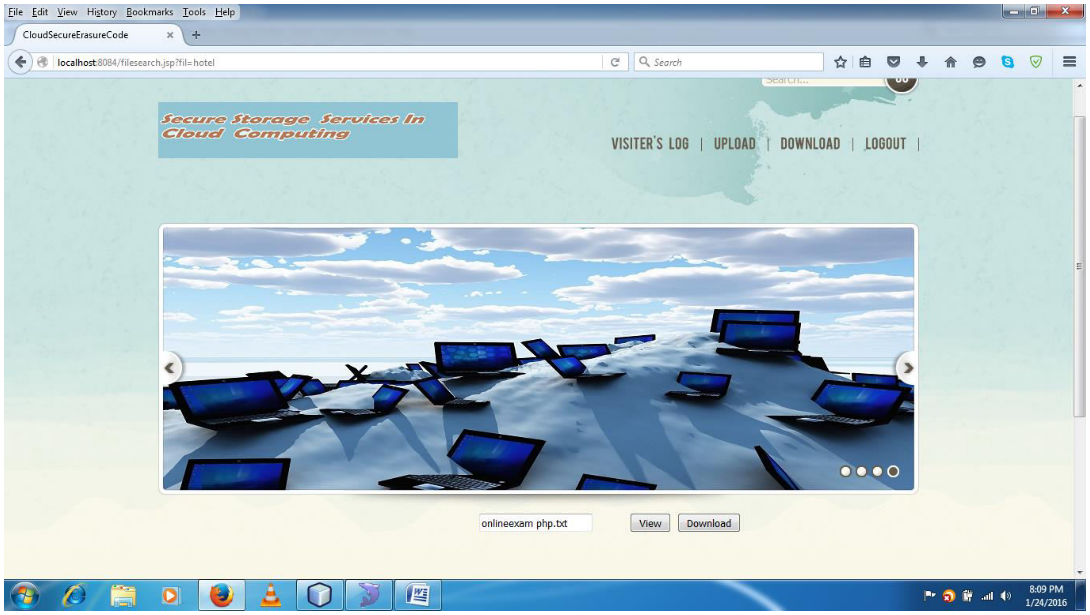
BACK

File Name	Accessed Person	Viewed	Edited	Downloaded	Timing	File Verification
hotel mangement php.txt	diwakarkumar0038@gmail.com	YES	YES	YES	2016-01-23 18:53:23.0	
hotel mangement php.txt	diwakarkumar0038@gmail.com	YES	YES	YES	2016-01-23 18:53:23.0	
hotel mangement php.txt	diwakarkumar0038@gmail.com	YES	NO	YES	2016-01-23 18:53:23.0	
hotel mangement php.txt	diwakarsingh2906@gmail.com	NO	NO	YES	2016-01-23 19:03:09.0	
socail networkphp.txt	diwakarsingh2906@gmail.com	YES	YES	YES	2016-01-23 19:11:35.0	File Changed Approve
socail networkphp.txt	diwakarsingh2906@gmail.com	YES	YES	YES	2016-01-23 19:11:35.0	File Changed Approve

Figure 4: Uploaded data Modification Privilege.

The above mentioned figure 4 is presenting the complete information of the stored data in cloud. The data modification is also being verified in this section by the data owner, which allowing the modification of stored data in cloud from different users.

File View Process

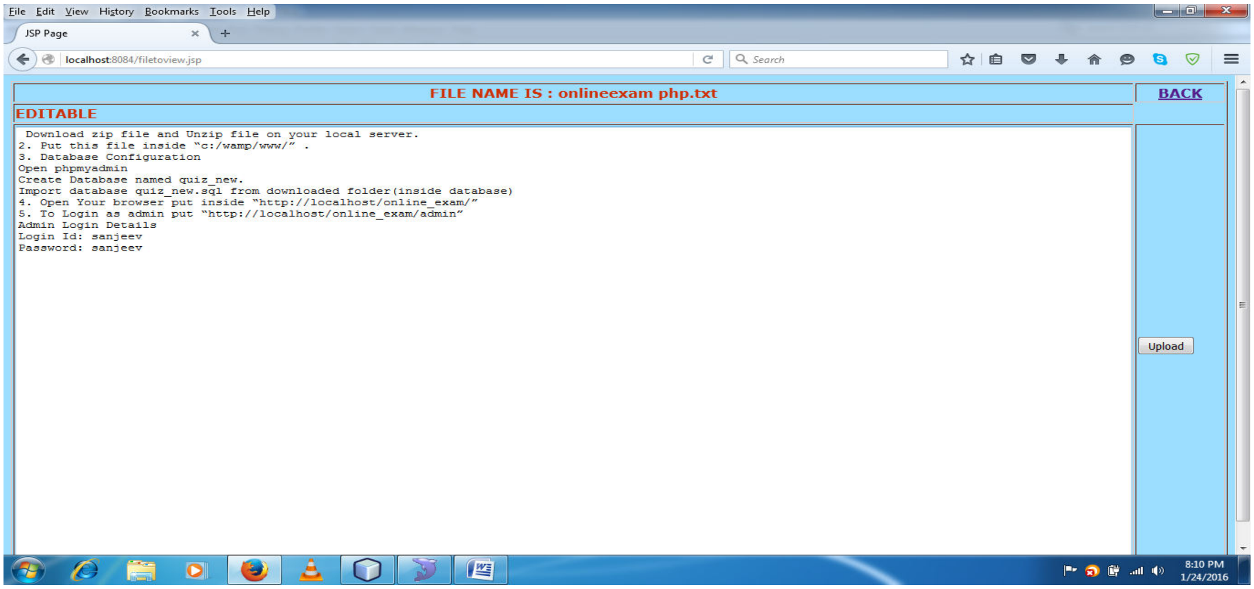

File Edit View History Bookmarks Tools Help
CloudSecureErasureCode
localhost:8084/filesearch.jsp?fil=hotel
Search
Secure Storage Services In Cloud Computing
VISITER'S LOG | UPLOAD | DOWNLOAD | LOGOUT |
View
Download
8:09 PM
1/24/2016

onlineexam php.txt

Figure 5: File View.

The above mentioned figure 5 is presenting the process of data view and downloading of the stored data by the data or file name. The data could be get downloaded by the users after viewing the file.

File updating Process



File Edit View History Bookmarks Tools Help
JSP Page
localhost:8084/filetoview.jsp
Search
BACK
Upload
8:10 PM
1/24/2016

FILE NAME IS : onlineexam php.txt

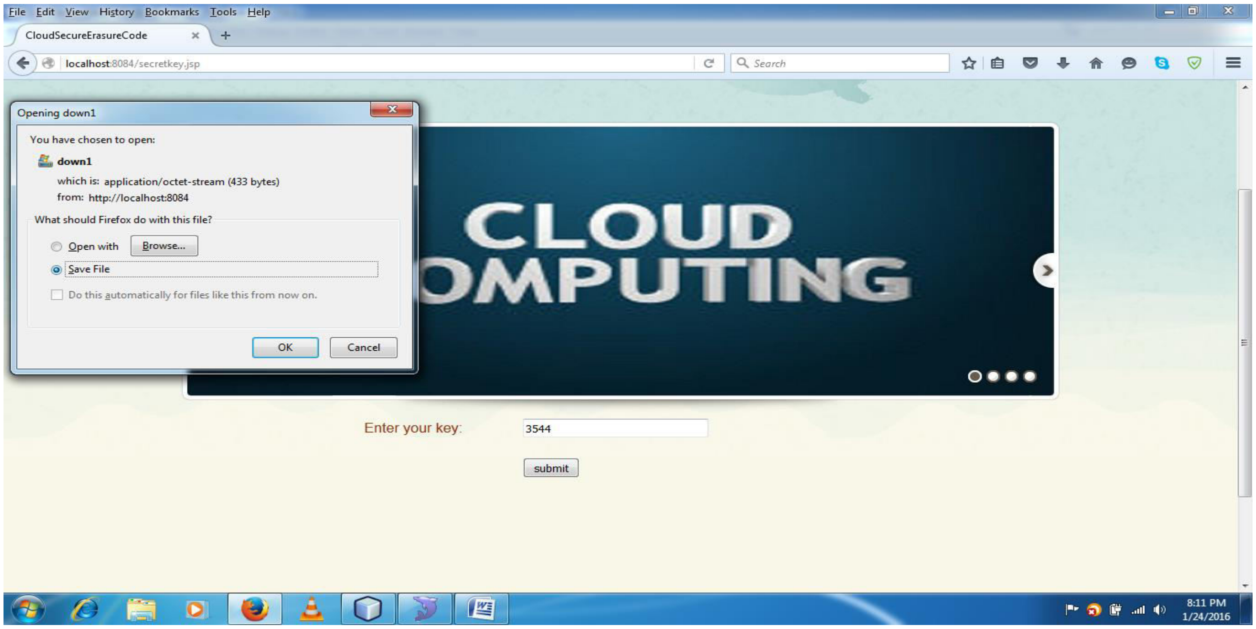
EDITABLE

```
 Download zip file and Unzip file on your local server.
2. Put this file inside "c:/wamp/www/" .
3. Database Configuration
Open phpmyadmin
Create Database named quiz_new.
Import database quiz_new.sql from downloaded folder(inside database)
4. Open Your browser put inside "http://localhost/online_exam/"
5. To Login as admin put "http://localhost/online_exam/admin"
Admin Login Details
Login Id: sanjeev
Password: sanjeev
```

Figure 6: File Viewing and Updating.

The above mentioned figure 6 is presenting the file editing, modifying, and updating process from collecting the data through cloud. The data or content could get edited and stored into the server.

Data Downloading Process



File Edit View History Bookmarks Tools Help
CloudSecureErasureCode
localhost:8084/secretkey.jsp
Search
CLOUD
OMPUTING
8:11 PM
1/24/2016

Opening down1

You have chosen to open:

down1

which is: application/octet-stream (433 bytes)

from: http://localhost:8084

What should Firefox do with this file?

○ Open with [Browse...]

● Save File

□ Do this automatically for files like this from now on.

[OK] [Cancel]

Enter your key: 3544

[submit]

Figure 7: Data Downloading Process.

The above mentioned figure 7 is presenting the process of data downloading, where user have to provide the secret key for the verification process and then user will be able to download the data.

5. Conclusion

The proposed technique is providing better and enhanced result over the scenario of cloud storage system for data uploading and downloading. The data owner is verifying the different users to modify the stored data in cloud. The proposed technique is splitting the content in several parts and uploading to the cloud storage within encryption process. While any user is looking for accessing the stored file could get or search the file by searching within the file name and will be able to modify the content after downloading, where user have to get a secret key for downloading the file or user could suggest a modification in the content. But the file modification will be done within the data owner privilege.

5.1 Future Work

The future work might be considering over the load-balancing in multi cloud server within maximum storage capacity and better accuracy for several users.

References

1. M. Nabeel and E. Bertino, “Privacy preserving delegated access control in public cloud,” in IEEE Transactions on Knowledge and Data Engineering, 2014.

2. M. Nabeel and E. Bertino, “Privacy preserving delegated access control in the storage as a service model” in IEEE International Conference on Information Reuse and Integration (IRI), 2012.

3. M. Nabeel and E. Bertino, “Privacy preserving policy based content sharing in public clouds,“In IEEE Transactions on Knowledge and Data Engineering, 2012.

4. M. Nabeel, E. Bertino, M. Kantarcioglu, and B. M. Thuraisingham, “Towards privacy preserving access control in the cloud,” in Proceedings of the 7th International Conference on Collaborative Computing: Networking, Applications and Work sharing, ser. Collaborate Com ’11, 2011, pp. 172–180.

5. M. Moniruzzaman, M.S. Ferdous and R. Hossain, “A study of privacy policy enforcement in access control models,” In proceedings of 13th International Conference on Computer and Information Technology (ICCIT). Dhaka, Bangladesh, pp. 352 – 357, 2010. DOI:10.1109/ICCITECHN.2010.5723883.

6. M. Jafari, P. W. L. Fong, R. Safavi-Naini, K. Barker, and N. P. Sheppard, “Towards Defining Semantic Foundations for Purpose- Based Privacy Policies,” In proceedings of the First ACM Conference on Data and Application Security and Privacy (CODASPY), San Antonio, Taxas, USA, 213-224, 2011.

7. M. Nabeel and E. Bertino, “Towards attribute based group key management,” in Proceedings of the 18th ACM conference on Computer and communications security, Chicago, Illinois, USA, 2011.

8. X. Zhang, S. Oh and R. Sandhu, “PBDM: a flexible delegation model n RBAC,” In proceedings of the eighth ACM symposium on Access control models and technologies (SACMAT), New York, NY, USA, pp. 149–157, 2003.

9. N. Shang, M. Nabeel, F. Paci, and E. Bertino, “A privacy preserving approach to policy-based content dissemination,” in ICDE ’10: Proceedings of the 2010 IEEE 26th International Conference on Data Engineering, 2010.

10. M. Nabeel and E. Bertino, “Privacy preserving delegated access control in the storage as a service model,” in EEE International Conference on Information Reuse and Integration (IRI), 2012.

11. S. Coull, M. Green, and S. Hohenberger, “Controlling access to an oblivious database using stateful anonymous credentials,” in Irvine: Proceedings of the 12th International Conference on Practice and Theory in Public Key Cryptography. Berlin, Heidelberg: Springer-Verlag, 2009, pp. 501–520.

12. S. D. C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, “Over-encryption: Management of access control evolution on outsourced data,” in Proceedings of the 33rd International Conference on Very Large Data Bases, ser. VLDB ’07. VLDB Endowment, 2007, pp. 123–134.

13. M. Nabeel and E. Bertino, “Privacy preserving delegated access control in public cloud,” in IEEE Transactions on Knowledge and Data Engineering, 2014.

14. M. Nabeel and E. Bertino, “Towards attribute based group key management,” in Proceedings of the 18th ACM conference on Computer and communications security, Chicago, Illinois, USA, 2011.

15. Nesrine Kaaniche, Maryline Laurent,” A Secure Client Side Deduplication Scheme in Cloud Storage Environments” 6th International Conference on new Technologies, Mobility and Security year 2014.

Corresponding Author:

Diwakar kumar*,

Email: *diwakarkumar0038@gmail.com*