VOL. 12, NO. 17, SEPTEMBER 2017 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

SECURE AUDITING OF SHARED DATA IN A PRIVATE CLOUD USING EMAIL NOTIFICATION

Anusha N., Abilash G. and Balaji T.
Department of Computer Science and Engineering, Sathyabama University, Chennai, India
E-Mail: abilashranade@live.com

ABSTRACT

Files in the cloud have chances of getting misused by a hacker or a malicious person. In order to solve this issue, we introduce a method where the owner of the file in a cloud sent an email notification regarding the file modification. The file is uploaded by a group owner in a private cloud, users have access to register for the group and download the required file. An auditor is assigned to check for any modification that has been to made to the file .The files are encrypted and kept initially, slight changes made in the encrypted content is also detected by the auditor and the file owner is notified about the modification via email.

Keywords: cloud computing, data De-duplication; email notification, data leakage cloud storage.

1. INTRODUCTION

Cloud computing is one of the developing technology in the current times .It has made the life simple by its way of accessing a file anywhere and anytime. The requirement of a cloud computing technology is simple i.e. an internet connection and a device to access internet. It is known for it online tools through which one can actually access application without installing it on your computer. The cloud computing provides an enormous amount of storage in which a user can store his data, open his files anywhere also with any device. The technology has come all its way and now, one can share his files to others.

File sharing in cloud has become one of the popular features in the field of cloud. Sharing files via email has its own demerits since the size of should be limited. A user who needs to share his music, images, videos, documents etc with other person can easily share it via cloud and there is a enormous storage capacity which one can make utilise of it. The file sharing can be one to one or one to many based on the users requirement. It has helped the corporate world in the modern days by making things simpler. Let us consider a scenario where a project manager has share a load of files to his fellow mates who are working from different places. Now, it is tedious process when the manager sends unique files to his each member in his project .The file sharing technology in cloud helps him to create a group for his team, make his fellow mates to register for the group and share his files to the team. Hence, the team members can download their required files and the file is also confidential since the members are only from the team.

Data duplication and illegal file accessing are major problems in the cloud. When multiple copies of the same data are saved in the cloud, it becomes a hard time to recognize the original data also the wrong information may be delivered to the users. The method of illegal accessing of files in the cloud and making changes to file can also results in confusions. Such actions are done by a hacker or malicious person to make problems to an organisation or a company. Hence an auditor is needed to look after the files and notify the file owner when any modifications are made to the file.

2. LITERATURE SURVEY

[1] Proposed identity-based data outsourcing (IBDO) where the proxies are given permission to access the files but there is no explanation for user revocation since the files can also by misused the group members themselves. [2] The files are audited using TPA (Third Party Auditor), there are chances that the files maybe access by them also the data confidentiality is lost [3] Users need to obtain the secret keys from the TPA (Third Party Auditor) every time when they download the file which is tedious and time consuming process [4] Employed PDP (Provable Data Possession) and Signature algorithm, where the data is cut in to blocks. Since the data is cut to pieces, it arises a problem when one piece of data is corrupted and will have impact on the whole file [5] Used Resigned techniques, where the information should be confidential to the group and cannot be public. [6] Proposed fuzzy fingerprint method and protocol, which is tedious and this method can have only one owner and the owner cannot share the data. [7] Used secret sharing scheme, the system uses unique keys for the files that is being uploaded, a small change/edit in the secret keys can end up showing another file which is closely related to the original file. [8] Proposed security of duplicate-check token Method, It allows files duplication and duplicated files are stored along with the original ones which is a memory consuming process [9] uses SecCloud and SecCloud+ process which does not inform the file owner when duplication or modification is done to the file. [10] Introduced a method where the integrity of data can be verified with the public keys of existing users only. [11] Proposed a technique called secret sharing Technique where instead of using a encryption technique the files are split and kept in independent cloud servers. When any one of the multiple cloud servers fails crashes, the data cannot be accessed [12]It uses a method of file encryption while storing the data in the cloud also the same can be decrypted only by an valid user and the data is not accessible any other person . [13] The keys are assigned to a file based on different privileges and TPA is assigned to monitor the files which can end up in losing data confidentiality. [14] The system uses Proof Of Ownership

(POW) and the two factor authentication-one time password (2FA-OTP) Where the system does not inform file owner when duplication or modification is made to file [15] Hashing technique is complex, it is aimed only to reduce auditing time and reduce memory consumption but cannot share files to others. [16] Uses SecCloud and SecCloud+ the duplication is allowed and data is saved cloud storage which is a drawback because cloud storage cannot be infinite [17] In case of any duplication or modification in the data, the owner is not notified about it. [18] Same copy of a file is kept in different cloud servers for security which is suitable for files with less size but it cannot be reliable since it is a memory consuming technique. [19] Proposed an examination identified with single and multi-cloud security and locations possible explanations which was able to inform the owner about the modifications made in the file after data integrity check. [20] in this proposed method when a staff overcomes their privileges, then the intimation will be given to the user instead the information should be intimated to the administrator for the recovery process.

3. PROPOSED METHOD

In the proposed method, the files are created under a group name and each group will consist of respective group owner who uploads the files. The system consist of two main entities namely group owner and group users. The group owner creates a group with a 16bit key for his files and uploads them under the same name. Now, the group user registers for the respective groups and gain access to download the files. The group owner has authority to remove an user from the group if he needs to. An auto generated email containing the secret key of the respective group (assigned by the group owner) is sent to the users who register for the group. The users need to type-in the 16-bit secret key while downloading the file (which will be sent to their mail). The files are encrypted once uploaded in the cloud. The cloud system is monitored by an auditor and he checks the file in regular intervals .An hacker or any malicious person tries to modify or misuse the files the respective group owner is notified via email by an auditor about the modification or mismatch.

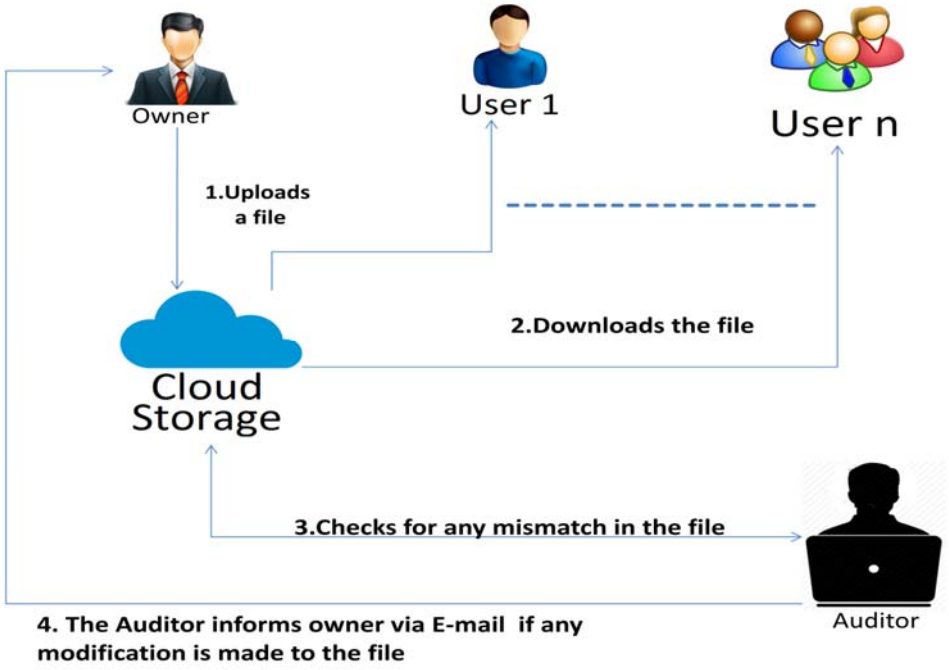

Figure-1. Public auditing system associated with multiple owners.

A. Registration and file uploading

It is the first phase of the proposed cloud system; it allows an owner to register by giving a group name and also allows to upload his files. As shown in Figure-2 the users who needs to join the group should undergo user registration and gain download acess to the file.

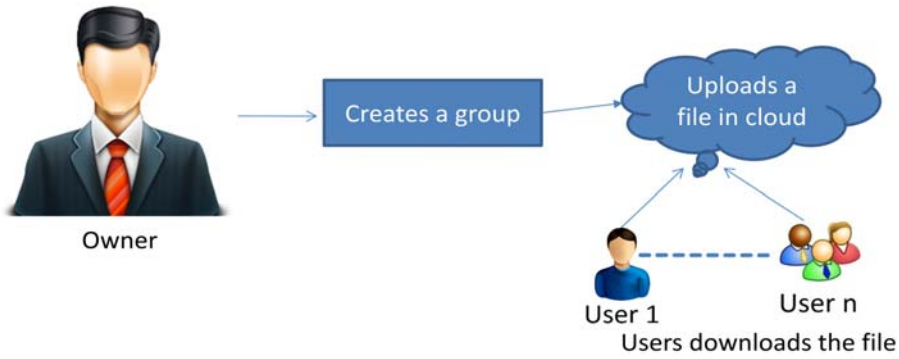

Figure-2. Registration and file uploading.

B. Auditing

An auditor's job is to monitor the files whether any modifications is done or not. As shown in the Figure-3, the auditor job is check the individual files and see to that any if any modification or illegal access has made to the file. If he finds out any mismatch in the file, the owner will be alerted.

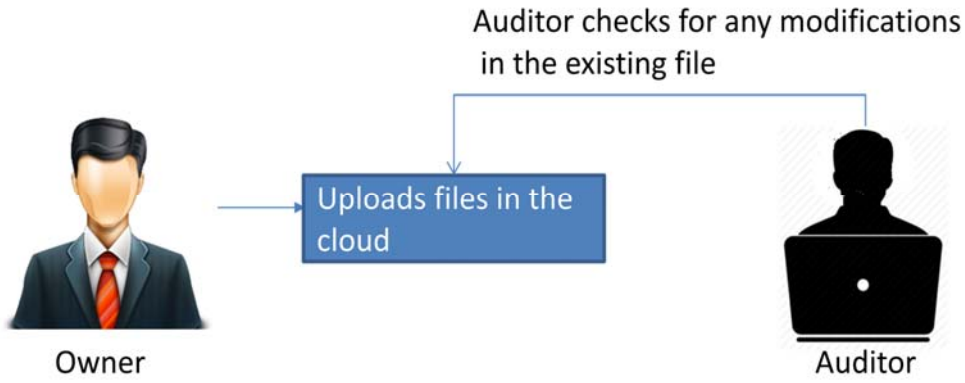

Figure-3. Illustration of auditing technique.

C. E-mail notification

An e-mail notification system reacts based on the audtior's result. When auditor acknowledges any modification or mismatch in the files that is uploaded in a cloud, it will send an email notification to the respective file owner stating that his file uploaded in the cloud is corrupted or modified.

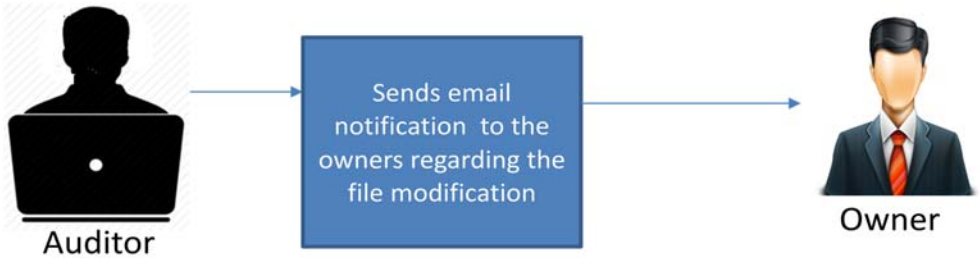

Figure-4. E-mail notification system.

4. RESULTS AND DISCUSSIONS

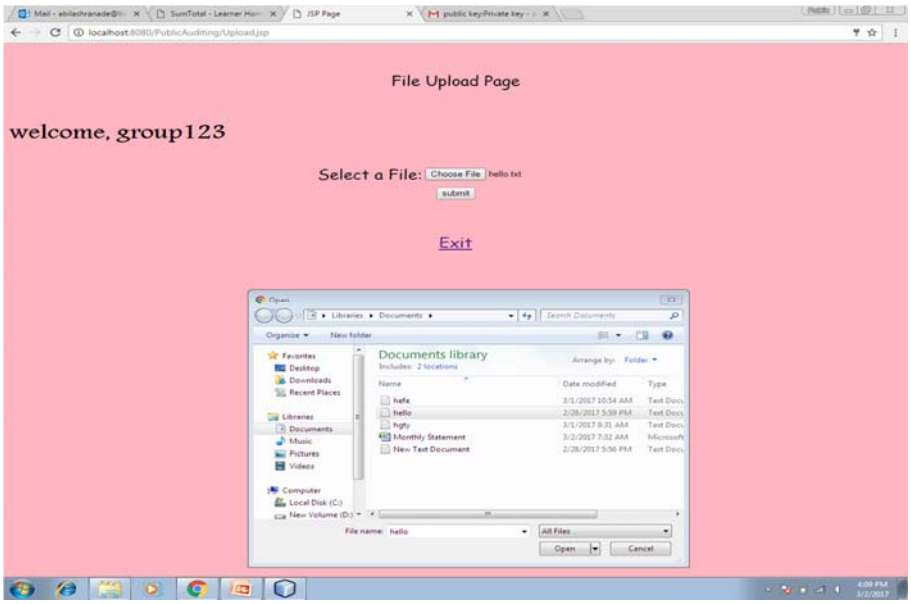

Figure-5. Uploading file into the group.

In Figure-5, the owner uploads the file into the group, which can be downloaded by the user who are registered for that group. In order to download a file, the user must have a secret key which will be sent to the user via E-mail by the file owner.

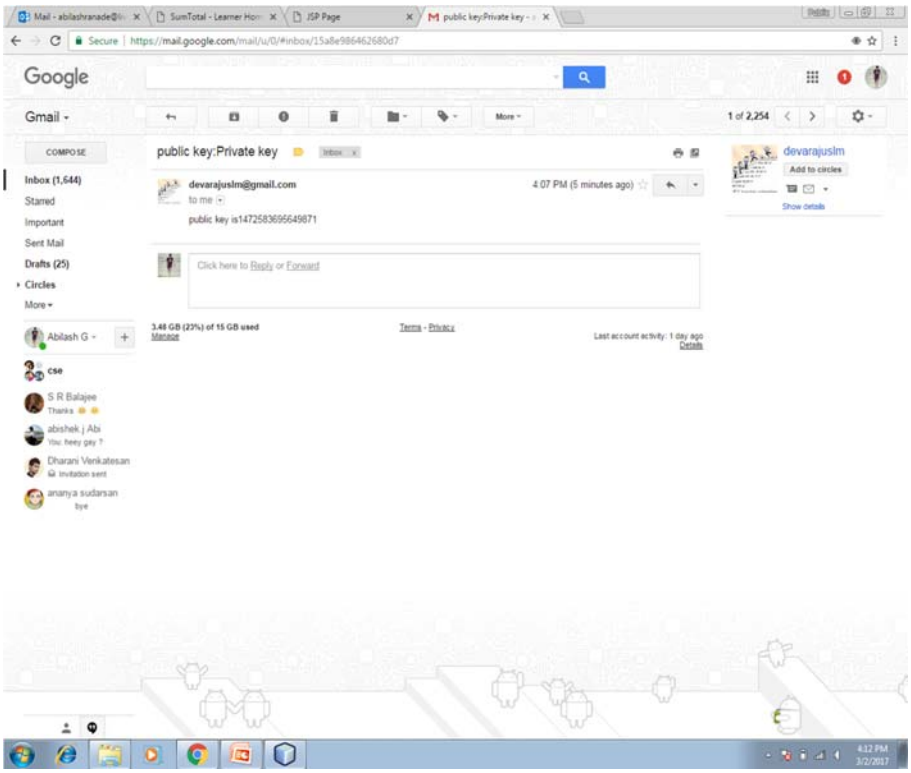

Figure-6. E-Mail notification to the user along with the public key.

In Figure-6, we can see the secret key allotted by owner for his file, which the user gets in his E-Mail after the registration process. Only with this secret key, he can have access to the files that have been uploaded into the group.

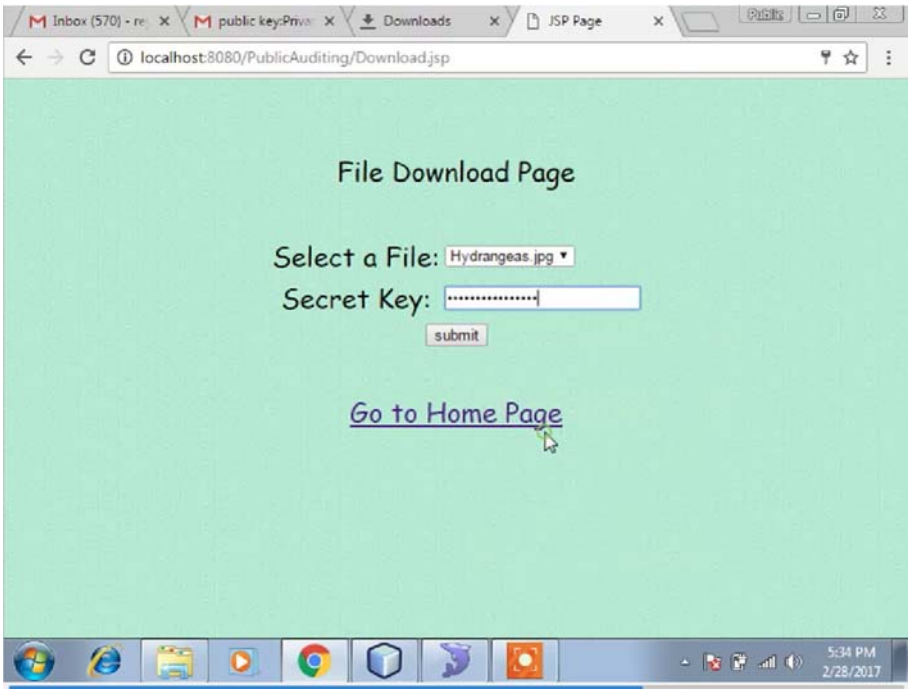

Figure-7. File accessing or downloading process.

In Figure-7, here the user has to enter the secret key which he got in his E-Mail from the owner of the group during the registration process. Once the user selects the file and enters the secret key, he will have access to download the file.

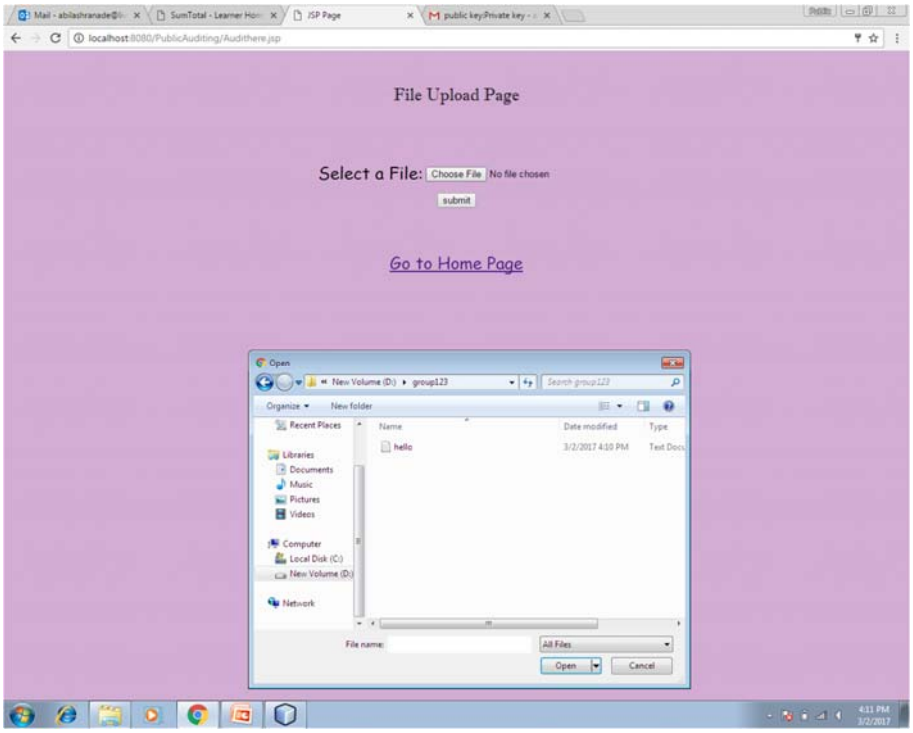

Figure-8. File auditing process.

In Figure-8, the auditor checks the file for any modification during the auditing process. If the file has no modification, there will be a message stating there in no modification in the file, whereas if there is a modification

in the file, the auditor will send a notification to the group owner via E-Mail, stating that his file has been corrupted or modified.

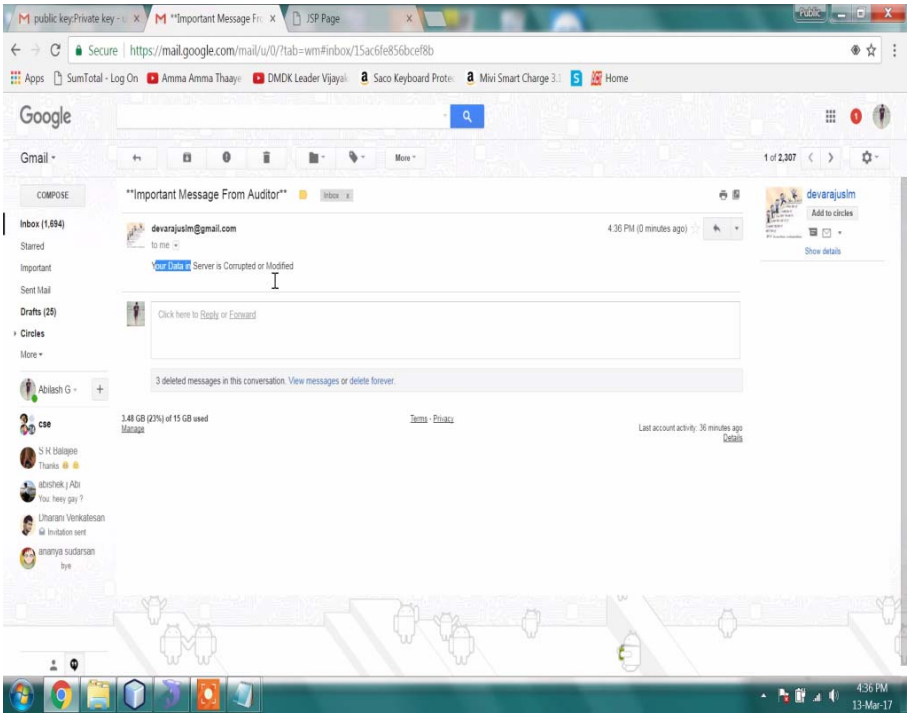

Figure-9. E-Mail notification from the auditor.

In Figure-9, since the file in a group that has been modified by a malicious person, Auditor finds out the mismatch and informs the respective group owner about the modification.

5. CONCLUSIONS

The notion of the proposed system is to eliminate data leakage and illegal access to the confidential data .It is designed in a way that data owner is notified when any duplication or modifications are done to the data. The system also helps the file owner to take control over his file by removing his group members when they themselves try to misuse it. Future enhancement can be done by allowing ownership for two or more users for a single file and also allowing them to make changes in the file by getting permission from the actual file owner.

REFERENCES

[1] Yujue Wang, Qianhong Wu, Member, Bo Qin, Wenchang Shi Robert and H. Deng, Jiankun Hu. 2016. Identity-Based Data Outsourcing with Comprehensive Auditing in Clouds. IEEE Transactions on Information Forensics and Security. pp. 1-13.

[2] Sonal Shukla, Brahmdutt Bohra and Surendra Yadav. 2016. Public auditing services in cloud networks for data sharing including privacy preserving. IEEE.

[3] Jia Yu, Kui Ren and Cong Wang. 2016. Enabling Cloud Storage Auditing With Verifiable Outsourcing of Key Updates. IEEE transactions on information forensics and security. 11(6): 1362-1375.

[4] Boyang Wang, Sherman S. M. Chow, Ming Li and Hui Li. 2014. Privacy- Preserving public auditing for shared data in Cloud. IEEE transactions on cloud computing. 2(1): 43-56.

[5] Boyang Wang, Baochun Li, and Hui Li. 2015. Public Auditing for Shared Data with Efficient User Revocation in the Cloud. IEEE transactions on services computing. 8: 92-106.

[6] Xiaokui Shu, Danfeng Yao and Elisa Bertino. 2015. Privacy-Preserving Detection of Sensitive Data Exposure. IEEE transactions on information forensics and security. 10(5): 1092-1103.

[7] Yongge Wang. 2015. Privacy-Preserving Data Storage in Cloud Using Array BP-XOR Codes IEEE transactions on cloud computing. 3(4): 425-435.

[8] Jin Li, Yan Kit Li, Xiaofeng Chen, Patrick P.C. Lee, and Wenjing Lou. 2015. A Hybrid Cloud Approach for Secure Authorized Deduplication. IEEE transactions on parallel and distributed systems. 26(5): 1206-1216.

[9] Jingwei Li, Jin Li, Dongqin Xie and Zhang Cai. 2016. Secure Auditing and Deduplicating Data in Cloud. IEEE transactions on computers. 65(8): 2386-2395.

[10] Kai He, Chanhe Huang, Jiaoli Shi and Jinhai Wang. 2016. Public Integrity Auditing for Dynamic Regenerating Code Based Cloud Storage. IEEE 2016 on Computers and Communication (ISCC).

[11] Meghana Vijay Kakde and Prof. N.B. Kadu. 2016. Survey Paper on Deduplicating Data and Secure Auditing in Cloud. International Journal of Computer Science and Information Technologies. 7(1): 94-95.

[12] Sutar, A.V. Survase, N.K. Malvadkar, M.V. Patil and P.V. Raut. 2016. A combined cloud architecture for prevention of duplication and anonymous user authentications. International Engineering Research Journal (IERJ). 2(2): 652-655.

[13] Namrta Singh and Puneet Sharma. 2016. Analysis of Empower Auditing and Secure Deduplication in Hybrid Cloud. IJIRCCE. 4(3): 3037-3039.

[14] A Telkar, S. A. Maindakar) and Dr M Z Shaikh. 2016. Secured and Efficient Cloud Storage Data Deduplication System. Sumedha IJARCCE. 5(1): 301-304.

[15] Manreet Kaur and Jaspreet Singh. 2016. Data De-duplication Approach based on Hashing Techniques for Reducing Time Consumption over a Cloud Network. IJCA. 142(5): 4-10.

[16] A. Arthi and Sowmya. 2016. Secure Evaluation and Prevention of Duplicate Data in Cloud. IJIRST. 2(11): 227-233.

[17] Abid Mehmood, Iynkaran Natguanathan and Yong Xiang. 2016. Protection of Big Data privacy. IEEE transactions. pp. 1821-1834.

[18] Hsiao-Ying Lin and Wen-Guey Tzeng, 2012. A Secure Erasure Code-Based Cloud Storage System with Secure Data Forwarding. IEEE transactions on parallel and distributed systems. 23(6): 995-1003.

[19] N. Anusha and Raveendrareddy Maram. 2015. Dynamic Data Security Considerations in Multi-Cloud Storage. International Journal of Applied Engineering Research. 10(2): 3947-3955.

[20] Morusu Rahul Reddy, Anusha N and Naga Vishnu Shankar B. 2016. Secured Health Records Storage & Retrieval System Using Keyword Based Key Generation and Attribute Based Encryption (ABE). Research Journal of Pharmaceutical, Biological and Chemical Sciences. pp. 1420-1426.