Secure Cloud Storage Access with Regeneration of Code

[1] Ms.Aarti P. Kadam, [2] Dr. Archana C. Lomte,
Computer Engineering, JSPM'S Bhivrabai Sawant Institute of Technology & Research
Wagholi, Pune-421207,Maharashtra,India

ABSTRACT

Number of users makes the use of cloud computing in order to store a large amount of data. Cloud allows the users (home and professional users) to store their data on cloud. As the use of cloud increases it is necessary to provide more security to data that is stored on cloud. When some users are trying to access the data stored on cloud and if they are not able to get that data then at that time regeneration of code is required. Existing methods for the regeneration of code requires that data owner must be always online and handle all activities like auditing, repairing, regeneration of code and which practically impossible. So a public auditing scheme is proposed for regeneration of code and the operation is done in absence of data owner which totally removes online burden of data owner and to do this TPA (Third Party Auditor) and Proxy Agents are introduced. TPA is used for the Auditing while Proxy agent works on the behalf of the data owner.

Keyword : - *TPA, Proxy Agent, Cloud Storage, Code Regeneration, Privacy Preservation, Public Auditing.*

1. INTRODUCTION

Nowadays Cloud computing has become popular among various fields like information technology and various business enterprises because in cloud user has to pay only according to their usage. In cloud computing, the cloud service providers (CSPs), like Amazon and others are available and that are able to deliver various service to cloud users. Cloud Storage could be a service wherever knowledge is remotely maintained, managed, and insured. The service permits the users to store files on web, so they will access them from any location via the internet simply data stored on cloud is location independent. Cloud also provides the facilities like backup, sharing of data, recoverability, location independence etc. With a recent survey on cloud computing it is found that 800 business call manufacturers and users worldwide and the quantity of organizations gaining competitive advantage through high cloud adoption has nearly doubled within the previous few years and by 2017, the general public cloud services market is foreseen to exceed $244 billion. The main goal of cloud computing is to provide security or protection to the data stored on cloud. The basic idea is to develop a privacy preserving public auditing system for regeneration of code based cloud storage. In existing system all task like data uploading, auditing, encryption, decryption ,regeneration of code if it is needed are personally looked up by the data owner only, but it is not always possible that data owner is always online. Sometimes it might be possible that the data given by the user for the uploading may be corrupted or some contents of that data may be changed or the data present on cloud is corrupted but the cloud service provider's act dishonestly to maintain reputation of the cloud. So that to overcome such drawbacks of existing system and to reduce the burden on data owner simply TPA is introduced, TPA takes care of all operations that must be performed by data owner only so it simply removes the online burden of data owner. First task that is performed by TPA is verification about whether the user is authorized or not. If user is authorized then files are taken from the user for uploading and files stored on cloud are given to the user.

1.1 EXISTING SYSTEM

Various mechanisms that are dealing with the integrity of outsource data without a local copy have proposed under different systems and security models up till now like PDP(Provable Data Possession)model and POR(Proof of retrievability) model, which were proposed for the single server scenario by Atenies el.al.It is considered that files are usually striped and stored across multiple servers. And for that it is necessary to select the integrity verification schemes that are suitable for such multi-servers or multi-clouds with different redundancy schemes such as replication, regeneration of code etc.

1.1.1 DISADVANTAGES OF EXISTING SYSTEM

- The systems are designed only for the private audits and all data owner is able to perform activities like auditing, regeneration of code etc.
- Considering the large size of outsource data and users constraints resource capability the task of auditing in cloud can be expensive for the user.
- It necessary that data owner must be always online to handle all activities related to that cloud.

1.2 PROPOSED SYSTEM

In the proposed system the main focus is on integrity verification problem in regenerating code based cloud storage especially with function repair strategy. To fully ensure data integrity and users computational resources an public auditing scheme is proposed for regenerating cloud based storage in cloud computing, in which integrity checking and regeneration of code is done by the Third Party Auditor and semi trusted proxy separately on the behalf of the data owner. TPA performs all the tasks that must be performed by data owner in the traditional system. When any of the stored files are corrupted then codes are regenerated by the TPA with the help of proxy agent.

1.2.1 ADVANTAGES OF PROPOSED SYSTEM

- Auditing and regeneration of codes are performed by the TPA so it removes the data owner from online burden.
- Multiple copies of the data are available on various servers so it simply provides an easy method for regeneration of code.
- Signatures are assign before uploading the data on the cloud so that data cannot be altered by anyone including the TPA and data owner.

2. LITERATURE SURVEY

1) Privacy-Preserving Public Auditing for Secure Cloud Storage
Authors: Cong Wang, Sherman S.-M. Chow, Qian Wang, Kui Ren, Wenjing Lou.
To provide security to the data stored on cloud an privacy preserving public auditing system is proposed. In that method homomorphic linear authenticator and random masking are used to guarantee that TPA will not know anything about the data content that are stored on cloud during auditing process. This scheme gives an assurance to user about the security of their private data. The system is further extended into multi-server setting where TPA can perform multiple auditing tasks to improve the efficiency.

2) Enabling Data Integrity Protection in Regenerating-Coding-Based Cloud Storage
Authors: Henry C. H. Chen and Patrick P. C. Lee
Number of user storing the data on cloud is increases rapidly at the same time it is necessary to verify the integrity of the data stored on cloud. To Do this system is developed for the practical data integrity protection (DIP) scheme for functional minimum storage regenerating (FMSR) codes on multi-server setting. The DIP scheme preserve fault tolerance and also it repairs traffic saving properties of FMSR. Security strength of FMSR and DIP are analyzed for its integritation, its running time can be evaluated by using various experiments. Provide the facility of regeneration of code when data stored on cloud is corrupted or the server is corrupted.

3) An efficient and secure dynamic auditing protocol for data storage in cloud computing.
Authors: K. Yang and X. Jia.
New Methodology is proposed which includes an efficient and inherently secure dynamic auditing protocol. It protects the data privacy against the auditor by combining the different cryptographic methods with the bilinearity property of bilinear paring, rather than using the mask technique.

4) Towards secure and dependable storage services in cloud computing
Authors: C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou
To improve the security of the data stored on cloud flexible distributed storage integrity auditing mechanism is proposed which utilizing the holomorphic token and distributed erasure-coded data. The proposed design allows users to audit the cloud storage with very less communication and computation cost. The results of auditing ensures strong cloud storage correctness guarantee and also help to find out exact error location on multi server.

5) Erasure Coding for Cloud Storage Systems: A Survey
Authors: Jun Li and Baochun Li
Number of users storing the data on cloud is increases rapidly so at the same time chances of data corruptions are also increases so to overcome it is necessary to examine the existing results of coding techniques for cloud storage systems. So here coding techniques are presented into two categories: regenerating codes and locally repairable codes.

6) Simple Regenerating Codes: Network Coding for Cloud Storage
Authors: Dimitris S. Papailiopoulosy, Jianqiang Luoz, Alexandros G. Dimakisy, Cheng Huang , and Jin Li_y
A novel family of distributed storage codes that are formed by using MDS codes and simple locally decodable parities for efficient repair and high fault tolerance is introduced. As the amount of the data stored on cloud increases it is necessary to increase the security levels of the data stored on cloud MD5 can be used. Theoretical explanation is given in the paper to prove reliability of system. Information is stored on a node and if that node fails then in order to access the data same information is also stored on some another node. New methodology is proposed for the regeneration of code in such cases. When user request for the data stored on cloud first authentication is done to validate that user is authorized or not if user is valid user then only access of the data is given to user. While giving the data to user if it is found that data present on node is corrupted at that time regeneration of code is necessary. Comparison of the proposed codes is done with replication and Reed-Solomon codes using a cloud storage simulator.

3.SYSTEM ARCHITECTURE

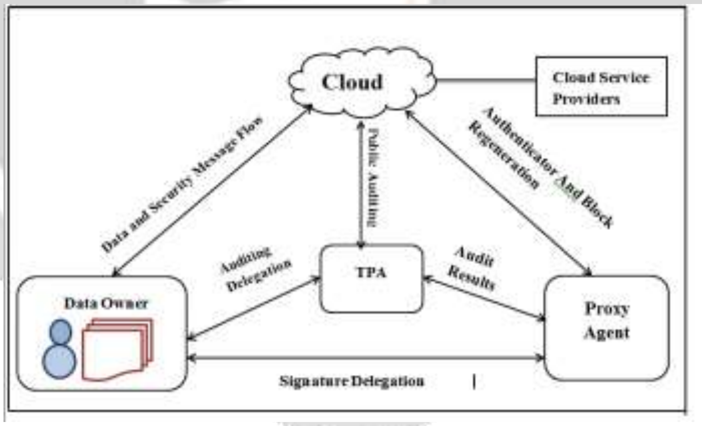

Fig 1: System Architecture

Fig.1 represents the System Architecture of Auditing Model for regeneration of code based cloud storage. It has following four main components.

Cloud: Storage place where all authorised users can store their data and it is managed by various cloud service providers.

Data Owner: The Person who is in charge of all the data stored on cloud and held responsible for all activities related to data present on that cloud.

TPA (Third Party Auditor): It must be an Expert person who is capable of handling all activities and taking all decisions in absence of data owner.

Proxy Agent: Is a semi-trusted person after the TPA and it works on behalf of data owner. The main tasks performed by proxy agent are authentication and block regeneration. It actually Perform the work as follows:

In this System First User can submit Registration Details and create username & Password to get access to data stored on cloud, after that user can login to system. All the request about access or storage of data are associated with the third Party Authority (TPA).TPA Encrypts the data or document and then outsources it to the cloud, when user requests a document, TPA Decrypts the document and then provides it to the user. Along with Encryption and Decryption the TPA authenticates the data Owner and user. The most important part of the project is when a server goes down or in other words a server is corrupted ,the proxy server collects the data from other servers and regenerates the code .The approach will provide great security to data and also Reduce burden of data owner and data user.

The fig 2 shows that how actually the regeneration of code take place. First multiple copies of the data which is submitted by the user are created and those copies are placed on different server. If the original data submitted by the user is corrupted or if server is corrupted at that time that particular data can be taken from any other server. If the Data submitted by the user is corrupted then firstly files are search on the on the first server if files on the first server are also corrupted then searching of the files will be on the remaining server likewise if the original data is corrupted it can be regenerated by using its other copies those are present on the other server.

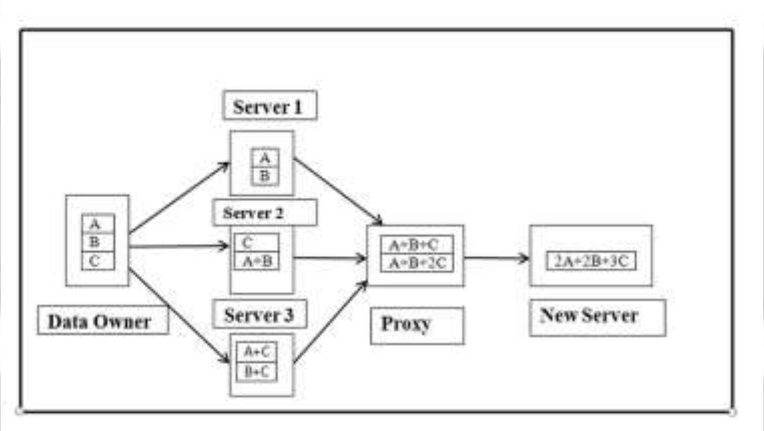

Fig 2: Regeneration of code

4.OBJECTIVES:

- To achieve access control of encrypted data in an untrusted environment.
- Reduce burden and risk of single authority domain.
- Perform auditing with minimum communication and computation overhead.
- Avoid unauthorized user access to the confidential data stored in cloud server.

5.METHODOLOGY

For the implementation of the privacy preserving public auditing system AES (Advance Encryption Standard) algorithm is used and it will work as follows.

1) Data owner

```
a. if (user == authorized)
```

Allow access

b. upload file

2) Data user

a. if (user == authorized)

Allow access

b. search & download file

3) Authority: TPA

a. authenticate users

b. encryption

c. decryption

AES Algorithm:

1) Add round stage: There are 9 rounds of following 4 stages:

a) Substitute bytes

b) Shift rows

c) Mix Columns

d) Add Round Key

2) The tenth round simply leaves out the Mix Columns stage. The first nine rounds of the decryption algorithm consist of the following steps:

1. Inverse Shift the rows
2. Inverse Substitute the bytes
3. Inverse Add the Round Key
4. Inverse Mix the Columns

Again, the tenth round simply leaves out the Inverse Mix Columns stage.

Following are the steps of AES Algorithm.

Step 1: Start of an Algorithm

Step 2: Key Generation by **Advanced Encryption Standard (**AES) Algorithm (keys are Generated)

Step 3: Map the Key to the files

Step 4: Divide the files into the blocks

Step 5: Each Encrypted Block is associated with an Key

Step 6: Store the data blocks to cloud storage server.

Step 7: Simultaneously copy of keys are send to TPA

Step 8: On request of Cloud Service Provider (CSP), the Auditing processes will be done by TPA

Step 9: Validate the data by signatures and data Integrity proofs.

Step 10: Successful validation, verification will be done for Dynamic auditing by TPA

Step 11: End of Algorithm.

6 .DESIGN GOALS

Public Auditability: To allow the TPA to perform various activities on the data given by user to reduce the burden of data owner.

Privacy Preserving: It ensures that the auditor and proxy cannot derive the user content in auditing and regeneration process.

Authenticator Regeneration: Authentication of the repaired blocks is correctly generated by the TPA in absence of the data owner.

Error Location: Exact error location or server is detected when corruption in found.

7. EXPERIMENTAL RESULT

Here are the some current reports of the performance results of the experiment. I think about this auditing mechanism happens between an ardent TPA and a few cloud storage node, where user's information is outsourced to. In this experiment, the TPA/user feature method is enforced on a digital computer. Currently the performance of the planned privacy-preserving public auditing schemes are assessed to indicate that they are so light-weight and for that an execution time of the privacy-preserving system is assess. The experiment is conducted on 3 rule i.e. AES rule, RSA algorithm and DES rule.

Table 1: Execution time for files with AES, RSA and DES Algorithm

File Name	File Size (KB)	Execution time with AES(ms)	Execution Time with RSA(ms)	Execution Time with DES(ms)
Abc.pdf	337	109.375	178.5	340.5
Abc .doc	10	125	200.8125	364.25
Abc.txt	4	94.3	120.4	150.54
Abc.jpeg	860	234.375	320	532.625

Table 1 displays Execution Time for files with AES, RSA and DES algorithmic program. The execution time required for AES is very less as compare to DES and RSA algorithmic program. From this it is concluded that an AES algorithm gives the best results as compared to RSA and DES algorithm.

The following Figure 3 shows graph illustration of above Table. It will show the comparison of AES, RSA and DES algorithmic program with relevance Execution time.

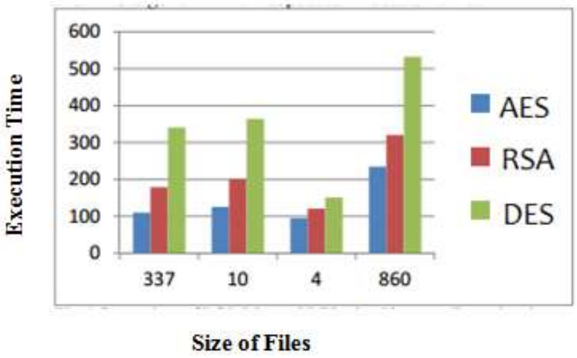

Fig 3: Comparison of AES with RSA and DES Algorithm

This theme provides a system for preserving the confidentiality of the info. Confidentiality is preserved through Third Party Auditor (TPA) it will support knowledge integrity and validation through challenge verification.

8. CONCLUSION

The proposed methodology provides huge security to users. This is very user friendly system. This system reduces the burden of data Owner & data Users. If Data is get corrupted then also authorized users can get data again and for that a public auditing scheme which is developed for the regenerating code based cloud storage system is proposed, where the data owners are privileged to delegate TPA for their data validity checking. To protect the original data privacy against the TPA, the coefficients are randomize in the beginning rather than applying the blind technique during the auditing process. Considering that the data owner cannot always stay online in practice, in order to keep the storage available and verifiable after a malicious corruption, a semi-trusted proxy is introduced into the system model and provides a privilege for the proxy to handle the reparation of the coded blocks and authenticators. To better appropriate for the regenerating-code-scenario, authenticator is designed based on the BLS signature. This Authenticator can be efficiently generated by the data owner simultaneously with the encoding procedure. Extensive analysis shows that this scheme is more secure, and the performance valuation shows that the proposed scheme is highly efficient and can be feasibly integrated regeneration of code in cloud storage.

9. ACKNOWLEDGEMENT

I take this special opportunity to express my sincere gratitude towards professor and all the people who supported me during my entire project work. I would like to express my gratitude to my guide and also the project coordinator Dr. Archana Lomte for providing special guidance. I would also like to thank our HOD Dr. G.M.Bhandari who always has enough time to solve student’s problems at any time. Finally thanks to all teachers who are always supportive at us.

10.REFERENCES

[1] S. S. Chow ,C.Wang, Q.Wang, K. Ren, and W. Lou,“**Privacy-preserving public auditing for secure cloud storage**” *Computers, IEEE Transactions on*, vol. 62, no. 2, pp. 362–375, 2013.

[2] P. Lee and H. Chen “**Enabling data integrity protection in regenerating coding-based cloud storage: Theory and implementation**” *Parallel and Distributed Systems, IEEE Transactions on*, vol. 25, no. 2, pp. 407–416,Feb 2014.

[3] Oruta: **Privacy-Preserving Public Auditing for Shared Data in the Cloud** Boyang Wang, Baochun Li, *Member, IEEE*, and Hui Li, *Member, IEEE are with the State Key Laboratory of IntegratedServices Networks, Xidian University, Xi’an, 710071, China. Boyang .*

[4] Cheng Huang_, Dimitris S. Papailiopoulosy, Jianqiang Luoz, Alexandros G. Dimakisy, and Jin Li_Y University of Southern California, Los Angeles, CA 90089 "**Simple Regenerating Codes: Network Coding for Cloud Storage".**

[5] Ke Wang,Benjamin C M Fung, Rui Chen, **Privacy-Preserving Data Publishing: A Survey of Recent Developments,** ACM Computing Surveys, Vol. 42, No. 4, Article 14, Publication date: June 2010.

[6] A. Joseph ,A. Fox, R. Griffith, R. Katz, A. Konwinski, G. Lee,D. Patterson, A. Rabkin, and I. Stoica, "**Above the clouds: A Berkeley view of cloud computing,**" *Dept. Electrical Eng. and Comput. Sciences,University of California, Berkeley, Rep. UCB/EECS*, vol. 28, p. 13, 2009.

[7] R. Burns, ,G. Ateniese, R. Curtmola, J. Herring, L. Kissner, Z. Peterson,and D. Song, **"Provable data possession at untrusted stores,"** in *Proceedings of the 14th ACM Conference on Computer and Communications Security*, ser. CCS '07. New York, NY, USA: ACM, 2007, pp. 598–609.

[8] B. S. Kaliski Jr and, A. Juels **"Pors: Proofs of retrievability for large files,"** in *Proceedings of the 14th ACM conference on Computer and communications security*. ACM, 2007, pp. 584–597.

[9] O. Khan, R. Curtmola, R. Burns, and G. Ateniese, "**Mr-pdp: Multiplereplica provable data possession**" in *Distributed Computing Systems,2008. ICDCS'08. The 28th International Conference on* . IEEE, 2008,pp. 411–420.

[10]X. Jia and K. Yang "**An efficient and secure dynamic auditing protocol for data storage in cloud computing**" *Parallel and Distributed Systems, IEEE Transactions on*, vol. 24, no. 9, pp. 1717–1726, 2013.

[11] Janani.G.K ,Arun Kumar.K, Gnanadeepa.S, Hepzibha John,"***Survey on Security and Privacy Preserving Public Auditing for Content Storage in Cloud Environment***", International Conference on Electrical, Electronics, Signals, Communication and Optimization (EESCO) – 2015.

[12] K. Ren ,C. Wang, Q. Wang, and W. Lou, **"Towards secure and dependable storage services in cloud computing**" *Service Computing, IEEE Transactions on*, vol. 5, no. 2, pp. 220–232, May 2012.

[13] A. Kupcu, C. ErwayC. Papamanthou, and R. Tamassia, "**Dynamic Provable Data Possession**" in *Proc. ACM Conference on Computer and Communications Security (CCS)*, 2009, pp. 213–222.

[14] A. Fox, M. Armbrust, R. Griffith, A. D.Joseph, R. H.Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "**A View of Cloud Computing**" *Communications of the ACM*,vol. 53, no. 4, pp. 50–58, Apirl 2010.