ISSN 2395-1621

# Implementation on Secure Data Storage and Efficient Search System based on Encryption Algorithm

Prof. Pallavi Gulave, Sameer J Pathan, Akash K Vasekar, Shrikant P Mane.

Associate Professor, Department of Computer Engineering, JSPM’s BSIOTR, Wagholi, Pune, Maharastra, India.

Student, Department of Computer Engineering, JSPM’s BSIOTR, Wagholi, Pune, Maharastra, India.

## ABSTRACT

**Cloud computing has been emerged as a computing network over the Internet. Cloud data indulge storing of the data in the cloud as well as has sharing capability among multiple users. Due to failures of human or hardware and even Software errors cloud data is associated with data integrity. Several mechanisms have been proposed in order to allow both the data owners as well as the public auditors to audit cloud data integrity efficiently without retrieving the entire data from the cloud servers. A Third Party Auditor will perform integrity checking and the identity of the signer on shared data is kept private from them. In this project, we only investigate for auditing the integrity of shared data in the cloud with efficient user cancelation while still preserving identity privacy. We also enhance this system, when any user change the data from files then we analysis that files and generate the log for future analysis.**

**Keyword: Analysis data update, Cloud computing, Data security, auditing.**

ARTICLE INFO

**Article History**

Received: 30th June 2021

Received in revised form : 30th June 2021

Accepted: 2nd July 2021

**Published online : 2nd July 2021**

## I. INTRODUCTION

Cloud storage is a cloud computing model in which data is stored on remote servers accessed from the Internet, or "cloud." It is maintained, operated and managed by a cloud storage service provider on storage servers that are built on virtualization techniques.

Cloud computing is being intensively referred to as one of the most influential innovations in information technology in recent years. With resource virtualization, cloud can deliver computing resources and services in a pay-as-you-go mode, which is envisioned to become as convenient to use similar to daily-life utilities such as electricity, gas, water and telephone in the near future. These computing services can be categorized into Infra-structure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS).

Cloud computing is a type of Internet-based computing that provides shared computer processing resources and data to computers and other devices on demand. It is a model for enabling ubiquitous, on-demand access to a shared pool of configurable computing resources (e.g., computer networks, servers, storage, applications and services).

***Problem Statement:***

The Data Security and Data Integrity is the most important factor to any data centre, company and government records. To let off the burden of management of data of the data owner, TPA will audit the data of client.

## II. LITERATURE SURVEY

[1] The main problem associated with is the size of signatures and verification time linearly increase with the number of users in the group that is solved with Knox considering audit of the data integrity which is to be shared with a large group while still preserving identity privacy from the TPA by leveraging group signatures.

[2] This system proved the data freshness (proved the cloud possesses the latest version of shared data) while still preserving identity privacy. An experimental result of this ensures that retrieved data always reflects the most recent updates and prevents rollback attacks.

[3] They have utilized the idea of proxy re-signatures to allow the cloud to re-sign blocks on behalf of existing users during user revocation, so that existing users need not to download and re-sign blocks by themselves. Moreover, this mechanism is able to support batch auditing by verifying multiple auditing tasks simultaneously. Experimental results show that the mechanism can significantly improve the efficiency of user revocation.

[4] To introduce the TPA effective safely, the audit process should not compensate an additional fee for online users and carry-in; there is no new compromise to the privacy of user data. This proposed approach is a secure cloud storage mechanism as public auditing mechanism for secure cloud storage. At the same time this approach extends to the TPA performance to audit multiple users efficiently. By showing high efficiency and provable security and performance analysis a wide range of security, the proposed scheme.

[5] They have exploit ring signatures to compute the verification information needed to audit the integrity of shared data. With this mechanism, the identity of the signer on each block in shared data is kept private from a third party auditor (TPA), who is still able to publicly verify the integrity of shared data without retrieving the entire file.

## III. PROPOSED WORK

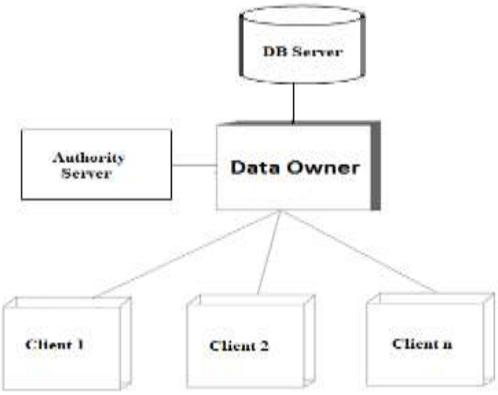

Fig 1. System architecture

### A. Module Description:

Admin

They are responsible for granting access privileges to the users of the respective group. Admin has the main access permission for maintaining the files over cloud. Admin can navigate through the group as well. Admin can view the log details of the activities carried on the cloud file storage.

User

Every user needs to register with the corresponding group for getting access permission and signature key from the same. Using the signature key they can get the access permission. they can upload the files to cloud. User from same group can view the content of the file from cloud and make changes over it and can save them. Simultaneously they can download the files as well.

Third Party Auditor (TPA)

TPA has the rights to validate the files which are available in the cloud. TPA is the respective authority for performing the verification of files which are uploaded by any user who are registered under a single group.

### B. Mathematical Model:

System Description:
Input:

Upload file ()
U : Upload file on local cloud.
E : Encryption File.
H : Generate encrypt data.
I : Unique id to all file.

Output:
Generate encrypted data of the all uploaded data

Input Function auditing (id, request, log, data)
ID : unique id for each file.
Request : User request for the any file.
Log : Check all file log on cloud.
Data: check log data.

Output:
Generate the log data of each modification file.

Success Conditions:
Generate the log data and auditing on file upload.

Failure Conditions:
Our system fails when no any security policy applies to the input file.

## IV. SYSTEM ANALYSIS

We have created system in java. Data is stored in mysql database. We have created a web application with local server. Web application that communicates with local server and Trustee Server using REST API. We have uploaded text document on cloud. We have evaluated time required for tag generation and file encryption for security. Here we also calculate the file each file time, date which time user can do any activity for analysis purpose.

## V. ACKNOWLEDGMENT

I wish to express my profound thanks to all who helped us directly or indirectly in making this paper. Finally I wish to thank to all our friends and well-wishers who supported us in completing this paper successfully I am especially grateful to our guide for him time to time, very much needed, valuable guidance. Without the full support and cheerful encouragement of my guide, the paper would not have been completed on time.

## VI. SCREEN SHOT

Public Integrity Auditing

Member Registration

## VII.CONCLUSION

Data privacy has become extremely important in the Cloud environment. The issue of file auditing of data on networks has been summarized. Data storage that is secure and easy to share across platforms. Data stored is highly secured using the cryptography algorithms and digital signatures. It integrates some new concepts like data security, storage optimality, file integrity and authentication access which are not present in the current system.

## REFERENCES

[1] Y. Zhu, G.-J. Ahn, H. Hu, S. S. Yau, H. G. An, and S. Chen, “ Dynamic Audit Services for Outsourced Storage in Clouds,” IEEE Transactions on Services Computing, accepted.

[2] Balkrishnan. S, Saranya. G, Shobana. S and Karthikeyan.S, “ Introducing Effective Third Party Auditing (TPA) for Data Storage Security in Cloud” , International Journal of computer science and Technology, vol. 2, no. 2, ISSN 2229-4333 (Print) | ISSN: 0976- 8491(Online), June 2012

[3] K. Kiran Kumar, K. Padmaja, P. Radha Krishna, Automatic Protocol Blocker for Privacy-Preserving Public Auditing in Cloud Computing” , International Journal of Computer science and Technology, vol. 3 pp, ISSN. 0976-8491(Online), pp. 936-940, ISSN: 2229-4333 (Print), March 2012 .

[4] H. Shacham and B. Waters, “ Compact Proofs of Retrievability,” in the Proceedings of ASIACRYPT 2008. SpringerVerlag,2008,pp.90– 107.

[5] C. Wang, Q. Wang, K. Ren, and W. Lou, “ Towards Secure and Dependable Storage Services in Cloud Computing,” IEEE Transactions on Services Computing, vol. 5, no. 2, pp. 220– 232, 2011.

[6] S. Marium, Q. Nazir, A. Ahmed, S. Ahthasham and Aamir M. Mirza, “ Implementation of EAP with RSA for Enhancing The Security of Cloud Computig” , International Journal of Basic and Applied Science, vol 1, no. 3, pp. 177-183, 2012

[7] Jachak K. B., Korde S. K., Ghorpade P. P. and Gagare G. J.,“ Homomorphic Authentication with Random Masking Technique Ensuring Privacy & Security in Cloud Computing” , Bioinfo Security Informatics, vol. 2, no. 2, pp. 49-52, ISSN. 2249-9423, 12 April 2012

[8] J. Yuan and S. Yu, “ Proofs of Retrievability with Public Verifiability and Constant Communication Cost in Cloud,” in Proceedings of ACM ASIACCS-SCC’ 13, 2013

[9] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson,and D. Song, “ Provable Data Possession at Untrusted Stores,” in the Proceedings of ACM CCS 2007, 2007, pp. 598– 610.

[10] C. Wang, Q. Wang, K. Ren, and W. Lou, “ Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing,” in the Proceedings of IEEE INFOCOM 2010, 2010, pp. 525– 533.

[11] N. Cao, S. Yu, Z. Yang, W. Lou, and Y. T. Hou, “ LT Codes-based Secure and Reliable Cloud Storage Service,” in the Proceedings of IEEE INFOCOM 2012, 2012, pp. 693– 701.