# SEC CLOUD DATA STORAGE USING TPA (AUDITING)

Motukuri Prashanthi
CMR Engineering College (JNTU), Hyderabad

**ABSTRACT**

**As the cloud computing technology develops during the last decade, outsourcing data to cloud service for storage becomes an attractive trend, which benefits in sparing efforts on heavy data maintenance and management. Nevertheless, since the outsourced cloud storage is not fully trustworthy, it raises security concerns on how to realize data deduplication in cloud while achieving integrity auditing. In this work, we study the problem of integrity auditing and secure deduplication on cloud data. Specifically, aiming at achieving both data integrity and deduplication in cloud, we propose two secure systems, namely SecCloud and SecCloud+. SecCloud introduces an auditing entity with a maintenance of a MapReduce cloud, which helps clients generate data tags before uploading as well as audit the integrity of data having been stored in cloud. Compared with previous work, the computation by user in SecCloud is greatly reduced during the file uploading and auditing phases. SecCloud+ is designed motivated by the fact that customers always want to encrypt their data before uploading, and enables integrity auditing and secure deduplication on encrypted data. I would like to reduce time complexity by reducing number of audits and finally achieve constant amount of time.**

**KEY WORDS: Cloud service provider (CSP), SecCloud, Sec+ Cloud.**

## Introduction

Cloud computing is widely embraced by various organization for data outsourcing. Cloud computing provides flexible and cost effective way to access outsourced data to end user in multiform without any geographical restriction. According to National Institute of Standards and technology (NIST), Cloud computing is a model for enabling worldwide, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly managed with minimum effort or service provider interaction[1]. The basic concept behind cloud computing is virtualization; it provides virtual storage and computing service to the cloud clients. Virtualization is basically making available resources such as operating system, network, storage device and server so that they can be used by multiple users at the same time. In cloud computing the workload of users can be managed and make it more efficient, scalable and economical using virtualization.

Cloud model is composed of three service models**. First,** Software as a Service (SaaS) provides the capability to its users, to run their applications on cloud infrastructure. **Second**, Platform as a Service (PaaS) provides a platform to users to perform operations like develop, run, and manage applications. **Third,** Infrastructure as a service (IaaS) provides virtualized hardware support to its users so that they can save their investments over expensive local hardware requirements.

Cloud computing has four types of deployment models. **First**, Private cloud delivers its services same as public cloud but dedicate to single user or organization. **Second**, Public cloud provides its services shared over multiple users and organizations. **Third,** Hybrid cloud is a combination of Public cloud and Private cloud as it works like Private cloud but can access more computing resources from third party to enhance its performance. **Fourth** is Community cloud, as its name suggests that its services are shared over multiple organizations belonging to same working area or we can say community.

## Auditing

Public auditing allows a third party in addition to the users themselves, to check the integrity of outsourced data. We cannot fully trust on the external party as it may be honest but curious to see the data. So we can have trust on external auditing party. In this paper we have assumed that the auditor is honest over whole auditing process but it may curious to see confidential data. In addition Sometimes CSP might be dishonest. And there exists various reasons for CSP to behave unfaithfully toward the Data owner regarding their outsourced data status. For example, CSP might reclaim storage for budgetary reason by discarding data that have not been or rarely accessed, or hide data loss incident to maintain a reputation [5].In case of CSP is dishonest it may launch following attack to TPA [15]:

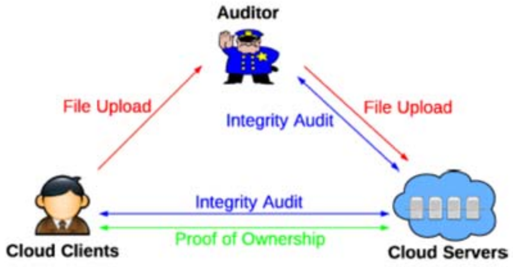
- **Forge attack:** The CSP may forge the data blocks and/or their tags to deceive the verifier.

- **Replace attack:** CSP can perform the replacement of corrupted data blocks and their tags with previously generated data blocks and tags so that CSP can pass the integrity check.

- **Reply attack:** The CSP may attempt to pass the verification using the proof generated from the previous ones or other former information.

## System Model:

In auditing model we consider three main entities are involving they are: Data owner, Cloud service Provider and Third party auditor .The Data owner create their data and upload it on the cloud. The cloud service provider stores the data into cloud and allows accessing the data from anywhere and at any time.[24] So it is necessary to make insure that the data is same as it was uploaded by the data owner. Here is the third entities is auditor who verify the data integrity of the outsourced data for both data owner and server.[25]To verify the outsourced data, the data owner does not provide original data instead of that they give them metadata; outsourced data is almost in encrypted form. When data owner send request to TPA to check the integrity of data, the TPA send challenge to cloud service provider and regarding that challenge the CSP send the proof.[22]This way the third party auditor ensures the integrity of outsourced data.



## Literature survey

Many solutions have been proposed to check the integrity of outsourced data which can be generally divided into two categories: private auditing and public auditing. Private auditing is the beginning model for checking data integrity of outsourced data, in which data integrity checking operation can be performed between CSP and data.[1] In public auditing data verification operation is performed by TPA which reduces the overhead of Data owner. And this is a more particle way.

**Proofs of Retrievability (POR)** data integrity scheme is proposed by Juels et al. [4] in 2007 .this is a private auditing solution it is done by TPA cryptographic method for authenticate the integrity outsourced data stored in the cloud, without keeping a copy of the user's original files in local storage. It check the integrity of outsourced data and make sure the retrivability of data with the use of error correcting code.

**PDP(Provable Data Possession)** is First public auditing scheme is proposed by Ateniese et al. in 2007 ,which involve Homomorphic tags based on RSA and can remotely check the integrity of outsourced data by randomly sampling a some blocks from the file[13][15]. If differentiate with private auditing it is the first data integrity checking scheme which performed by external party not by user themselves. This scheme reduces the dispensable overhead of the user. It ensure public audit but does not have privacy preserving facility and like private audit data recovery is not supported [9].

**Partially Dynamic –** PDP is proposed by Atenies et al. [19] in 2008, a highly efficient and secure method for dynamic auditing based on symmetric key cryptography that not required extent encryption.it delimit is it perform only limited number of audit and not support privacy preserving. **PDP(first privacy preserving PDP)** is introduced by , Wang et al. [6] in 2010 presented a public auditing scheme which ensure the privacy preserving for outsourced data using Integrating the Homomorphic authenticator with random masking technique. Applied the bilinear aggregate signature to expand auditing in batch manner for multiple user, where Third party auditor can perform auditing in simultaneously manner.[2]

**Cooperative PDP (CPDP)** technique proposed by Zhu et al in 2012 which is scheme based on hash index hierarchy and Homomorphic verifiable scheme.[3]It Support public auditing, Privacy preserving and Batch auditing in multi cloud but it had not provision for multi user auditing.[14] **DAP (Dynamic Auditing Protocol)** in 2013, Yang et al.[14] proposed further enhance auditing scheme which support dynamic auditing using the Index table scheme as data owners dynamically update their data. This paper introduced the auditing scheme for both multiuser and mult cloud to achieve batch auditing. To ensure the privacy of outsourced data they used the bilinearity property of the bilinear pairing.[5]

**DPDP-MHT(dynamic provable data possession )** propounded by Wang et al[18], In 2013 presented another classic public auditing scheme for dynamic auditing using Merkle Hash Tree construction for block tag authentication (MHT), to achieve efficient data dynamics. It support public auditing, Privacy preserving. Support dynamic auditing and Batch auditing in multi cloud.[12]

**IHT-PA( Index Hash Table-public audit)** In 2013, Zhu et al. [17] proposed further enhanced public auditing scheme based on index hash table.IN this paper auditing service formulated on random sampling, fragment structure.

### Back ground

In previous papers the algorithms

Designed in such a way that some algorithms support public auditing and some support private auditing and some algorithms support batch auditing and some does not support batch auditing as the number of audits increase the running time complexity increases which is not efficient way of utilizing.

### Disadvantages of Exising system

1. The first problem is integrity auditing. The cloud server is able to relieve clients from the heavy burden of storage management and maintenance. The most difference of cloud storage from traditional in-house storage is that the data is transferred via Internet and stored in an uncertain domain, not under control of the clients at all, which inevitably raises clients great concerns on the integrity of their data.

2. The second problem is secure deduplication. The rapid adoption of cloud services is accompanied by increasing volumes of data stored at remote cloud servers. Among these remote stored files, most of them are duplicated: according to a recent survey by EMC, 75% of recent digital data is duplicated copies.Unfortunately, this action of deduplication would lead to a number of threats potentially affecting the storage system, for example, a server telling a client that it (i.e., the client) does not need to send the file reveals that some other client has the exact same file, which could be sensitive sometimes. These attacks originate from the reason that the proof that the client owns a given file (or block of data) is solely based on a static, short value (in most cases the hash of the file).

### PROPOSED SYSTEM:

1. In this paper, aiming at achieving data integrity and deduplication in cloud, we propose two secure systems namely SecCloud and SecCloud+.

2. SecCloud introduces an auditing entity with maintenance of a Map Reduce cloud, which helps clients generate data tags before uploading as well as audit the integrity of data having been stored in cloud.

3. Besides supporting integrity auditing and secure deduplication, SecCloud+ enables the guarantee of file confidentiality.

4. We propose a method of directly auditing integrity on encrypted data.

### Secure De-duplication System

- ✓ We consider several types of privacy we need protect, that is, i) unforgeability of duplicate-check token: There are two types of adversaries, that is, external adversary and internal adversary.

- ✓ As shown below, the external adversary can be viewed as an internal adversary without any privilege.
- ✓ If a user has privilege p, it requires that the adversary cannot forge and output a valid duplicate token with any other privilege p′ on any file F, where p does not match p′. Furthermore, it also requires that if the adversary does not make a request of token with its own privilege from private cloud server, it cannot forge and output a valid duplicate token with p on any F that has been queried.

## Conclusion

As after proposal of sec cloud and sec+ cloud with internal and external adversary priviliges to avoid forge there is a future enhancement combining with huge amount of data like big data emerging a new technology by reducing time complexities.

## REFERENCES

[1] H. Dewan and R. C. Hansdah. ″A Survey of Cloud Storage Fa- cilities″, Proc. 7th IEEE World Congress on Services, pp. 224-231, July 2011.

[2] C. Wang, Q. Wang, K. Ren, N. Cao and W. Lou. ″Toward Secure and Dependable Storage Services in Cloud Computing″, IEEE Trans. Service Computing, vol. 5, no. 2, pp. 220-232, 2012.

[3] K. Ren, C. Wang and Q. Wang. “Security Challenges for the Public Cloud,” IEEE Internet Computing, vol. 16, no. 1, pp. 69– 73, 2012.

[4] J. Ryoo, S. Rizvi, W. Aiken and J. Kissell. ″Cloud Security Audit- ing: Challenges and Emerging Approaches″, IEEE Security & Privacy, vol. 12, no. 6, pp. 68-74, 2014.

[5] C. Wang, K. Ren, W. Lou and J. Li. ″Toward Publicly Auditable Secure Cloud Data Storage Services″, IEEE network, vol. 24, no. 4, pp. 19-24, 2010.

[6] Q. Wang, C. Wang, K. Ren, W. Lou and J. Li. ‘‘Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing,’’ IEEE Trans. on Parallel and Distributed Systems, vol. 22, no. 5, pp. 847-859, 2011.

[7] F. Sebé, J. Domingo-Ferrer, A. Martínez-Ballesté, Y. Deswarte and J.-J. Quisquater, “Efficient Remote Data Possession Check- ing in Critical Information Infrastructures,” IEEE Trans. Knowledge Data Eng., vol. 20, no. 8, pp. 1034-1038, 2008.

[8] A. Juels and B.S. Kaliski Jr., “PoRs: Proofs of Retrievability for Large Files,” Proc. ACM Conf. Computer and Communications Se- curity (CCS ’07), pp. 584-597, 2007.

[9] G. Ateniese, R.B. Johns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson and D. Song, ‘‘Provable Data Possession at Untrusted Stores,’’ Proc. 14th ACM Conf. on Comput. and Commun. Security (CCS), pp. 598-609, 2007.

[10] K. Yang and X. Jia. ″Data Storage Auditing Service in Cloud Computing: Challenges, Methods and Opportunities″. World Wide Web, vol. 15, no. 4, pp. 409-428, 2012

[11] C. Wang, Q. Wang, K. Ren and W. Lou, ‘‘Privacy-Preserving Public Auditing for Data Storage Security in Cloud Compu- ting,’’ Proc. IEEE INFOCOM, pp. 1-9, 2010.

[12] C. Wang, S. M. Chow, Q. Wang, K. Ren and W. Lou, ″Privacy- Preserving Public Auditing for Secure Cloud Storage,″ IEEE Trans. on Computers, vol. 62, no. 2, pp. 362-375, 2013.

[13] Y. Zhu, H. Hu, G. Ahn, and M. Yu, “Cooperative Provable Data Possession for Integrity Verification in Multi-Cloud Storage,” IEEE Trans. Parallel and Distributed Systems, vol. 23, no. 12, pp. 2231-2244, 2012.

[14] K. Yang and X. Jia, “An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing,” IEEE Trans. on Parallel and Distributed Systems, vol. 24, no. 9, pp.1717-1726, 2013.

[15] C. C. Erway, A. Küpçü, C. Papamanthou and R. Tamassia.“Dynamic Provable Data Possession,” Proc. 16th ACM Conf. Computer and Comm. Security, pp. 213-222, 2009.

[16] Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu and S. S.Yau, “Dy- namic Audit Services for Outsourced Storage in Clouds,” IEEE Trans. on Services Computing, vol. 6, no. 2, pp. 227–238, 2013.