Designing Efficient Security Technique for Data Storage in Cloud Computing

Ingale Pragati Purushottam
Dept of Computer Science and Information Technology SGBAU, Amravati

V. M. Thakare, PhD
HOD, Dept of Computer Science and Information Technology SGBAU, Amravati

ABSTRACT
Cloud computing is an environment in which data owner move data from local system to cloud storage, next job of cloud service provider (CSP) to store that data and provide it to the user on their demand. In this simplest environment exist various security risk on cloud storage because it consist sensitive data of owner, sometime it may happened cloud services provide is dishonest. On the brief view it is clear there is various risk on cloud data storage. In this paper firstly introduce recycle storage method for reliability of data and for improving the performance and security concern proposed audit storage system.

Index term- Cloud computing, security risk, recycle storage, audit storage.

1. INTRODUCTION
Everywhere on demand access of services is done because of cloud computing. Cloud service provider store large amount of owner's data on cloud server and provide it to the user on their demand. It is curious to handle all data on the cloud so it believed on third party auditor (TPA) and also exits various challenges regarding to the data integrity on cloud storage. Many researcher provides various integrity checking methods with different parameters and security model [1][2]. Data owner worried about data because data may be lost on any infrastructure (cloud storage)[3] or cloud service provide could dishonest. Data which is not access from long time, CSP discarded data from storage system hide it from the owner or shows lie data still available [4]. In this paper proposed recycle storage service, which access those data which was discarded by CSP. Another concern with cloud storage is of security, here proposed audit storage to improve the performance of services.

2. BACKGROUND
Traditionally, owners can check data integrity base on two party storage auditing system. But either side cloud service provider (CSP) or data owner, it's inappropriate to conduct such auditing because there is no guaranty to provide unbiased result. So now for security purposed deploy on third party auditing (TPA). The TPA could improve performance and having capability to do more efficient work and convince cloud service provider and owners. But TPA cannot provide data privacy preserving; it may not support dynamic data operations, and not support bath auditing for multi-cloud environment. So there is need to improved existing storage system to improve the performance and to provide security to stored data. Efficient security techniques for data storage system were proposed by various researchers. These storage systems depends either on audit services, dynamic data operations, data integrity checking on untrusted server and outsource storage or indirect mutual trust between cloud service provider and owners. In this paper proposed two methods firstly introduced recycle storage scheme to improved mutual trust between cloud service provider and data owners. And then proposed audit storage scheme to support secure dynamic data operations on cloud storage system or on multi-cloud environment and integrity checking on untrusted server.

3. PREVIOUS WORK DONE
Kan Yang, et al. [4] work on an efficient and privacy preserving auditing protocol. Qian Wang, et al. [5] proposed public auditability and data dynamics for cloud data storage. Yan Zhu, et al. [6] proposed a dynamic audit service which is used to verify the integrity of an untrusted and outsourced storage. Ayad Barsoum, et al. [7] proposed a cloud-based storage scheme that allows data owners to get benefits from the facilities offered by the CSP and enables indirect mutual trust between them. Cong Wang, et al. [8] proposed a flexible distributed storage integrity auditing mechanism, utilizing the homomorphic token and distributed erasure-coded data.

4. EXISTING METHODOLOGY
To solve the data privacy problem, used–"Efficient and secure dynamic auditing protocol" [4] generate an encrypted proof with the challenge stamp by using the bilinearity property of the bilinear pairing, such that the auditor cannot decrypt it, but the auditor can verify the correctness of the proof without decrypting it.

This protocol can reduce the computing loads of the auditor by moving it to the cloud server. The data fragment technique can reduce number of data tags, storage overhead and improve the system performance. By using the homomorphic verifiable tags, server only responses the sum of data blocks and the product of tags to the auditor, whose size is constant and equal to only one data block. Thus, it reduces the communication cost.

Homomorphic authenticator technique [5] to use PKC-based homomorphic authenticator to equip the verification protocol with public auditability for supporting public auditability without retrieving data blocks themselves. authors use BLS signature scheme which can also be implemented in RSA scheme with data dynamics.

Dynamic auditing sevice [6] used to verify integrity verification of untrusted and outsource data. According to authors this auditing sevice can provide public auditability without downloading any raw data and protect privacy of data. This auditing service also support for dynamic data

operations and errors detection in timely manner with the help of various techniques such as fragment structure, random sampling and index hash table. Here authors also proposed an efficient approach which is base on periodic verification and probabilistic query for improving the performance of proposed auditing service. And also introduced a proof-of-concept protocol for viability and feasibility of proposed auditing service.

Ayad Barsoum, et al[7] proposed a scheme that addresses important issues related to outsourcing the storage of data, namely dynamic data, newness, mutual trust, and access control. The remotely stored data can be not only accessed by authorized users, but also updated and scaled by the owner. After updating, authorized users should receive the latest version of the data (newness property), i.e., a technique is required to detect whether the received data are stale. Mutual trust between the data owner and the CSP is another imperative issue, which is addressed in the proposed scheme. A mechanism is introduced to determine the dishonest party, i.e., misbehavior from any side is detected and the responsible party is identified. The access control is considered, which allows the owner to grant or revoke access rights to the outsourced data.

A flexible distributed storage integrity auditing mechanism, [8] uses homomorphic token with distributed erasure-coded data. This design permitted user to secure cloud storage with very lightweight communication and computation cost. The auditing result ensures strong cloud storage correctness guarantee, as well simultaneously achieves fast data error localization, i.e., the identification of misbehaving server.

5. ANALYSIS AND DISCUSSIONS

5.1 Existing methods working

Efficient and secure dynamic auditing protocol: Storage auditing is a very resource demanding service in terms of computational resource, communication cost, and memory space.

Working: storage auditing protocol consists of three phases: owner initialization, confirmation auditing, and sampling auditing. During the system initialization, the owner generates the keys and the tags for the data. After storing the data on the server, the owner asks the auditor to conduct the confirmation auditing to make sure that their data is correctly stored on the server. Once confirmed, the owner can choose to delete the local copy of the data. Then, the auditor conducts the sampling auditing periodically to check the data integrity.

Public auditability and data dynamics for cloud data storage:

Working: Setup: The client's public key and private key are generated by invoking KeyGen(.). By running SigGen(.), the data file is preprocessed, and the homomorphic authenticators together with metadata are produced.

Default Integrity Verification: The client or TPA can verify the integrity of the outsourced data by challenging the server.

Dynamic Data Operation with Integrity Assurance(manipulation of MHT):

Data Modification: A basic data modification operation refers to the replacement of specified blocks with new ones.

Data Insertion: data insertion, refers to inserting new blocks after some specified positions in the data file.

Data Deletion: For single block deletion, it refers to deleting the specified block and moving all the latter blocks one block forward.

A dynamic audit service: It is used for files which are stored at cloud server. That's why the performance of audit service is different in different parameter which is based on file size, sampling rate and sector number per block.

The audit service architecture consist of four phases- 1)DO: store data on cloud. 2)CSP: provide data storage service. 3)TPA: having capability to manage outsource data. 4) Authorized application(AA): Can access data from cloud. To validate approaches, have implemented a prototype public audit service.

A cloud-based storage scheme: This scheme used in many techniques for static data and confidentiality requirement.

Working: cloud base storage scheme consists of four modules: OModule (owner module), CModule (CSP module), UModule (user module), and TModule (TTP module). OModule, which runs on the owner side, is a library to be used by the owner to perform the owner role in the setup and file preparation phase. CModule is a library that runs on Amazon EC2 and is used by the CSP to store, update, and retrieve data from Amazon S3. UModule is a library to be run at the authorized users' side, and include functionalities that allow users to interact with the TTP and the CSP to retrieve and access the outsourced data. TModule is a library used by the TTP to perform the TTP role in the setup and file preparation phase.

A flexible distributed storage integrity auditing:

Working: before subset of the indices, the requested response file distribution the user precomputes a certain number of short verification tokens on individual vector , each token covering a random subset of data blocks. Later, when the user wants to make sure the storage correctness for the data in the cloud, he challenges the cloud servers with a set of randomly generated block indices. Upon receiving challenge, each cloud server computes a short "signature" over the specified blocks and returns them to the user. The values of these signatures should match the corresponding tokens precomputed by the user.

6. COMPARISONS AND DRAWBACKS

Privacy preserving technique lack the rigorous performance analysis for the construction audit system so there is need to used dynamic auditing service with data privacy preserving scheme.

A BLS/RSA-based construction offers both public auditability and data dynamics. BLS-based instantiation having smaller size block as compare to the RSA- base instantiation, so it two times faster than RSA- base instantiation. However, it has larger computation cost at the verifier side as the pairing operation in BLS scheme consumes more time than RSA techniques. BLS construction is not suitable to use variable sized blocks the RSA construction can support variable sized blocks.

Audit services base on scheme may support great deal of audit tasks, and performance of this simple schedule is more

preferable than individual audit service. For detection of CSP's misbehavior in random sampling audit system used probabilistic query evaluation. But enormous audit activities would increase the computation and communication overheads of audit service. Less frequent activities may not detect errors in a timely manner. Therefore the scheduling of audit activities is significant for improving the quality of audit services.

Practical implementation of cloud base storage scheme based on four modules, which wants different environment to run and form a large network.

In cloud base storage scheme there is key issue to detect any unauthorized modification and corruption, in distributed environment this instances is successfully detected. The main aim of distributed system is to verify the errors in cloud storage system.

7. PROPOSED METHODOLOGY

Data storage on cloud having curious task it represents huge risk of security. Owners also worried about their sensitive data and loss of infrastructure, there are various reasons that not convenience owner to store data on cloud. These papers proposed method recycle storage to store loss data of cloud and for security improvement also proposed audit storage scheme.

7.1 Recycle storage:

Whenever data is no longer used by the user, CSP discard these data from cloud storage system. And shows like data still available and hide details of data from owner or user. When CSP discard data, it enters into recycle storage. Recycle storage store data for long while. When user demanding, that data provided to the user. This method is used to improve honesty of CSP.

Architecture:

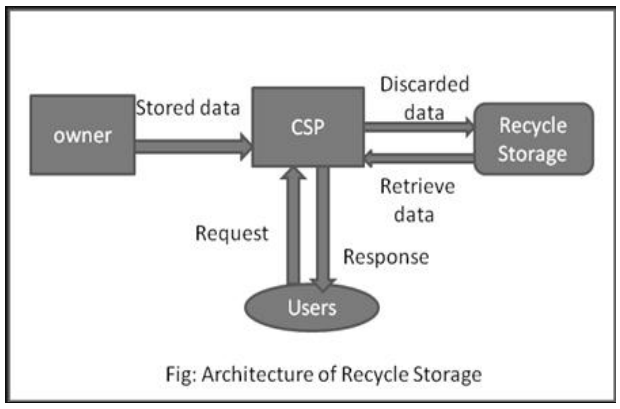

Fig: Architecture of Recycle Storage

Above figure shows the overview of Recycle Storage. There are four phases:

1 Owner: Move data on cloud server.

2 CSP: Store data on cloud and maintained, CSP discard data from cloud which was not longer used. And these data enters into recycle storage.

3 User: Access data on their demand. If data not present into cloud, CSP send request to the Recycle storage.

4 Recycle Storage: Send requested data to cloud server. CSP retrieve that data and send to demanding user.

7.2 Audit storage scheme:

When user first time login to cloud, CSP generate unique pin code and gives to user. User could perform operations on Cloud storage system to update data like data insertion, data deletions, data modification and appending. But it introduce various challenges on cloud storage system. Whenever use access data and update it, in cloud audit storage scheme users pin code generate on cloud server. Cloud server store this pin code proof with user account. CSP also having pin code this store on owner's machines, in multi-cloud environment deferent owners having unique (deferent from one another) pin code, If CSP update some data, pin code is tag implicitly (it work like CSP gives another pin code to owners machine). So owners of data could identify on local machine cloud service provider is honest or not.

8. EXPECTED RESULT

Recycle storage service improved reliability of cloud storage system.

If there are any updation on data block, owners of data knows about that updated block. Audit storage system reduces overheads of security on cloud storage system. Owners could trust on CSP for dynamic data on untrusted server. And user could access data as well as update it securely.

9. CONCLUSION

This paper design efficient security technique for data storage in cloud computing. First give the brief view of various existing techniques with their working and discus about various aspects regarding those techniques and also explain drawbacks. Paper proposed two methods regarding data storage and for providing security on cloud storage scheme. Using trusted third party scheme clients don't have right to update data dynamically but using audit storage scheme client can achieve this right. Recycle storage scheme could used to retrieve discarded data on cloud server and it improve performance of dynamic operations and availability of data.

10. FUTURE SCOPE

There need some improvement in audit storage so in future this scheme is used to support static as well as dynamic update operations on cloud storage. Separate storage for discarded data (recycle storage scheme) reduce overhead of memory space on cloud server, improved the performance of operation and reliability of data.

11. REFERENCES

[1] E-C. Chang and J.Xu, "Remote integrity check with dishonest storage server, " Proc, 13th European symp. Research in computer security (ESORICS' 08) pp.223 - July,2008

[2] Q. Wang, K. Ren, W. Lou, and Y. Zhang, "Dependable and Secure Sensor Data Storage with Dynamic Integrity Assurance," Proc. IEEE INFOCOM, pp. 954-962, Apr. 2009.

[3] J. Li, M.N. Krohn, D. Mazie`res, and D. Shasha, "Secure Untrusted Data Repository (SUNDR)," Proc. Sixth Conf. Symp. OperatingSystems Design Implementation, pp. 121-136, 2004.

[4] Kan Yang and Xiaohua Jia, Fellow- "An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing". IEEE Transaction On Parallel and distributed system Vol: 24 no 09, pp 1717-1726, Supt 2013.

[5] Qian Wang, Cong Wang, Kui Ren, Wenjing Lou, and Jin Li "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing," IEEE Transaction On Parallel And Distributed System Vol: 22, NO. 5, pp 847-859 MAY 2011.

[6] Yan Zhu, Gail-Joon Ahn, Hongxin Hu, Stephen S. Yau, Ho G. An, and Chang-Jun Hu "Dynamic Audit Services for Outsourced Storages in Clouds", IEEE Transaction On Services Computing, Vol: 6, NO. 2, pp 227-238APRIL-JUNE 2013.

[7] Ayad Barsoum and Anwar Hasan, "Enabling Dynamic Data and Indirect Mutual Trust for Cloud Computing Storage Systems", IEEE Transaction On Parallel And Distributed System, Vol: 24, NO. 12, pp 2375-2385, DECEMBER 2013.

[8] Cong Wang, Qian Wang, Kui Ren, Ning Cao, and Wenjing Lou, "Toward Secure and Dependable Storage Services in Cloud Computing", IEEE Transaction On Services Computing, Vol: 5, NO. 2, pp 220-232, APRIL-JUNE 2012.