ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 5, March 2017

# EFFICIENT AUDIT SERVICE OUTSOURCING FOR DATA INTEGRITY IN CLOUDS

[1]J.Pavithra, [2]V.Pavithra,[3]S.Sneka,[4]Mrs.A.Saravanan
[123]B.Tech., (CSE) , [4]Assistant Professor,
[1234]Department of CSE,
[1234]Kalasalingam University, Krishnan koil.
pavithrajayaprasath95@gmail.com

**ABSTRACT :**

Cloud computing is a forthcoming revolution in information technology (IT) industry because of its performance, accessibility i.e., cloud storage enables users to access their data anywhere and at any time, pay per use service. Cloud-based outsourced storage relieves the client's burden for storage management and maintenance by providing a comparably low-cost, scalable, location-independent platform. However, the reality that clients no longer have physical possession of data indicates that they are facing a potentially formidable risk for missing or corrupted data. To avoid the security risks, audit services are critical to make sure the integrity and availability of outsourced data and to achieve digital forensics and credibility on cloud computing.Provable data possession (PDP), which is a cryptographic technique for verifying the integrity of data without retrieving it at an un-trusted server, can be used to realize audit services. In this we introduced the building of a well-organized audit service for data integrity in clouds. Profiting from the typical interactive verification system, we predictable an interactive audit procedure to apply the audit service based on a third party auditor. In this audit inspection, the third party auditor can concern a periodic authentication to check the transform of outsourced data by providing an optimized to-do list. To realize the audit model, we only want to protect the security of the third party auditor and organize an insubstantial daemon to execute the verification protocol. We present askilled method for selecting abest parameter value to decreasecomputational expenditure of cloud audit services. Our results show the effectiveness of our approach.

## I.INTRODUCTION

In current days, the up-and-coming cloud-computing model is rapidly in move on force as an unconventional to traditional information technology. Cloud computing make available a scalability surroundings for growing amounts of data and processes that work on a variety of services and applications by means of on-demand self-services. One basiccharacteristic of this model shifting is that data are being centralized and outsourced into clouds. This kind of outsourced storage services in clouds have become a new profit growth point by providing a comparably low-cost, scalable, location-independent platform for managing client's data. The

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 5, March 2017

cloud storage service (CSS) relieves the load of storage management and maintenance. These security risks come from the subsequent reasons: the cloud infrastructures are much more great and reliable than private computing devices. However, they are still at risk to safety threats both from outside and inside the cloud for the benefits of their possession, there exist various motivations for cloud service providers (CSP) to actfalsely toward the cloud users furthermore, the dispute occasionally suffers from the be deficient in of trust on CSP. Thus, their behaviors may not be recognized by the cloud users, even if this dispute may outcome from the users own offensive operations. Traditional cryptographic technologies for data integrity and availability, based on hash functions and signature scheme, cannot work on the outsourced data not including a local copy of data. In addition, it is not a realisticresult for data validation by downloading them due to the sophisticated transaction, particularly for large-size files. Additionally, the solutions to audit the correctness of the data in a cloud environment can be formidable and expensive for the cloud users. As a result, it is important to realize public audit ability.

## II. RELATED WORK

The traditional cryptographic technologies for data integrity and availability, based on Hash functions and signature schemes [4], [5], cannot work on the outsourced data. It is not a practical solution for data validation by downloading them due to the expensive communications, especially for large size files. Moreover, the ability to audit the correctness of the data in a cloud environment can be formidable and expensive for the cloud users. Therefore, it is crucial to realize public audit ability for CSS, so that data owners (Dos) may resort to a third party auditor (TPA), who has expertise and capabilities that a common user does not have, for periodically auditing the outsourced data. This audit service is significantly important for digital forensics and credibility in clouds. To implement public audit ability, the notions of proof of irretrievability (POR) [6] and provable data possession (PDP) [7] have been proposed by some researchers. Their approach was based on a probabilistic proof technique for a storage provider to prove that clients' data remain intact.

There exist some solutions for audit services on out-sourced data. For example, Xie et al. [8] proposed an efficient method on content comparability for outsourced database, but it was not suitable for irregular data. Wang et al. [9] also provided a similar architecture for public audit services. To support their architecture, a public audit scheme was proposed with privacy-preserving property. However, the lack of rigorous performance analysis for a constructed audit system greatly affects the practical application of their scheme. For instance, in this scheme an outsourced file is directly split into n blocks, and then each block generates a verification tag. To maintain security, the length of block must be equal to the size of cryptosystem, that is, 160 bits, which is 20 bytes. This means that 1M bytes file is split into 50,000 blocks and generates 50,000 tags [10], and the storage of tags is at least 1M bytes. Therefore, it is inefficient to build an audit system based on this scheme. To address such a problem, we introduce a fragment technique to improve the system performance and reduce the extra storage.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 5, March 2017

Another major concern is the security issue of dynamic data operations for public audit services. In clouds, one of the core design principles is to provide dynamic scalability for various applications. This means that remotely stored data might be not only accessed by the clients but also dynamically updated by them, for instance, through block operations such as modification, deletion and insertion. However, these operations may raise security issues in most of existing schemes, e.g., the forgery of the verification metadata (called as tags) generated by DOs and the leakage of the user's secret key. Hence, it is crucial to develop a more efficient and secure mechanism for dynamic audit services, in which a potential adversary's advantage through dynamic data operations should be prohibited. [3] discussed about a method, Optimality results are presented for an end-to-end inference approach to correct(i.e., diagnose and repair) probabilistic network faults at minimum expected cost. One motivating application of using this end-to-end inference approach is an externally managed overlay network, where we cannot directly access and monitor nodes that are independently operated by different administrative domains, but instead we must infer failures via end to-end measurements. We show that first checking the node that is most likely faulty or has the least checking cost does not necessarily minimize the expected cost of correcting all faulty nodes. In view of this, we construct a potential function for identifying the candidate nodes, one of which should be first checked by an optimal strategy. Due to the difficulty of finding the best node from the set of candidate nodes, we propose several efficient heuristics that are suitable for correcting fault nodes in large-scale overlay networks. We show that the candidate node with the highest potential is actually the best node in at least 95% of time, and that checking first the candidate nodes can reduce the cost of correcting faulty nodes as compared to checking first the most likely faulty nodes.

## III. EXISTING SYSTEM

To securely introduce an effective third party auditor (TPA), the following two fundamental requirements had been met: TPA were been able to efficiently audit the cloud data storage without demanding the local copy of data, and introduce no additional on-line burden to the cloud user. The third party auditing process had not brought in any new vulnerability towards user data privacy. The cloud infrastructures are much more powerful and reliable than personal computing devices. However, they are still susceptible to security threats both fromoutside and inside the cloud for the benefits of their possession, there exist various motivations for cloud serviceproviders (CSP) to behave unfaithfully toward the cloud users furthermore, the dispute occasionally suffersfrom the lack of trust on CSP. Consequently, their behaviors may not be known by the cloud users, even if this dispute may result fromthe users' own improper operations.

## DRAWBACKS OF EXISTING SYSTEM

The disadvantages of the existing system are

- TPA demands retrieval of user data, here privacy is not preserved.
- TPA has to remember which key had been used.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 5, March 2017

- These two schemes good for static data not for dynamic data.

## IV. PROPOSED SYSTEM

Provable data possession (PDP) has been used, which is a cryptographic technique for verifying the integrity of data without retrieving it at an un-trusted server; can be used to realize audit services. It is a random mask technique to achieve a privacy-preserving public auditing system for cloud data storage security while keeping all above requirements in mind to support efficient Handling of multiple auditing tasks and further explore the technique of bilinear aggregate signature to extend our main result into a multiuser setting, where TPA can perform multiple auditing tasks simultaneously. Extensive security and performance analysis shows the proposed schemes are provably secure and highly efficient and also show how to extent our main scheme to support batch auditing for TPA upon delegations from multi-users.

### FEATURES OF PROPOSED SYSTEM

The advantages of the proposed system are

- Data verified in the cloud without download the source data.
- Data privacy is guaranteed in out proposed system.
- Key verification set is used for higher level data security for file access in cloud.
- Every user should be register in cloud if the user wants to access the data. It is help to identify the data spread in the world.

## V. MODULE DESCRIPTION

### AUDIT SERVICE SYSTEM

This module provides an efficient and secure cryptographic interactive audit scheme for public audit ability. An efficient and secure cryptographic interactive retains the soundness property and zero-knowledge property of proof systems. These two properties not only prevent the deception and forgery of cloud storage providers, but also prevent the leakage of outsourced data in the process of verification.

### DATA STORAGE SERVICE SYSTEM

This module includes four entities to store the data in secure manner:

**Data owner (DO)**

DO have store a large amount of data in the cloud.

**Cloud service provider (CSP)**

CSP provides data storage service and has enough storage spaces and computation resources.

**Third party auditor (TPA)**

TPA has capabilities to manage or monitor – outsourced data under the delegation of data owner.

**Granted applications (GA)**

GA has the right to access and manipulate stored data. These applications can be in either inside clouds or outside clouds according to the specific requirements.

### AUDIT OUTSOURCING SERVICE SYSTEM

In this module the client (data owner) uses the secret key to preprocess the file, which consists of a collection of blocks, generates a set of public verification information that is stored in TPA, transmits the file and some verification tags to cloud service providerCSP, and may delete its local copy.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 5, March 2017

At a later time, using a protocol of proof of irretrievability TPA (as an audit agent of clients) issues a challenge to audit (or check) the integrity and availability of the outsourced data in terms of the public verification information. It is necessary to give an alarm for abnormal events.

## SECURE AND PERFORMANCE ANALYSIS

This module is used to secure the data and give performance to the following:

**Audit-without-downloading**

It allows TPA (or other clients with the help of TPA) to verify the correctness of cloud data on demand without retrieving a copy of whole data or introducing additional on-line burden to the cloud users.

**Verification-correctness**

To ensure there exists no cheating CSP that can pass the audit from TPA without indeed storing users' data intact.

**Privacy-preserving**

To ensure that there exists no way for TPA to derive user's data from the information collected during the auditing process.

**High-performance**

To allow TPA to perform auditing with minimum overheads in storage, communication and computation, and to support statistical audit sampling and optimized audit schedule with a long enough period of time.

## VI.CONSTRUCTION OF INTERACTIVE AUDIT SCHEME

In this section, we propose a cryptographic interactive audit scheme to support our audit system in clouds. This scheme is constructed on the standard model of interactive proof system, which can ensure the confidentiality of secret data (zero-knowledge property) and un-decidability of invalid tags (soundness property).A key-aggregate encryption scheme consists of five polynomial-time algorithms as follows.

The data owner establishes the public system parameter via Setup and generates a public/master secret key pair via KeyGen. Messages can be encrypted via Encrypt by anyone who also decides what cipher text class is associated with the plaintext message to be encrypted. The data owner can use the master-secret to generate an aggregate decryption key for a set of cipher text classes via Extract. The generated keys can be passed to delegates securely (via secure e-mails or secure devices) finally; any user with an aggregate key can decrypt any cipher text provided that the cipher text's class is contained in the aggregate key via Decrypt.

## VII. IMPLEMENTATION AND RESULTS

To authorize the effectiveness of our approach, we have implemented a prototype of an audit system based on our proposed solution. This system have been developed in an experimental cloud computing system environment, which is constructed within the framework of the IaaS to provide powerful virtualization, distributed storage, and automated management.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 5, March 2017

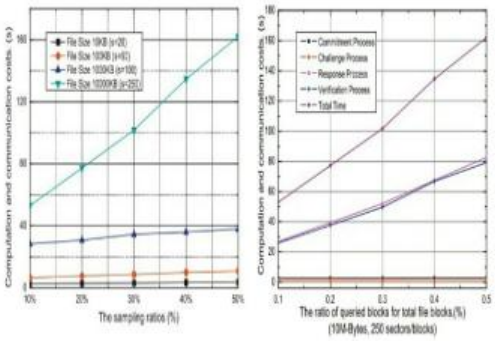


**Fig.1: Experiment results under different file size, sampling ratio, and sector number**.

## VIII.CONCLUSION

In this paper, the construction of an efficient audit service for data integrity in clouds has been addressed. Profiting from the standard interactive proof system and proposed an interactive audit protocol to implement the audit service based on a third party auditor. In this audit service, the third party auditor, known as an agent of data owners, can issue a periodic verification to monitor the change of outsourced data by providing an optimized schedule. To realize the audit model, only need to maintain the security of the third party auditor and deploy a lightweight daemon to execute the verification protocol. Hence, this technology can be easily adopted in a cloud computing environment. This experiment clearly showed that this approach could minimize computation and communication overheads.

## IX.REFERENCES

[1].C. Wang, Q. Wang, K. Ren, and W. Lou, “Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing,” Proc. IEEE INFOCOM, pp. 1-9, 2010.

[2].Syam Kumar P, Subramanian R “An Efficient and Secure Protocol for Ensuring Data Storage Security in Cloud Computing” In International Journal of Computer Science Issues, Vol. 8, Issue6, No 1, November 2011.

[3].Christo Ananth, Mona, Kamali, Kausalya, Muthulakshmi, P.Arthy, “Efficient Cost Correction of Faulty Overlay nodes”, International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE), Volume 1,Issue 1, August 2015,pp:26-28

[4].Ning Cao, Cong Wang, Ming Li, KuiRen and Wenjing Lou, "Privacy-Preserving Multi-keyword Ranked Search over Encrypted Cloud Data,"IEEE Transactions on Parallel andDistributed Systems(TPDS), Jan. 2014.