DATA INTEGRITY AND AVAILABILITY FOR CROSS CLOUD ENVIRONMENT BY USING CPDP SCHEME

Khudaija Nazhath M R[1], Pushpa.S.Tempad[2]

[1]Student, [2]Assistant Professor, Dept. of Computer Science and Engineering,
STJIT, Ranebennur (India)

ABSTRACT

In recent years, cloud storage service has become a faster profit growth point by providing a comparably scalable, position-independent, low -cost platform for client's data. Since cloud computing environment is constructed based on open architectures and interfaces. It has the capability to incorporate multiple internal and external cloud services together to provide high interoperability there can be multiple accounts associated with a single or multiple service providers (SPs).so, Security in terms of integrity is most important aspect in cloud computing environment. Cooperative Provable data possession (CPDP) is a technique for ensuring the integrity of data in storage outsourcing. Therefore, we address the construction of an efficient CPDP scheme and dynamic audit service for distributed cloud storage as well verifying the integrity guarantee of an entrusted and outsourced storage which support the scalability of service and data migration.

Keywords: Availability, Cloud Admin, Integrity,Multicloud, TTP, Verification

I. INTRODUCTION

Cloud Computing, which is an Internet-based development and use of computer technology. Consider the large size of the outsourced electronic data and the client's constrained resource capability, the core of the problem can be generalized as how can the client find an efficient way to perform periodical integrity verifications without the local copy of data files.

The main objective of this paper is to provide security in terms of integrity and availability of client's data which is stored on cloud. This paper shall not put any burden on to computation and communication and further, performance guarantee shall also be taken care of by allowing trusted third party to verify the correctness of the cloud data on demand without retrieving a copy of the whole data or introducing additional on-line burden to cloud users. Several schemes are proposed to solve the problem. Those schemes focus on achieve the following requirements: high efficiency, stateless verification, retrievability of data, unbounded use of queries and public verification. In general, if one scheme supports private verification, it can possess higher efficiency,new challenges and new problems.

One of the most important and most attention issues, that is in the cloud environment, servers within the data storage with security in terms of integrity verification. For example, storage service providers may order their own interests to save the data to hide an error, more seriously, storage service providers in order to save cost and storage space, deliberately remove rarely accessed data, and then who, due to extensive confidential information, outsourcing and limited computing power users.

Therefore, how to backup data files in the user not the case, found an efficient and securely ways of good information to perform periodically verification, allowing users to know his information file is stored securely on the server, this data storage is cloud computing environment is an important security issue (fig 1).

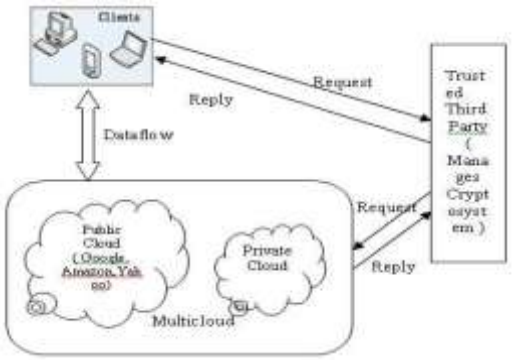

Figure 1: Verification of Integrity

II. EXISTING SYSTEM

Although existing CPDP schemes offer a publicly accessible remote interface for checking and managing the tremendous amount of data, the majority of existing CPDP schemes is incapable to satisfy the inherent requirements from multiple clouds in terms of communication and computation costs. To address this problem, we consider a multi-cloud storage service.

2.1 Disadvantage

- Integrity with lower computation and communication.
- Integrity is affected by the bilinear mapping operations due to its high complexity.

III. PROPOSED SYSTEM

Clients who have a large amount of data to be stored in multiple clouds and have the permissions to access and manipulate stored data Cloud Service Providers (CSPs) who work together to provide data storage services and have enough storages and computation resources. And Trusted Third Party (TTP) who is trusted to store verification parameters and offer public query services for these parameters.

We consider the existence of multiple CSPs to cooperatively store and maintain the clients' data. Moreover, a cooperative PDP is used to verify the integrity and availability of their stored data in all CSPs. The verification procedure is described as follows: Firstly, a client (data owner) uses the secret key to pre-process a file which consists of a collection of n blocks, generates a set of public verification information that is stored in TTP, transmits the file and some verification tags to CSPs, and may delete its local copy; Then, by using a verification protocol, the clients can issue a challenge for one CSP to check the integrity and availability of outsourced data with respect to public information stored in TTP.

3.1 Advantages

- Making information storage, bandwidth and computational smaller, more efficient.
- Unlimited number of storage server authentication.
- Provides a public authentication method.
- Entrusted storage server.

IV. DESIGN OF THE SYSTEM

4.1 Input Design

The input design is the link between the information system and the user. It comprises the developing specification and procedures for data preparation and those steps are necessary to put transaction data in to a usable form for processing can be achieved by inspecting the computer to read data from a written or printed document or it can occur by having people keying the data directly into the system. The design of input focuses on controlling the amount of input required, controlling the errors, avoiding delay, avoiding extra steps and keeping the process simple. The input is designed in such a way so that it provides security and ease of use with retaining the privacy. Input Design considered the following things:

- What data should be given as input?
- How the data should be arranged or coded?
- The dialog to guide the operating personnel in providing input.
- Methods for preparing input validations and steps to follow when error occur.

4.2 Objectives

1. Input Design is the process of converting a user-oriented description of the input into a computer-based system. This design is important to avoid errors in the data input process and show the correct direction to the management for getting correct information from the computerized system.

2. It is achieved by creating user-friendly screens for the data entry to handle large volume of data. The goal of designing input is to make data entry easier and to be free from errors. The data entry screen is designed in such a way that all the data manipulates can be performed. It also provides record viewing facilities.

3. When the data is entered it will check for its validity. Data can be entered with the help of screens. Appropriate messages are provided as when needed so that the user will not be in maize of instant. Thus the objective of input design is to create an input layout that is easy to follow.

4.3 Output Design

A quality output is one, which meets the requirements of the end user and presents the information clearly. In any system results of processing are communicated to the users and to other system through outputs. In output design it is determined how the information is to be displaced for immediate need and also the hard copy output. It is the most important and direct source information to the user. Efficient and intelligent output design improves the system's relationship to help user decision-making.

1. Designing computer output should proceed in an organized, well thought out manner; the right output must be developed while ensuring that each output element is designed so that people will find the system can use easily and effectively. When analysis design computer output, they should Identify the specific output that is needed to meet the requirements.

2. Select methods for presenting information.

3. Create document, report, or other formats that contain information produced by the system.

The output form of an information system should accomplish one or more of the following objectives.

- Convey information about past activities, current status or projections of the
- Future.

- Signal important events, opportunities, problems, or warnings.
- Trigger an action.
- Confirm an action.

4.4 Module Description

4.4.1 Number of Modules

After careful analysis the system has been identified to have the following modules:

- **Cloud Computing Module.**
- **Cooperative Provable Data Possession Module.**
- **Data Storage Module.**
- **Integrity Verification Module.**

4.4.1.1 Cloud Computing Module

Cloud Computing, which is an Internet-based development and use of computer technology. Consider the large size of the outsourced electronic data and the client's constrained resource capability, the core of the problem can be generalized as how can the client find an efficient way to perform periodical integrity verifications without the local copy of data files. The main objective of this paper is to provide security in terms of integrity and availability of client's data which is stored on cloud.

4.4.1.2 Cooperative Provable Data Possession Module:

Proposed a data storage proved cooperative Provable Data Possession (CPDP) system, which applies to of cloud in an entrusted storage server, based on Diffie-Hellman protocol systems of main plant with state verify that the label is used to check the integrity of the data stored in the cloud, which allows unlimited number of storage server authentication, and also provides a public authentication method,

4.4.1.3 Data Storage Module:

A data storage service involves three different entities: Clients who have a large amount of data to be stored in multiple clouds and have the permissions to access and manipulate stored data Cloud Service Providers (CSPs) who work together to provide data storage services and have enough storages and computation resources and Trusted Third Party (TTP) who is trusted to store verification parameters and offer public query services for these parameters.

4.4.1.4 Integrity Verification Module

Integrity verification in Multi cloud that is provided by improving the existing proof of storage models by manipulating the classic Merkle Hash Tree construction for block tag authentication. To support efficient handling of multiple auditing tasks, this paper further explore the technique of bilinear aggregate signature to extend the main result into a multiuser setting, where TPA can perform multiple auditing tasks simultaneously.

V. CONCLUSION

We focused the core issues, if an untrusted server to store customer information. We can use cooperative provable data possession scheme, which reduce the data block access, and amount of computation on the server and client. Also decreases server traffic.

Our design and development on the CPDP program is mainly based on the usage of Public and Private Key encryption system. It exceeds what we did in the past; the improvement has brought to the bandwidth, computation and storage system. And it applied the public (trusted third party) verification. Finally, we also

expect our program; it supports dynamic outsourcing of information make it a more realistic application of cloud computing environment.

VI. ACKNOWLEDGEMENT

I consider it is a privilege to express my gratitude and respect to all those who guiding me in the progress of my paper.

I wish my grateful thanks to ***Mrs. Pushpa.S.Tempad*** *M.Tech*, project guide, for invaluable support and guidance.

KHUDAIJA NAZHATH M R

REFERENCES

[1]. Yan Zhu, Hongxin Hu, Gail-Joon Ahn,"Cooperative Provable Data Possession for Integrity Verification in Multi-Cloud Storage" IEEE Transactions On Parallel And Distributed Systems,Digital Object Indentifier 10.1109/TPDS 2012.66 April 2012.

[2]. G. Ateniese, R. C. Burns, R. Curtmola, J. Herring, L. Kissner, Z. N. J. Peterson, and D. X. Song, "Hybrid Provable Data Possession at Untrusted Stores In Cloud Computing," in IEEE Conference on the 7th International Conference On Parallel And Distributed Systems 10.1109/ICTPDS 2011.70.

[3]. Y. Zhu, H. Hu, G.-J. Ahn, Y. Han, and S. Chen,"Collaborative integrity verification in hybrid clouds," in IEEE Conference on the 7th International Conference on Collaborative Computing: Networking Applications and Worksharing, collaborateCom, Orlando,Florida, USA, October 15-18, 2011, pp. 197–206

[4]. Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu, and S. S. Yau, "Study on the Third-party Audit in Cloud Storage Service s," in IEEE TRANSACTIONS ON SERVICES COMPUTING, Digital Object Indentifier 10. 1109/ TCS.2011.51.

[5]. Qian Wang,, Cong Wang, Kui Ren, Wenjing Lou, and Jin Li "Dynamic audit services for integrity verification ofoutsourced storages in clouds", VOL. 22, NO. 5, MAY 201, 1045- 9219/11/$26.00 2011 IEEE. 10.1109/ IMCCC. 2011.135.

[6]. Qian Wang, Cong Wang, Kui Ren, Wenjing Lou, and Jin Li "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing" IEEE Transactions on Parallel And Distributed Systems.