Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 5, May 2014, pg.1046 – 1050

RESEARCH ARTICLE

Verifying Data Integrity in Hybrid Cloud

Sachin Lakade[1], Mirza Baig[2]

[1]Computer Science and Engineering & RTMNU, India

[2]Computer Science and Engineering & RTMNU, India

[1] sachinlakde@gmail.com; [2] mirzammb@gmail.com

Abstract— In this paper we are going to say an efficient technique that describe how integrity is maintained in storage of the data. Cloud computing is used to store the data from various resources by the user. It is very complex for the user to store whole data within the system. In that case cloud has to provide to store as much large amount of the data as user wants. This Stored data has to be integrated by cloud in very efficient way and maintain with the help of Trusted Third Party Auditor (TTPA). In this paper, we present two scheme based on homomorphism verifiable response and hash index hierarchy. We propose a secure cloud storage system supporting data integrity and availability in multi-cloud storage. We further extend our result to enable the TPA to monitor for multiple users simultaneously and efficiently. Our resulting is focuses on introduces lower computation & communication overheads in comparison with the non co-operative approaches.

Keywords — Cloud Computing Security; data availability; data integrity; TTPA; key Cryptography; Multi-cloud Storage

I. INTRODUCTION

In cloud computing, one of the core design principles is dynamic scalability, which guarantees cloud storage service to handle growing amounts of application data in a flexible manner or to be readily enlarged. By integrating multiple private and public cloud services, Multi-clouds can effectively provide dynamic scalability of service and data migration. Parallel computing can be implemented in several ways of computing like instruction level, bit level, task and data parallelism. Based on the level at which hardware supports parallelism, it can be classified as multi-core and multi-processor. Although Provable Data Possession schemes evolved around public clouds offer a publicly accessible remote interface to check and manage the tremendous amount of data, the majority of existing Provable Data Possession schemes are incapable of satisfying such an inherent requirement of hybrid clouds in terms of bandwidth and time.

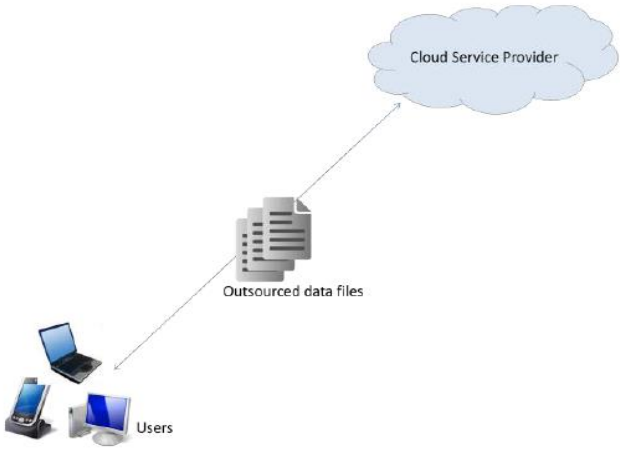

Fig 1 Cloud Data Storage Architecture

In this work, we focus on the construction of Provable Data Possession scheme for hybrid clouds, supporting privacy protection and dynamic scalability. We first provide an effective construction of Cooperative Provable Data Possession using Homomorphic[1] Verifiable Responses (HVR) and Hash Index Hierarchy (HIH)[1]. This construction uses homomorphic property, such that the responses of the client's challenge computed from multiple CSPs can be combined into a single response as the final result of hybrid clouds[3]. By using this mechanism, the clients can be convinced of data possession without knowing what machines or in which geographical locations their files reside. More importantly, a new hash index hierarchy is proposed for the clients to seamlessly store and manage the resources [3] in hybrid clouds. Our experimental results also validate the effectiveness of our construction.

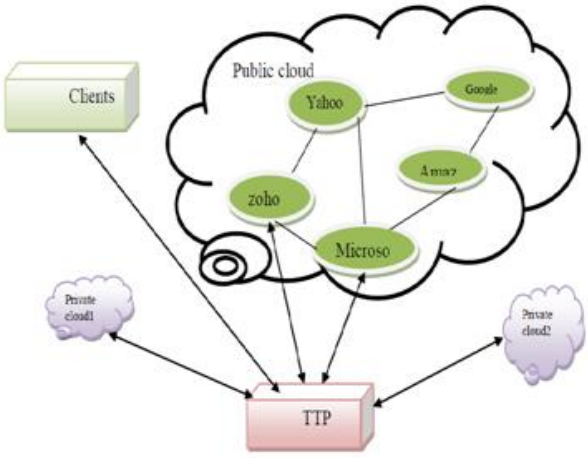

Fig. 2 Architecture of Data Integrity

Outages and security breaches of noteworthy cloud services appear from time to time. Amazon S3"s recent downtime [5], Gmail's mass email deletion incident [6] is such examples. For benefits of their own, there are various motivations for CSPs to behave unfaithfully toward cloud customers regarding the status of their outsourced data.

II. PROBLEM DEFINITION

Users resort to data replication to ensure the availability and durability of their sensitive data, especially if it cannot easily be reproduced. In the Cloud Computing paradigm, customers rely on the CSP to undertake the data replication task relieving the burden of local data storage and maintenance, but they have to pay for their usage of the CSP's storage infrastructure. On the other side, cloud customers should be securely and efficiently convinced that the CSP is actually possessing all data copies that are agreed upon, these data copies are complete and intact, and thus customers are getting the service they are paying for. Therefore, in this paper we address the problem of creating multiple copies of owner's data file over untrusted CSP and auditing all these copies to verify their completeness and correctness.

III. LITERATURE SURVEY

Provable data possession (PDP) is a methodology for validating the integrity of data in outsourcing storage service. The fundamental goal of the PDP scheme is to allow a verifier to efficiently, periodically, and securely validate that a remote server — which supposedly stores the owner's potentially very large amount of data — is not cheating the verifier. The problem of data integrity over remote servers has been addressed for many years and there is a simple solution to tackle this problem as follows. First, the data owner computes a message authentication code (MAC) of the whole file before outsourcing to a remote server. Then, the owner keeps only the computed MAC on his local storage, sends the file to the remote server, and deletes the local copy of the file. Later , whenever a verifier needs to check the data integrity.

PDP Schemes of Deswarte et al. Deswarte et al. [8] thought of a better solution by using two functions f and H'. H' is a one-way function and f is another function such that $f(C,H'(File)) = H(C||File)$, where H is any secure hash function and C is a random challenge number sent from the verifier to the remote server.

IV. STRUCTURE & TECHNIQUE

Data protection technology was launched by cipher cloud in which tokenization and encryption of data is provided by a web proxy before sending the data to the cloud application. This technology does not have much effect on the application. Another technology has been adopted known as okta that was designed to speed up the cloud applications by the integrating the cloud applications with that of the previous ones and this helps the users to quickly access the cross platforms.

A. *Verification of Multi-Cloud Framework*

Multi-cloud technique is the use of two or more cloud services to minimize the risk of large amount of data loss or temporary fault in the computers due to a localized component failure in a cloud computing environment. Such a failure may occur in hardware, software, or infrastructure.

A multi-cloud approach is also used to control the traffic from different customer bases or partners through the fastest possible parts of the network. Some clouds are better suited than others for a particular task.

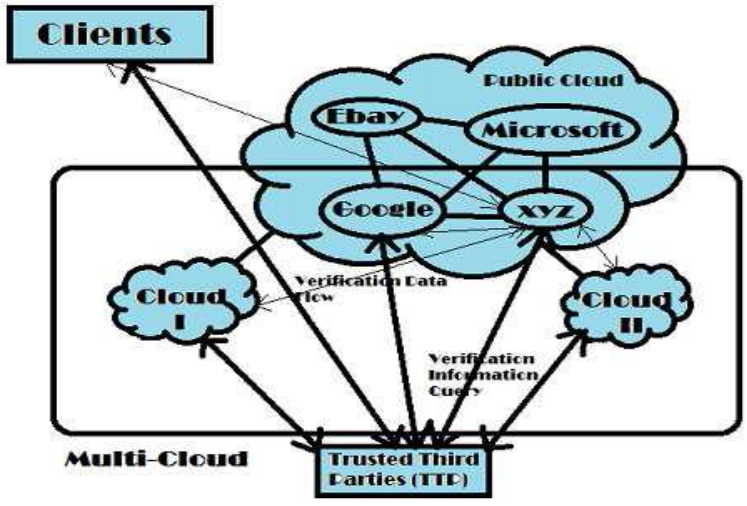

Fig. 3 Multi-cloud working principle

B. *Cooperative PDP*

Based on zero knowledge proof system and interactive proof system we prove the integrity of data stored in a multi cloud. A CPDP is a collection of two algorithms (Key Gen, Tag Gen) and interactive proof system Proof.

· Key Gen : It takes a security parameter as an input and returns a secret key as output.

· Tag Gen : It takes a secret key, file and set of cloud storage providers as input and returns triples.
· |Proof : It is a protocol of proof of data possession between the CSP's and verifier.
Let H = { Hk } be a family of hash functions
where Hk : index by k ε K.

This algorithm has a benefit in breaking the collision resistance of H. Collision-Resistance H: In this a hash family H(t, ε) collision resistant if no t-Time adversary has advantage at least ε in breaking collision of H. First the KeyGen algorithm is run in this scheme to obtain the public or the private key for users. Then TagGen is generated by the clients for the outsourced data.

C. *Hash Index Hierarchy for CPDP*
Three layers are used to illustrate the relationships among the blocks for stored resources .They are as follows:
1. Layer 1 : Express Layer shows representation of stored resources.
2. Layer 2 : Service Layer offers and manages cloud storage and services and
3. Layer 3 : Storage Layer realizes data storage on physical devices.

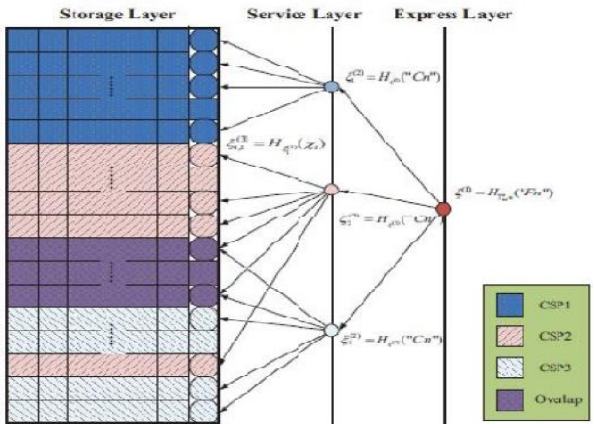

Fig. 4 Representation of hash index hierarchy working

D. *Homomorphic Verifiable Response for CPDP*
A homomorphism is a map f : P Q between two groups such that f (g1+ g2) = f(g1) x f(g2) for all g1,g2 ε P, where + denotes the operation in P and x denotes the operation in Q. Homomorphic verifiable response is the key technique of CPDP because it not only reduces the communication bandwidth, but also conceals the location of outsourced data in the distributed cloud storage environment

V. CONCLUSION

In this paper, we addressed the construction of PDP scheme for hybrid clouds. Based on homomorphic verifiable responses and hash index hierarchy, we proposed a cooperative PDP scheme to support dynamic scalability on multiple storage servers. Our focuses are that our schemes require a small, constant amount of overhead.

REFERENCES

[1] Yan Zhu, Hongxin Hu, Gail-Joon Ahn "Cooperative Provable Data Possession for Integrity Verification in Multi-Cloud Storage", *IEEE Parallel and distributed systems*, vol. 13, no. 5, pp. 14–22,2012.

[2] H. Shacham and B. Waters, "Compact proofs of retrievability," in*ASIACRYPT*, ser. Lecture Notes in Computer Science, J. Pieprzyk, Ed., vol. 5350. Springer, 2008, pp. 90–107.

[3] C. Wang, Q. Wang, K. Ren, "Privacy-preserving public auditing for storage security in cloud computing", in *Proc. of IEEE INFOCOM'10*, San Diego, CA, USA, March 2010.

[4] 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, Orlando, Florida, USA, October 15-18, 2011, pp. 197–206.

[5] Kavitha Murugesan, Shilpa Sudheendran "Ensuring User Security and Data Integrity in MultiCloud" nternational Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-3, Issue-2, May 2013.

[6] P. Jaikar & M. V. Nimbalkar IOSR Journal of Computer Engineering (IOSRJCE) ISSN: 2278-0661 Volume 1, Issue 6 (July-Aug. 2012), PP 43-49 "Securing Cloud Data Storage"

[7] R. Sravan kumar and Saxena ,"Data integrity proofs in cloud storage" in IEEE 2011.

[8] Priyanka V. Mogre, Girish Agarwal, Pragati Patil "Data Security and its techniques in Cloud Storage – A Review" Author Name et. al. / International Journal of Engineering Research and Technology Vol. 1 (02), 2012, ISSN 2278 – 181

[9] A. Juels, J. Burton, and S. Kaliski, "PORs: Proofs of Retrievability for Large Files," Proc. ACM CCS „07, Oct. 2007, pp. 584–97.

[10] B. Sotomayor, R. S. Montero,and I. T. Foster, "Virtual infrastructure management in private and hybrid clouds," IEEE Internet Computing, vol. 13, no. 5, pp. 14–22, 2009.

