ISSN: 2320-1363

Verifying Integrity and Authentication in Multi-Cloud Storage

A.Phanindra Kumar*1, Mr.G.Rama Swamy*2

M.Tech (CSE) Student Department of CSE, Priyadarshini Institute of Technology & Science, Chintalapudi, Guntur(Dist), Ap, India.

Professor, Principle in Priyadarshini Institute of Technology & Science, Chintalapudi, Guntur(Dist), Ap, India

ABSTRACT

Provable data retention is a technique which certain the security of data in storage outsourcing. In this article we are going to say an efficient technique that describes how integrity is maintained in storage of the data. We provide this by using the concept of provable data possession which supports a good service and migration if data in a distributed cloud environment, where we take into account of multi-cloud service to store and also to maintain the data of the clients. We are present a Cooperative Provable Data Possession (CPDP) system based on homomorphic verifiable response. Security of the system is proved based on a scheme zero-knowledge proof system. We use optimal parameters to improve the system performance and cost of computation for the client and cloud storage providers.

Keywords: Provable Data Possession, Multi-Cloud, Cooperative, Zero Knowledge

1. Introduction

Cloud Computing is a web based application which provides computation, software, infrastructure, platform, devices and other resources to users on a pay as you use basis. The cloud services can be utilized by the consumers without installation and their personal files can be access from any computer with internet access. This technology provides more effective computing by organizing bandwidth and data storage and processing. In cloud computing one of the core design principle 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 hybrid clouds can effectively provide dynamic scalability of service and data from multiple private or public provides into a backup or archive file or service might capture the data from other services from

ISSN: 2320-1363

private clouds, but the intermediate data and results are stored in hybrid clouds. Provable data possession is such a probabilistic proof technique for storage provider to prove the integrity and ownership of client data without downloading data. The proof checking without downloading makes it especially important for large size files and folders to check whether these data have been tampered with or deleted without downloading the latest version of data. Thus it is able to replace traditional hash and signature functions in storage outsourcing. Various PDP schemes have been recently proposed such as scalable PDP and Dynamic PDP. However these schemes mainly focus on PDP issues at un-trusted services in a single cloud storage provider and are not suitable for a multi-cloud environment. Although various security models have been proposed for existing PDP schemes these models still cannot cover all security requirement, especially for provable secure privacy preservation and ownership authentication in. summary a verification scheme for data integrity in distributed storage environment should have the following features.

Usability aspect: A client should utilize the integrity check in the way of collaboration services. The scheme should conceal the details of the storage to reduce the burden on clients.

Security aspect: The aspect should provide adequate security features to resist some existing attacks, such as data leakage attack and tag forgery attack.

Performance aspect: the scheme should have the lower communication and computation overheads than non-cooperative solution.

Related Work

To ensure the integrity and availability of outsourced data in cloud storages, researchers have proposed two basec approaches called Provable data retention and Proofs of Retrievability. First proposed the PDR model for ensuring retention of files on untrusted storages and provided an RSA-based technique for a static case that achieves the communication cost. This property greatly extended application areas of PDR protocol due to the separation of data owners and the users. However, these techniques are insecure against replay

ISSN: 2320-1363

attacks in dynamic scenarios because of the dependencies on the index of blocks. Moreover they do not fit for multi-cloud storage due to the loss of homomorphisam property in the authentication process. Our contribution, in this paper we address the problem of provable data retention in distributed cloud environments from the following aspects: high performance, transparent authentication, and high security. To achieve these goals, we first proposes a authentication framework for multi-cloud storage along with two fundamental techniques: homomorphic verifiable response and hash index hierarchy. we further introduce an effective construction CPDR technique using above mentioned structure.

2. Structure and Techniques

In this section we present our authentication framework for multi-cloud storage and formal definition of CPDP. Here we introduce two fundamental techniques for constructing our CPDP technique: hash index hierarchy on which the responses of the clients challenges computed from multiple CSPs can be combined into a single response as the final result, and homomorphic verifiable response, these are supports distributed cloud storage in a multi-cloud storage and implements an efficient construction of collision resistant hash function, which can be viewed as a random oracle model in the authentication protocol. The clients are allowed to dynamically access and update their data for various applications and the verification process of PDP is seamlessly performed for the clients in multi clouds. Hence it is a challenging problem to design a PDP scheme for supporting dynamic scalability.

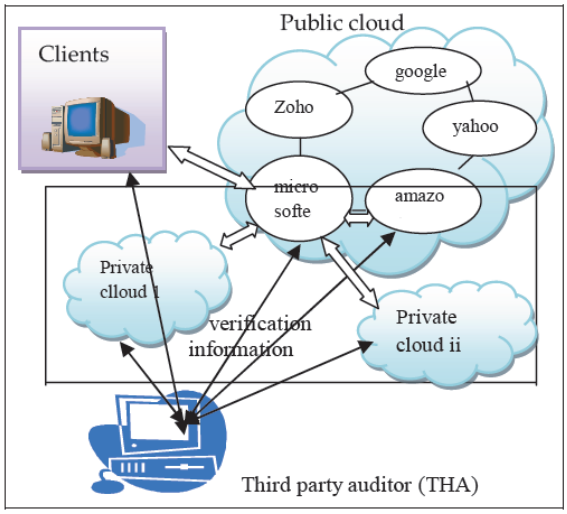

Fig.2.1 verification architecture for data integrity.

In this work we focus on the construction of PDP scheme for multi clouds, supporting

ISSN: 2320-1363

privacy protection and dynamic scalability. We first provide an effective construction of Cooperative Provable Data Possession (CPDP) using Homographic Verifiable Responses (HVR) and Hash Index Hierarchy (HIH). This construction uses homographic property such that the responses of the clients challenge computed from multiple CSPs can be combined into a single response as the client 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 in multi clouds. Our experimental results also validate the effectiveness of our construction.

2.1 Cooperative Provable Data Possession

Based on zero-knowledge proof system and interactive proof system we prove the integrity of data stored in a multi cloud. In this section, we introduce the principles of our cooperative provable data possession for hybrid clouds including the main technique, model, fragment structure, index hierarchy and the architecture to support our scheme.

2.2 Definition of CPDP model

In order to prove the integrity of data stored in Multi clouds, we define a framework for Cooperative Provable Data Possession (CPDP). To realize the CPDP, a trivial way is to check the data stored in each cloud one by one. However it would cause significant cost growth in terms of communication and computation overheads. It is obviously unreasonable to adopt such a primitive approach that diminishes the advantages of cloud storage scaling arbitrarily up and down on demand.

2.3 Fragment Structure of CPDP

We propose a fragment structure of CPDP scheme based on the above mentioned model as shown in fig 2.3.1, which has following characters: 1) A file is split into n x s sectors and each block corresponds to tag, so that the storage of signature tags can be reduced with the order of s. 2) The verifier can check the integrity of a file by random sampling approach which is a matter of the utmost importance for large or huge files. 3) This structure relies on

ISSN: 2320-1363

homomorphism properties to aggregate the data and tags into a constant size response which minimize network communication overheads.

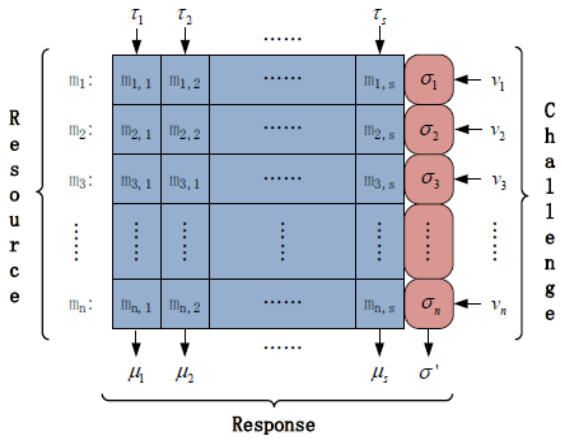

Fig.2.3.1 The fragment structure of CPDP model

The above structure considered as a common representation for some existing schemes [2, 4], can be converted to MAC based ECC or RSA schemes. By using BLS signature and random oracle model it is easy to design a practical CPDP scheme with the shortest homomorphism verifiable responses for public verifiability. This structure also creates favorable conditions for the architecture of CSPs.

2.4 Hash Index Hierarchy for CPDP

Three layers are used to illustrate the relationships among the blocks for stored resources. They are as follows:

- Express Layer: It shows representation of stored resources.
- Service Layer: It offers and manages cloud storage and services and
- Storage Layer: realizes data storage on physical layer

This architecture naturally accommodated the hierarchical representation of file system. We make use of a simple hierarchy to organize multiple CSP services, which involve private cloud or public clouds, by shading the differences between these clouds. In Fig.2.3.1 the resources in the express layer are split and stored into three CSPs in the service layers. In turn each CSP fragments and stores the assigned data into the storage services in the storage layer. This architecture could provide some special functions for data storage and management e.g. there may exist an overlap among data blocks and discontinuous blocks.

ISSN: 2320-1363

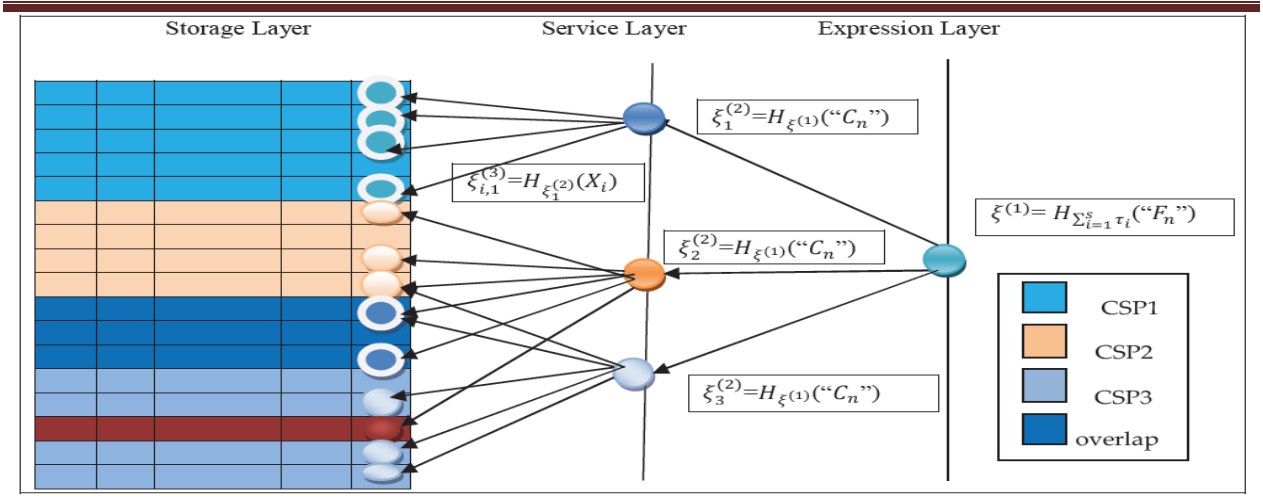

Fig. 2.3.1 The architecture of CPDP model.

They share several common character for the implementation of the CPDR framework in the multiple clouds: 1) a file is split into n x s sectors and each block corresponds to a tag, so that the storage of signature tags can be reduced by the increase of s; 2) a verifier can verify the integrity of file in random sampling approach, which is of utmost importance for large files; 3) these techniques rely on homomorphic properties to aggregate data and tags into a constant size response, which minimizes the overhead of network communication; 4) the hierarchy structure provides a virtualization approach to conceal the storage details of multiple CSPs.

We employ this architecture to construct a new Hash Index Hierarchy H, which is used to replace the hash function in original PDP schemes. By using this structure it is obvious that our CPDP scheme can also support dynamic data operations.

3 Performance Analysis

We are implemented out PDP scheme and validated the effect of dispersed secret data on private clouds and hybrid clouds. The code was written in C++ and the experiments were run on an Intel Core 2 processor with 2.16GHz. All cryptographic operations utilize the QT and bilinear cryptographic library. In our CPDP scheme, the client's communication overhead is not

ISSN: 2320-1363

changed in contrast to common PDP scheme, and the interaction among CSPs needs c-1 times constant size communication overheads, where c is the number of CSPs in hybrid clouds. Therefore the total of communication overheads is not significantly increased. Next we evaluate the performance of our CPDP scheme in terms of computational overhead. Another advantage of probabilistic verification based on random sampling is that it is easy to identify the tempering or forging data blocks or tags. The identification function is obvious: when the verification fails, we can choose the partial set of challenging indexes as a new challenging set, and continue to execute the verification protocol. The above search process can be repeatedly executed until the bad block is found. The results indicate that the overheads are reduced when the values of s are increased. Hence it is necessary to select the optimal number of sectors in each block to minimize the computation costs of clients and storage service providers.

4 Conclusion

Cooperative provable data possession concept has been achieved and hence integrity and availability is verified. The Zero-knowledge proof system is used and hence increases the security so it can be used widely in public cloud services thereby increasing their performance. Based on homomorphic verifiable responses and hash index hierarchy, we proposed a cooperative PDP scheme to support dynamic scalability on multiple storage servers. Finally our solution can be treated as a new candidate for data integrity verification in outsourcing data storage systems. In future we would like to improve the performance of the cooperative provable data possession scheme for larger files since many complex operations take place at the same time.

5. References

[1] YanZhu,Hongxin Hu,Gail-Joon Ahn,Senior Member,IEEE,Mengyang Yu "Cooperative Provable Data Possession for Integrity Verification in Multi-Cloud Storage" IEEE Transactions on parallel and distributed systems.10.1109/TPDS.2012.66,PP 1-13.

[2] G. Ateniese, R. C. Burns, R. Curtmola, J. Herring, L. Kissner, Z. N. J. Peterson, and D. X. Song. Provable data possession at untrusted stores. In ACM Conference on Computer and Communications Security, pages 598–609, 2007.

[3] S. Y. Ko, I. Hoque, B. Cho, and I. Gupta. On availability of intermediate data in cloud

ISSN: 2320-1363

computations. In Proc. 12th Usenix Workshop on Hot Topics in Operating Systems (HotOS XII),
2009.
[4] H. Shacham and B. Waters. Compact proofs of retrievability. In ASIACRYPT, pages 90–107, 2008.
[5] C. C. Erway, A. K¨upc¸ ¨u, C. Papamanthou, and R. Tamassia, "Dynamic provable data possession," in ACM Conference on Computer and Communications Security, E. Al-Shaer, S. Jha, and A. D. Keromytis, Eds. ACM, 2009, pp. 213–222.
[6] 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.
[7] Q. Wang, C.Wang, J. Li, K. Ren, and W. Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing," in ESORICS, ser. Lecture Notes in Computer
Science, M. Backes and P. Ning, Eds., vol. 5789. Springer, 2009, pp. 355–370.
[8] Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu, and S. S. Yau, "Dynamic audit services for integrity verification of outsourced storages in clouds," in SAC, W. C. Chu, W. E. Wong, M. J.
Palakal, and C.-C. Hung, Eds. ACM, 2011, pp. 1550–1557.
[9] K. D. Bowers, A. Juels, and A. Oprea, "Hail: a high-availability and integrity layer for cloud storage," in ACM Conference on Computer and Communications Security, E. Al-Shaer, S. Jha, and A. D. Keromytis, Eds. ACM, 2009, pp. 187–198.