International Refereed Journal of Engineering and Science (IRJES)
ISSN (Online) 2319-183X, (Print) 2319-1821
Volume 3, Issue 4(April 2014), PP.80-82

Provable data possession for integrity verification

Anchal Srivastava, Ashutosh sehgal, Vikas Kumar Singh, Nitish Kumar Bose
B.Tech (CSE), Institute Of Technology and Management, GIDA, Gorakhpur

Abstract:- this topic is based on the cloud computing. Cloud computing is a new and fast growing technology that offers an innovative and the Cloud storage is now an important development trend in information technology. The cloud storage server is stateless and independent from verifier, which is an important secure property in PDP schemes. Through security analysis and performance analysis, our scheme is provable secure and high efficiency.

Cooperative Provable data possession (CPDP) is a technique for ensuring the integrity of data in storage outsourcing [1]. 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 [6].(CPDP) using hash index hierarchy and holomorphic 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 efficiently and cost of computation for the client and cloud storage providers.

Keywords:- Cooperative Provable Data Possession (CPDP), Innovative, Holomorphic, Scalability.

I. INTRODUCTION

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics

1. On-demand self-service
2. Broad network access
3. Resource pooling
4. Rapid elasticity
5. Measured Service

Cloud storage service has become a faster profit growth point by providing a comparably low-cost, scalable, position-independent platform for clients' Data. Since cloud computing environment is constructed based on open architectures and interfaces, it has the capability to incorporate multiple internal and/or external cloud services together to provide high interoperability. We call such a distributed cloud environment as a multi-Cloud (or hybrid cloud). There exist various tools and technologies for multicloud, such as Platform VM Orchestrator, VMware vSphere, and Ovirt. These tools help cloud providers construct a distributed cloud storage platform (DCSP) for managing clients' data. However, if such an important platform is vulnerable to security attacks, it would bring irretrievable losses to the clients.

II. STRUCTURE AND TECHNIQUES

In which verification framework for multi-cloud storage and a formal definition of CPDP. We introduce two fundamental techniques for constructing our CPDP scheme:

1. ***Hash Index Hierarchy*** **(Hih):** on which the responses of the clients' challenges computed from multiple CSPs can be combined into a single response as the final result;

2. ***Homomorphism Verifiable Response*** **(Hvr):** which 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 verification protocol.

III. VERIFICATION FRAMEWORK FOR MULTI-CLOUD

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. In multi cloud architecture, a data storage service involves three different entities:

1. ***Clients:*** client have a large amount of data to be stored in multiple clouds and have the permissions to access and manipulate stored data
2. ***Cloud Service Providers*****:** who work together and have significant storages
3. ***Computation Resources:*** It manage client's data and providestorage service to them and Trusted Third Party (TTP) who is trusted to store verification parameters and offer public query services for these parameters. In this section we present a framework for multi cloud and formal definition of cooperative provable data possession (CPDP). Majority of existing CPDP schemes [1] are not capable to satisfy the inherent requirements to store and retrieve data from multiple clouds in terms of communication and computation costs. They offer publicly accessible remote interface to check integrity and manage tremendous amount of data. To address this problem, we consider a multi-cloud storage in Figure 1. Multi cloud storage is where multiple cloud service providers work together and provide storage services to clients. In multi cloud environment cloud service provider have significant storage and computation resources so as to provide storage and management for client data.

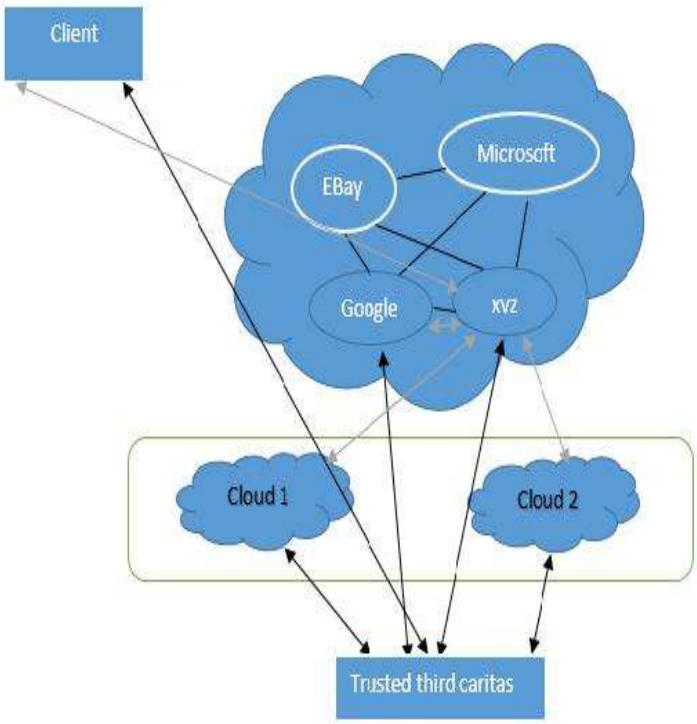

Figure I an illustration for multi-cloud working

IV. RELATED WORK

This paper mostly related to Multi Cloud Integrity using Provable data possession. These tools help cloud providers construct a distributed cloud storage platform (DCSP) for managing clients' data. However, if such an important platform is vulnerable to security attacks, it would bring irretrievable losses enterprise may be illegally accessed through a remote

To the clients. For example, the confidential data in an Interface provided by a multi-cloud, or relevant data and archives may be lost or tampered with when they are stored into an uncertain storage pool outside the enterprise. Therefore, it is indispensable for cloud service providers (CSPs) to provide security techniques for managing their storage services. Provable data possession (PDP) [2] is such a probabilistic proof technique for a storage provider to prove the integrity and ownership of clients' data without downloading data. The proof-checking without downloading makes it especially important for large-size files and folders (typically including many clients' files) 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. Vario us PDP schemes have been recently proposed, such as Scalable PDP [4] And Dynamic PDP [5]. However, these schemes mainly focus on PDP issues at un-trusted servers in a singlecloud storage provider and are not suitable for a multi-cloud environment

V. SECURITY ANALYSIS

This section will analyses the static PDP hybrid security agreement to confidentiality, integrity and confirms the analysis of three aspects.

A. Confidentiality: The principle of confidentiality specifies that only the sender and intended recipient(s) should be able to access the contents of a data. Confidentiality gets compromised if unauthorized person is able to contents of data.Before storing file on server owner (client) will use the *RSA* cryptosystem to encrypt the data to ensure that the file will not be intercepted by an unauthorized person to get the file content. Because encryption and decryption by *RSA* cryptosystem uses modular exponentiation, security is based on the factorization problem. Factorization problem is- given a composite number *N*, which consists of two large prime numbers *p* and *q* the product, if you want decomposition of *N*, the calculation is not feasible. Now, if the eavesdropper intercepts the cipher text files *M* there is no d.

B. Integrity: is lost if original data is modified. In the verification phase, the owner would like to check integrity of cipher text M which is stored as complete file on the server. Verification result calculated by owner is V. At thistime, the server will calculate the value of z to prove he has complete store cipher text file M. If verification value calculated by server z equal to owner verification value V, it means the server does have the correct storage cipher text file M.

VI. CONCLUTION

In this paper, we deal the construction of an efficient Provable data possession scheme for distributed cloud storage. With the techniques such as hash index hierarchy and homomorphism verifiable response, 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. 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.

REFERANCES

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

[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]. Shu Ni-Na, Zhang Hai-Yan "On providing integrity for dynamic data based on the third-party verifier in cloud computing" 978-0- 7695-4519-6/11 $26.00 © 2011 IEEE, DOI 10.1109/IMCCC.2011.135.

[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 TRANSACTIONS ON Parallel And Distributed Systems, VOL. 22, NO. 5, MAY 2011.

[6]. Shu Ni-Na, Zhang Hai-Yan "On providing integrity for dynamic data based on the third-party verifier in cloud computing" 978-0- 7695-4519-6/11 $26.00 © 2011 IEEE, DOI 10.1109/IMCCC.2011.135.