FRAMEWORK FOR SECURE DATA STORAGE ON CLOUD

Qamaruddin Shamsi[1], Mr.A.Isaacs[2]

[1]*Student of MSc, Department of Computer Science & IT, SHIATS, UP-Allahabad, India,* ***qamaruddinshamsi@yahoo.com***
[2]*Assistant Prof, Department of Computer Science & IT, SHIATS, UP-Allahabad, India,* ***ajendra.isaacs@shiats.edu.in***

Abstract

Secure Data Storage (SDS) is a technique for ensuring the integrity of data in storage outsourcing. In this paper, we address the construction of an efficient SDS scheme for distributed cloud storage to support the scalability of service and data migration, in which we consider the existence of multiple cloud service providers to cooperatively store and maintain the clients' data. We present a SDS scheme based on homomorphic verifiable response and hash index hierarchy. We prove the security of our scheme based on multi-prover zero-knowledge proof system, which can satisfy completeness, knowledge soundness, and zero-knowledge properties. In addition, we articulate performance optimization mechanisms for our scheme, and in particular present an efficient method for selecting optimal parameter values to minimize the computation costs of clients and storage service providers. Our experiments show that our solution introduces lower computation and communication overheads in comparison with non-cooperative approaches.

Key Words: *Cloud Security, Cloud Services Providers (CSP), Secure Data Storage, Trusted Third Parties (TTP).*

.

--- *** ---

1. INTRODUCTION

In recent years, 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). Often, by using virtual infrastructure management (VIM) , a multi-cloud allows clients to easily access his/her resources remotely through interfaces such as Web services provided by Amazon EC2. There exist various tools and technologies for multi-cloud, 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. For example, the confidential data in an enterprise may be illegally accessed through a remote 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. Secure Data Storage (SDS) (or proofs of Retrievability (POR)) 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. Various SDS schemes have been recently proposed, such as Scalable SDS and Dynamic SDS. However, these schemes mainly focus on SDS issues at untrusted servers in a single cloud storage provider and are not suitable for a multi-cloud environment.

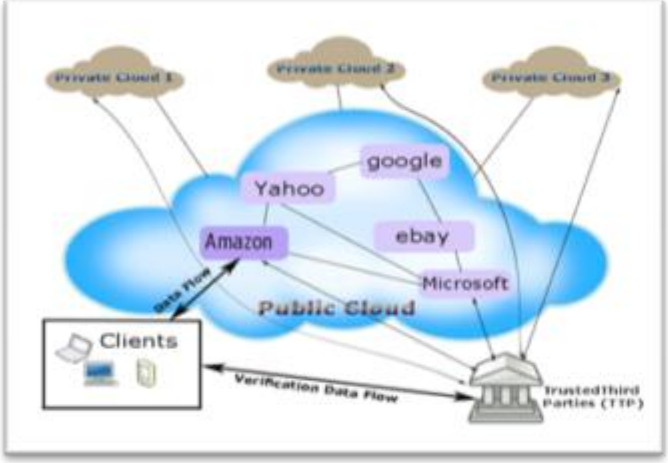

Fig-1: Users and service providers in cloud computing

2. COMPARISON WITH EARLIER SYSTEM

There exist various tools and technologies for multi-cloud, such as Platform VM Orchestrator, VMwarevSphere, and Ovirt. These tools help cloud providers construct a distributed cloud storage platform for an aging clients' data. However, if such an important platform is vulnerable to security attacks, it would bring irretrievable losses to the clients. For example, the confidential data in an enterprise may be illegally accessed through a remote 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 to provide security techniques for managing their storage services.To check the availability and integrity of outsourced data in cloud storages, researchers have proposed two basic approaches called Secure Data Storage and Proofs of Retrievability (POR). Atomies et al. first proposed the SDS model for ensuring possession of files on untrusted storages and provided an RSA-based scheme for a static case that achieves the communication cost. They also proposed a publicly verifiable version, which allows anyone, not just the owner, to challenge the server for data possession. They proposed a lightweight SDS scheme based on cryptographic hash function and symmetric key encryption, but the servers can deceive the owners by using previous metadata or responses due to the lack of randomness in the challenges. The numbers of updates and challenges are limited and fixed in advance and users cannot perform block insertions anywhere. We can use the traditionalauthentication method to authenticate user identification, but these are not enough. Because that some users (such as some students in the university) often use the tools to download large quantities electronic resources, which they have paid, or set up proxy server without permission for seeking illegal gains. In this case, the user's identity is trusted. However, the user behavior is not trusted. We often see some users are warned and even the account is closed because of misconduct. Therefore, in cloud computing environment, only to solve the user's identity trust is not enough, user's behavior trust must be combined to the identity trust to solve the problem of how to CSP trust user.

3. OBJECTIVE

With regards to this dissertation topic “Secure Data Storage on Cloud” It was undertaken with the following objectives.
1. To build Multi-Cloud System that provides services to user.
2. To divide uploaded file into 3 blocks.
3. To transfer each block to one server, and encrypt them.
4. To decrypt file, update file and download it from system.

4.STUDY OF THE SYSTEM

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. SDS Based on zero knowledge proof system and interactive proof system we prove the integrity of data stored in a multi cloud. A CSDS 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.

In this dissertation I have proposed a Secure Data Storage model for the storing of the user’s in multi-cloud environment. In the flexibility of the uses the interface has been developed a graphics concept in mind, associated through a browser interface the operational or generic user interface helps the users upon the system in transactions through the existing data and required services. The operational user interface also helps the ordinary users in managing their own information helps the ordinary users in managing their own information in a customized manner as per the assisted flexibilities. The system after careful analysis has been identified to be presented with the following modules.
The modules involved are:
✓ Login Panel
✓ Registration
✓ Cloud Service Provider
✓ User
✓ Third Party Auditor (TPA)

• Login Panel:-
It acts as a Gateway Interface which will give the credentials will allow or disallow the user.
• Registration:-
Any end user is allowed to register with the system .User can simply fill the specified form which after validation allows the user to register with the Cloud system because he got a unique user ID.
• Cloud Service Provider:
Cloud service providers (CSP) use the resources provided by resources layer and their technology (such as Virtualization Technology) to integrate the cloud services, and through the information transport layer to provide these services to users.
User: Access the Services provided by Providers.
Third Party Auditor (TPA):
Third Party Auditor depending on the principles and services are deactivated if terms and conditions are violated.

5.WORKFLOW APPLICATIONS

Many software systems exist to support workflows in particular domains. Such systems manage tasks such as automatic routing, partially automated processing and integration between different functional software applications and hardware systems that contribute to the value-addition process underlying the workflow.

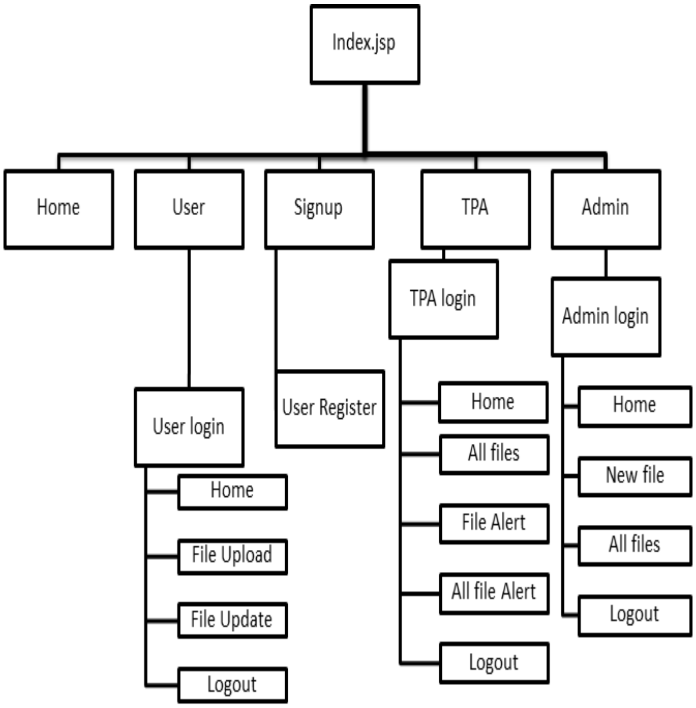

Fig-2: System Workflow

As shown in Figure 2,in the index page any end user is allowed to register with the system. User can simply fill the specified form which after validation allows the user to register with the cloud because the user has unique user id and all information will be stored in database. After registration a user can Login, it acts as a gateway Interface which will give the credentials. It will allow or disallow the user. After that user can use cloud's services such as uploading file to Multi-cloud, the file become automatic encrypt in separate in 3 blocks then trusted third parties(TPA) has ability to get file key and decrypt it and give allowance to every separate block to a cloud server. After TPA allows every cloud Server receives a part of file and is able to give allow or disallow to cloud server it can view this part of file but is not able to make changes in this part of file for cloud server it is not updateable. After allowance of cloud server the user can view all parts of file and can update and download. For cloud's safety level of security no one cloud server can makes updating in the file if cloud server try to update the TPA will receive an Alerts that TPA can easily know how want to update or delete users file, and by uploading file become encrypt and its will not readable just user and TPA are able to decrypt this file.

6. CONCLUSION

We presented the construction of an efficient SDS scheme for distributed cloud storage. Based on homomorphic verifiable response and hash index hierarchy, we have proposed a SDS scheme to support dynamic scalability on multiple storage servers. We also showed that our scheme provided all security properties required by zero knowledge interactive proof system, so that it can resist various attacks even if it is deployed as a public audit service in clouds. Furthermore, we optimized the probabilistic query and periodic verification to improve the audit performance. Our experiments clearly demonstrated that our approaches only introduce a small amount of computation and communication overheads. Therefore, our solution can be treated as a new candidate for data integrity verification in outsourcing data storage systems. As part of future work, we would extend our work toexplore more effective SDS constructions. Finally, it is still a challenging problem for the generation of tags with the length irrelevant to the size of data blocks. We would explore such a issue to provide the support of variable-length block verification.

ACKNOWLEDGEMENT

This paper is the end of my journey in obtaining my Master degree. I have not travelled in a vacuum in this journey. This paper has been kept on track and been seen through to completion with the support and encouragement of numerous people including my well-wishers, my friends and adviser. At the end I would like to thank all those people who made it possible and an unforgettable experience for me. At the end of my paper, it is a pleasant task to express my thanks to all those who contributed in many ways to the success of this study and made it an unforgettable experience for me.

REFERENCES

.
[1]. US Federal Could Computing Market Forecast 2010 2015,tabular analysis, publication: Available:http://www.marketreseachmedia.com 2009.5

[2]. David Hilley (2009, April).Cloud Computing: A Taxonomy ofPlat formand Infrastructure-level Offerings, College ofComputing Georgia Institute of Technology. [Online]. Available:https://smartech.gatech.edu/handle/1853/34402

[3]. FarzadSabahi (October 2012.)Secure Virtualization Technology.International Journal of Computer Theory and Engineering, Vol.4, No. 5[Online]. Available: http://www.ijcte.org/

[4]. Chandrashekhar S. Pawar and R.B.Wagh (2012, April)., Areview of resource allocation policies.World Journal of Scienceand Technology [Online]. Available:www.worldjournalofscience.com

[5]. V.Vinothina, Dr. R. Sridaran and Dr.PadmavathiGanapathi(2012). A Survey on Resource Allocation Strategies in Cloudcomputing. International Journal of advanced Computer Scienceand Applications, Vol. 3 [Online]. Available: www.ijert.org.

BIOGRAPHIES

QAMARUDDIN SHAMSI
Master in computer science from
SHIATS – Allahabad – India
Email: qamaruddinshamsi@yahoo.com
Mobile: 0093 705 40 33 40
From: Afghanistan

MR. AJENDARA ISAACS
Assistant Prof. Department of
Computer Science & IT,
SHIATS – Allahabad – India
Email: ajendra.isaacs@shiats.edu.in
From: India