Research Paper

Volume : 3 | Issue : 4 | April 2014 • ISSN No 2277 - 8179

Towards Secured and Trusted Multi Cloud Storage with Backup Link

Engineering

KEYWORDS : Cloud computing, security, storage, cost-effective, cloud service provider, customer.

Ashwini Agade	Information Technology, Bharati Vidyapeeth's College of Engineering for women, Pune, India
Arohi Kumari	Information Technology, Bharati Vidyapeeth's College of Engineering for women, Pune, India
Anupriya Kadlag	Information Technology, Bharati Vidyapeeth's College of Engineering for women, Pune, India
Sushama Hadule	Information Technology, Bharati Vidyapeeth's College of Engineering for women, Pune, India.

ABSTRACT

The end of this decade is marked by a paradigm shift of the industrial information technology towards a pay-per-use service business model known as cloud computing. Cloud Computing is a new environment in computer oriented services. It is a model for enabling 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 system have some similarities of distributed system, according to this similarities cloud computing also uses the features of networking. Cloud data storage redefines the security issues targeted on customer's outsourced data (data that is not stored/retrieved from the costumers own servers). In this work we observed that, from a customer's point of view, relying upon a solo Server for his outsourced data is not very promising. In addition, providing better privacy as well as ensuring data availability can be achieved by dividing the user's data block into data pieces and distributing them among the available Servers in such a way that no less than a threshold number of Servers can take part in successful retrieval of the whole data block. If one of the Servers get crashed or is down the data is retrieved from the backup link. In this paper, we propose a secured and trusted multi-cloud storage (STMCS) model in cloud computing which holds an economical distribution of data among the available Servers, to provide customers with data availability as well as secure storage.

1 Introduction

Cloud computing is the new paradigm which offers flexible services to world wide users.Its a pay per use service business model.The cloud is a term for a group of servers offering a service. So if you are storing your data in the cloud, it means you have signed up for a service that allows you to remotely store and retrieve your data.Privacy preservation and data integrity are two of the most critical security issues related to user data [4].The basic idea in the cloud computing is to move computing tasks from individual systems into the cloud, which provides hardware and software resources over the Internet.A main advantage of cloud computing is that the customers can avoid capital expenditure on hardware, software, and services but pay for only what they use to a cloud provider. The major issue in cloud computing is security of data, from any unauthorized person who is going to use it for any wrong purpose.To address such issues,we proposed an economical distribution of data among the available servers, to provide customers with data availability as well as secure storage. In this model, CSP (Cloud Service Provider) divides this data among several servers available, based on available space. As we are dividing data into multiple chunks and storing it on different servers, which have different physical locations, so no one can get the meaningful data unless the authenticated one. As we are storing data with their backups, we can retrieve data from backup server if the actual server is down from any network issue.

2 Existing Technology

In conventional simulation models, the organizations had the physical possession of their data and hence have an ease of implementing better data security policies.But in case of cloud computing, the data is stored on an autonomous business party that provides data storage as a subscription service.The users have to trust the CSP with security of their data.Many of the cryptographic approaches have been proposed for hiding the data from the storage provider and hence preserving data privacy [8],[5].These approaches concentrate on one single cloud service provider that can easily become a bottleneck for such services.In [6], the authors studied and proved that sole cryptographic measures are insufficient for ensuring data privacy in cloud computing.

One bigger concern that arises in such schemes of cloud storage services is that, there is no full-proof way to be certain that the service provider does not retain the user data, even after the user opts out of the subscription.With enormous amount of time, such data can be decrypted and meaningful information can be retrieved and user privacy can easily be breached.Since, the user might not be availing the storage services from that servers, he will have no clue of such a passive attack.The better the cryptographic scheme, the more complex will be it's implementation and hence the service provider will ask for higher cost.To provide users with better and fair chances to avail efficient security services for their cloud storage at affordable costs,Therefore, the conventional single service provider based cryptographic techniques does not seem too much promising. In [6], the authors discussed distributing the data over multiple clouds or networks in such a way that if an adversary is able to intrude in one network, still he can not retrieve any meaningful data, because complementary pieces are stored in the other network.Our approach is similar to this approach, because both aim to remove the centralized distribution of cloud data.This is why in our model;we propose to use a redundant distribution scheme, such as in [7], in which at least a threshold number of pieces of the data are required out of the entire distribution range,for successful retrieval.

To enhance Data Privacy and Integrity in the Cloud the concept of "Blind processing" has been used. Utilizing blind communication and execution services, a user exchanges his/her sensitive information with a cloud system via isolated processes whose execution environment and data is shielded from the rest of the system after ensuring the system has correct hardware, trusted computing base, correct credentials, and trustworthy state.In blind processing we have to implement multiple abstraction process. A main drawback of this concept is the use of more number of parameters which increases the complexity.

These are the some existing technologies (as discussed above) which had been developed yet.By analyzing above technologies it is noticed that still there are many drawbacks present in the system.So it is needed to think about some innovative ideas which will be more appreciated by the users.To overcome all

these drawbacks and make the system more efficient and user friendly we move towards the concept of "Towards Secured and Trusted multi-cloud storage with backup link".

3 System Overview

From a customer's point of view, relying upon a solo server for his outsourced data is not very promising.The cloud storage service is generally priced on two factors, how much data is to be stored on the cloud servers and for how long the data is to be stored.In our model,we assume that all the data is to be stored for same period of time.

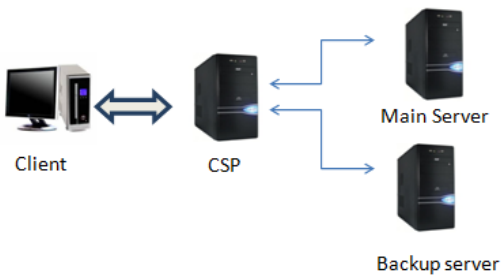

Fig.1. System Architecture

We consider p number of servers; each available server is associated with a QoS factor, along with its cost of providing storage service per unit of stored data (D).Every server has a different level of quality of service (QoS) offered as well as a different amount of storage space associated with it.Hence, the cloud user can store his data on more than one server according to the required level of security and storage space.

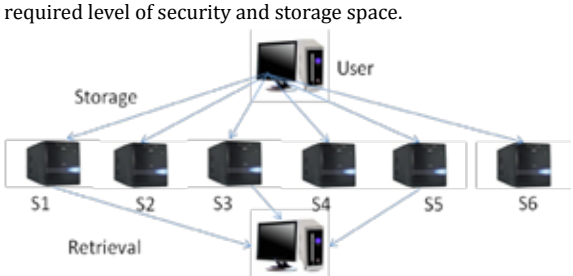

Fig.2. Data Storage and Retrieval

Therefore cost effective and better privacy as well as ensuring data availability can be achieved by dividing the user's data into data pieces and distributing them among the available servers in such a way that no less than a threshold number of servers can take part in successful retrieval of the whole data block.To encrypt the data we are using Triple DES algorithm that is helpful in enhancing the security of whole system.

A. Problem Statement

Given p number of servers (Si : i ∈ 1, 2, .., p). Each server is associated with a QoS factor (QSi ∈ (0, 1)) along with the cost of storing data units (Ci). Our Secured and Trusted Multi-Cloud Storage Model (STMCS) seeks a distribution of customer's data pieces among the available servers in such a way that, at least q number of servers must take part in data retrieval, while minimizing the total cost of storing the data on servers as well as maximizing the quality of service provided by the servers.

4 Numerical Results

In this section, to illustrate the performance of our secured and trusted model in providing secure storage scheme as well as availability of data for users we provide our results in two different scenarios.

Our proposed secured and trusted model has to choose the optimal storage allocation based upon the storage of each server, while maximizing the overall quality of service offered.

In our first scenario, we set that the total number of available servers to 6. Each server is associated with quality of service factor. We set the threshold value k = q = 3, which specifies that, at least 3 data pieces are needed to retrieve the whole data block. We assume that, there is no upper bound on the budget of the customer.

Such a model can be used to provide a lower bound for preplaning estimate for cloud data storage for a customer.User's data block was divided into 3 data pieces,to retrieve the whole data block with maintaining a maximized QoS from different servers, our model will retrieve the 3 data pieces that are required to reconstruct the whole data block from all servers.In our second scenario,we provide an initial budget for the user, which plays a role as an upperbound to the expenditure of storage and retrieving from Servers.Our proposed model will try to maximize the quality of service it can achieve within the available budget.

5 Conclusion

In this project,we proposed secured and Trusted multi cloud storage (STMCS) with backup link in cloud computing,which seeks to provide each customer with a better cloud data storage deci-sion,taking into consideration the user budget as well as providing him with the best quality of service(security and availability of data)offered by available cloud service providers,by dividing and distributing customers data on different Servers,our proposed model has shown its ability by providing a customer with a secured and trusted storage under his affordable budget.

REFERENCE

[1] Amazon.com, "Amazon s3 availablity event: July 20, 2008", Online at http://status.aws.amazon.com/s3-20080720.html, 2008. | [2] "A Mordern Language for Mathematical Programming", Online at | http://www.ampl.com. | [3] M. Arrington, "Gmail Disaster: Reports of mass email deletions", On line at http://www.techcrunch.com/2006/12/28/gmail-disasterreports-ofmass-email-deletions/, December 2006. | [4] P. S. Browne, "Data privacy and integrity: an overview", In Proceeding of SIGFIDET '71 Proceedings of the ACM SIGFIDET (now SIGMOD), 1971. | [5] A. Cavoukian, "Privacy in clouds", Identity in the Information Society, Dec 2008. | [6] J. Du, W. Wei, X. Gu, T. Yu, "RunTest: assuring integrity of dataflow processing in cloud computing infrastructures", In Proceedings of the 5th | ACM Symposium on Information, Computer and Communications Security (ASIACCS '10), ACM, New York, NY, USA, 293-304. | [7] R. Gellman, "Privacy in the clouds: Risks to privacy and confidentiality from cloud computing", Prepared for the World Privacy Forum, online at http://www.worldprivacyforum.org/pdf/WPF Cloud Privacy Report.pdf, | Feb 2009. | [8] The Official Google Blog, "A new approach to China: an update", online at http://googleblog.blogspot.com/2010/03/new-approach-to-chinaupdate.html, March 2010. | [9] N. Gruschka, M. Jensen, "Attack surfaces: A taxonomy for attacks on cloud services", Cloud Computing (CLOUD), 2010 IEEE 3rd International | Conference on, 5-10 July 2010. | [10] W. Itani, A. Kayssi, A. Chehab, "Privacy as a Service: Privacy-Aware Data Storage and Processing in Cloud Computing Architectures," Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, Dec 2009. |