International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 1, Issue 4, April 2014)

Secured Cost Effective Multi-Cloud Storage

Shilpa Biradar
GNDEC Bidar
E-mail :biradar.shilpa8@gmail.com

Prof. S.M.Joshi
GNDEC Bidar
E-mail:shrinivasjoshi999@gmail.com

Prof. Giriraj Patil
GNDEC Bidar
E-mail:giriraj.mpatil@gmail.com

Abstract:The end of this decade is marked by a paradigm shift of the industrial information technology towards a subscription based or pay per use service business model known as cloud computing. The concept of cloud computing is a very vast concept which is very effective and efficient security services. 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, it observed that, from a customer's point of view, relying upon a solo SP 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 SPs in such a way that no less than a threshold number of SPs can take part in successful retrieval of the whole data block. This paper, proposes a secured cost-effective multi-cloud storage (SCMCS) model in cloud computing which holds an economical distribution of data among the available SPs in the market, to provide customers with data availability as well as secure storage.

1. INTRODUCTION

Cloud computing is simply a rate server. A huge amount of data being retrieved from geographically distributed data sources, and non localized data-handling requirements, creates such a change in technological as well as business model. One of the prominent services offered in cloud computing is the cloud data storage, in which, subscribers do not have to store their data on their own servers[1], where instead their data will be stored on the cloud service provider's servers. In cloud computing, subscribers have to pay the service providers for this storage service. This service does not only provides flexibility and scalability for the data storage, it also provide customers with the benefit of paying only for the amount of data they need to store for a particular period of time, without any concerns for efficient pay the service providers for this storage service. This service does not only provides flexibility and scalability for the data storage, it also provide customers with the benefit of paying only for the amount of data they need to store for a particular period of time, without any concerns for efficient pay the service providers for this storage service. This service does not only provides flexibility and scalability for the data storage, it also provide customers with the benefit of paying only for the amount of data they need to store for a particular period of time, without any concerns for efficient storage mechanisms and maintainability issues with large amounts of data storage. In addition to these benefits, customers can easily access their data from any geographical region where the Cloud Service Provider's network or Internet can be accessed. An example of the cloud computing is shown in Fig. 1Since cloud service providers (SP) are separate market entities, data integrity and privacy are the most critical issues that need to be addressed in cloud computing. Even though the cloud service providers have standard regulations and powerful infrastructure to ensure customer's data privacy and provide a better availability, the reports of privacy breach and service outage have been apparent in last few years [4] [3] [6] and [5]. Also the political influence might become an issue with the availability of services [7]. In this work we observed that, from a customer's point of view, relying upon a solo SP for his out sourced data is not very promising. In addition, providing better privacy as well as ensure data availability, can be achieved by dividing the user's data block into data pieces and distributing them among the available SPs in such a way that no less than a threshold number of SPs can take part in successful retrieval of the whole data block.

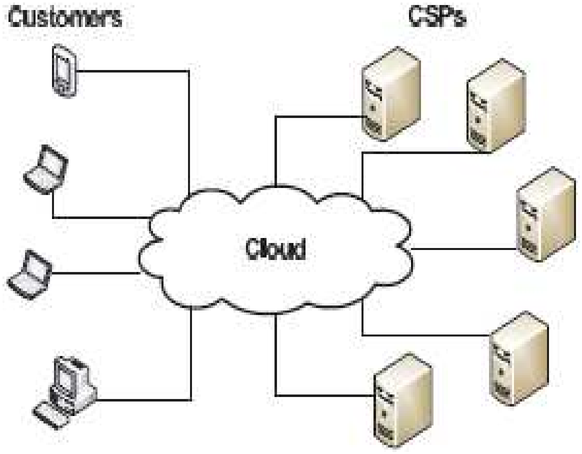

Fig1. Cloud computing architecture example

This proposed approach will provide the cloud computing users a decision model, that provides a better security by distributing the data over multiple cloud service providers in such a way that, none of the SP can successfully retrieve meaningful information from the data pieces allocated at their servers. Also, in addition, this provides the user with better assurance of availability of data, by maintaining redundancy in data distribution. In this case, if a service provider suffers service outage [4] [6] or goes bankrupt, the user still can access his data by retrieving it from other service providers.

2. WORKING OF CLOUD COMPUTING

As this paper have discussed about the basic about the cloud computing in section I, I can say that the cloud computing is a paradigm shift from the distribute computing where an organization uses the resources as services. This is a sort of "utility computing" where you pay-as-you-go like electricity bill. Cloud providers are the companies which manage large datacenters and can expertly manage this datacenters. Cloud users may be a single user or an entire organization which uses services from providers. Cloud users need not to deploy the computing resources at their site. These resources are available at the cloud providers on utility basis and charged on uses basis. This paper is taking an example of one cloud service provider that creates the world's largest cloud based infrastructure to understand the working of cloud computing mechanism, that is: **Google.**

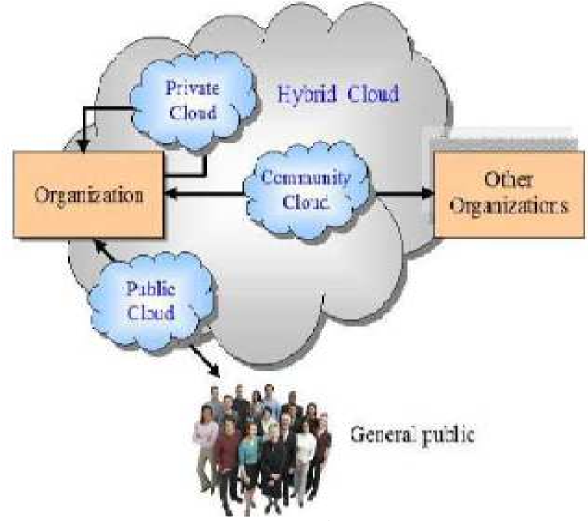

Fig2. General scenario of traditional cloud provider

Google provides the Google Apps Engine that lets you run web applications on Google's infrastructure. App Engine applications are easy to build, maintain, and scale as your traffic and data storage needs grow. Users just have to create an account in Google and that is the use of Public cloud of Google. User creates his/her own account and mange it, so user establishes his private cloud environment where he can use different services Provided by Google. Public cloud is used by the user in his private cloud that creates the Hybrid cloud. Google Apps now allows free hosting of your e-mail server (with your own domain name), up to 7.3 GB of storage per free user account **(IaaS)**, and free Google Talk, Google Calendar, Google Docs (for creating and sharing documents, spreadsheets and presentations, collaboration in real-time right inside a Web browser window), Google Sites (for easily creating and sharing a group Web site) and Start Page (**SaaS**), and so forth. Google cloud services can be run in any system from anywhere without any consideration of which platform system provide, which OS provide with internet connection. This thing provides the **PaaS** concept of cloud by Google to its user.

3. SINGLE CLOUD SERVICE PROVIDER

Privacy preservation and data integrity are two of the most critical security issues related to user data. In conventional paradigm, 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[8]. The users have to trust the cloud service provider (SP) with security of their data. In, the author discussed the criticality of the privacy issues in cloud computing, and pointed out that obtaining information from a third party is much easier than from the creator himself. Following the pattern of paradigm shift, the security policies also evolved from the conventional cryptographic schemes applied in centralized and distributed data storage, for enabling the data privacy.

3.1. Disadvantages:

- This service does not only provide flexibility and Scalability for the data storage.
- Data losses accrued.
- Do not use cryptography technology so less security
- Need High cost for cloud maintains process.

4. MODELS

This section, will describe this system model and the threat model. This two model goes to explain benefits of cloud storage two multi cloud storage techniques.

A. System Overview

These consider the storage services for cloud data storage between two entities, cloud users (U) and cloud service providers (SP). 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 this model, we assume that number of cloud service provider for data is to be stored and retrieved, because security is much more higher than cloud service provider.

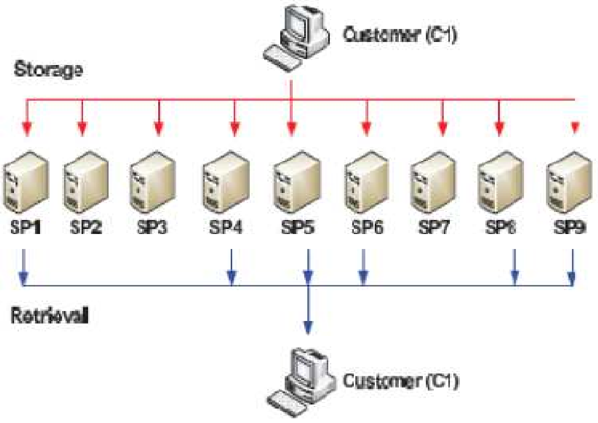

Fig3. Data Storage and Retrieval

B. Threat Model

Customers' stored data at cloud service providers is vulnerable to various threats. Previous studies in [9], [11] discussed in detail that a cloud service provider can be a victim to Denial of service attacks or its variants. In this work, we consider two types of threat models. First is the *single point of failure* [9], [11], which will affect the data availability, that could occur if a server at the cloud service provider failed or crashed, which make it hard for the customer to retrieve his stored data from the server. *Availability of data is also an important issue which could be affected, if the cloud service provider (SP) runs out of business*. Such worries are no more hypothetical issues, therefore, a cloud service customer can not entirely rely upon a solo cloud service provider to ensure the storage of his vital data.

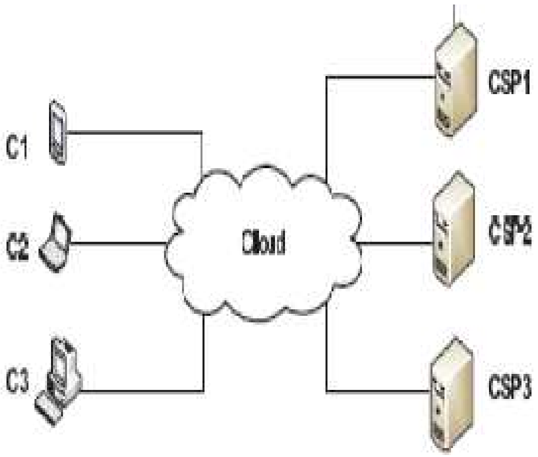

Fig4. CSP failure

To illustrate this threat we use an example in Fig 4. Let us assume that three customers (C1, C2 and C3) stored their three different data service providers (CSP1, CSP2 and CSP3) respectively. Each customer can retrieve his own data from the cloud service provider who it has a contract with. If a failure occur at CSP1,due to internal problem with server or some issues with the cloud service provider, all C1's data which was stored on CSP1's servers will be lost and cannot be retrieved.

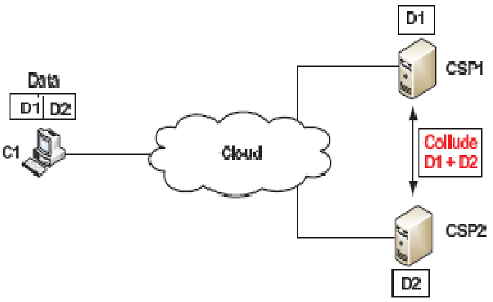

Fig5. Colluding cloud service providers

This illustrates the colluding service providers' threat in Fig 5. Let us assume that two cloud service providers are available for customer (C1), who wants to store his own data securely [8]. In here he will divide his data into two parts (D1 and D2) and distribute these parts on the two available CSPs (CSP1 and CSP2) respectively. The two cloud service providers might collude with each other, and exchange the part of data that the customer has stored on their server and reconstruct the whole data without being detected by the user. 5. SECURED COST EFFECTIVE MULTI CLOUD STORAGE

This propose an economical distribution of data among the available SP s in the market, to provide customer with data availability as well as secure storage. In this model customer divides his data among several SPs available in the market, based on his available budget. Also we provide a decision for the customer, to which SPs he must chose to access data, with respect to data access quality of service offered by the SPs at the location of data retrieval. This not only rules out the possibility of a SP misusing the customer's data, breaching the privacy of data, but can easily ensure the data availability with a better quality of service.

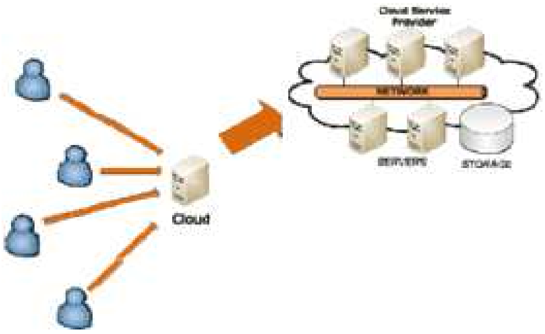

Fig6. Multi-cloud storage in cloud computing.

This approach will provide the cloud computing users a decision model, that provides a better security by distributing the data over multiple cloud service provider in such a way that, none of the SP can successfully retrieve meaningful information from the data pieces allocated at their servers[7]. Also, in addition, we provide the user with better assurance of availability of data, by maintaining redundancy in data distribution. In this case, if a service provider suffers service outage or goes bankrupt, the user still can access his data by retrieving it from other service providers.

5.1. Advantages:

-> With out any concerns for efficient storage
mechanisms and maintainability issues with
large amounts of data storage.
-> Cloud data storage also redefines the
security issues targeted on customer's
outsourced data.
-> Using cryptography technology for data base
security
-> Less cost and cost based on client requirements..
-> Easy to maintains large databases with Security

6. CONCLUSION

This paper proposed a secured cost-effective multi-cloud storage (SCMCS) in cloud computing, which seeks to provide each customer with a better cloud data storage decision, 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. This work gives a preliminary idea about compare to single cloud storage, security and availability of data

is much more efficient in multi-cloud computing. So finally in secured cost-effective multi-cloud storage provide high security compare to other cloud storage.

REFERENCES

[1] P. Mell, T. Grance, "Draft NIST working definition of cloud computing", Referenced on June.3rd,2009,Online,at http://csrc.nist.gov/groups/SNS/cloud-computing/index.html,2009.

[2] Arvind D Meniya, Harkishan B Jethva " Single-Sign-On (SSO) across open cloud computing federation", Vol. 2, Issue 1,Jan-Feb 2012

[3] M. Arrington, "Gmail Disaster: Reports of mass Email deletions", Online at www.techcrunch.com/2006/12/28/gmail-

[4] Amazon.com, "Amazon s3 availability event: July 20, 2008", Online at http://status.aws.amazon.com/s3-20080720.html, 2008.

[5] B. Krebs, "Payment Processor Breach May Be Largest Ever", Online at http://voices.washingtonpost.com/ securityfix/2009/01/payment processor breach may b.html, Jan, 2009.

[6] J. Kincaid, "MediaMax/TheLinkup Closes Its Doors", Online at http://www.techcrunch.com/2008/ 7/10/mediamaxthelinkup-closes-itsdorrs/,July 08.

[7] The Official Google Blog, "A new approach to China: an update", online at http://googleblog.blogspot.com/2010/03/new-approach-tochinaupdate. html, March 2010.

[8] Peter Mell, and Tim Grance, "Draft NIST Working Definition of Cloud Computing," 2009, From http://csrc.nist.gov/ groups/SNS/cloud-Computing

[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] M. Jensen, J. Schwenk, N. Gruschka, L.L. Iacono, "On Technical Security Issues in Cloud Computing", IEEE International Conference on Cloud Computing, (CLOUD II 2009), Bangalore.