ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 2, Issue 4, April 2013

A survey on cost effective multi-cloud storage in cloud computing

Nitesh Shrivastava, Ganesh Kumar

***Abstract*— As novel storage model, cloud storage has gain attentions from both the academics and industrial communities. However along with variant advantages, it also brings new challenges in maintaining data integrity and highly available reliable data storage facility. The integrity of the data stored in the service provider is one of challenges to be addressed before the cloud storage is applied widely. Cost is also a major issue in cloud computing when we are switching to multi cloud. To address all the scenario we present a survey paper.**

This survey paper is based on the recent research related to single and multi cloud cost , security and availability based scenario. This work aim to promote the use of multi cloud environment over single cloud to reduce the risk.

Index Terms*— cloud computing, data integrity, data intrusion, service availability, cloud service provider.*

I. INTRODUCTION

Cloud computing is an internet based model for enabling convenient on demand network access to shared recourses [1]. It provides various services over internet such as software hardware, data storage, infrastructure. Cloud computing providers delivers application via internet, which are access from desktop and mobile apps.Cloud computing technology grouped into three section: they are SaaS, PaaS, laaS[2] as shown in fig.1. . SaaS(software as a service) it's an on demand application service. It eliminates the need of installing and running application on customers own computers.PaaS (platform as a service)it's an on demand platform service to host costumer application. It is a delivery of computer platform and solution as a service.IaaS (infrastructure as a service) in this user can benefit from networking infrastructure services,datastorage and computing services. Rather than purchasing server , software, data centre space client can buy those resources as a fully outsourced service.

To accessed these cloud services security and reliability we are using different models like: i) Using single service provider. ii) Using multiple service providers. The weakness of single service provider is that it can be easily be hacked by intruders and if the service provider fails or down for some technical reasons than client will not at all access his/her data. The problem in Multiple service provider models is to compromise the security because there is lack of security technique used here but availability is up to the mark

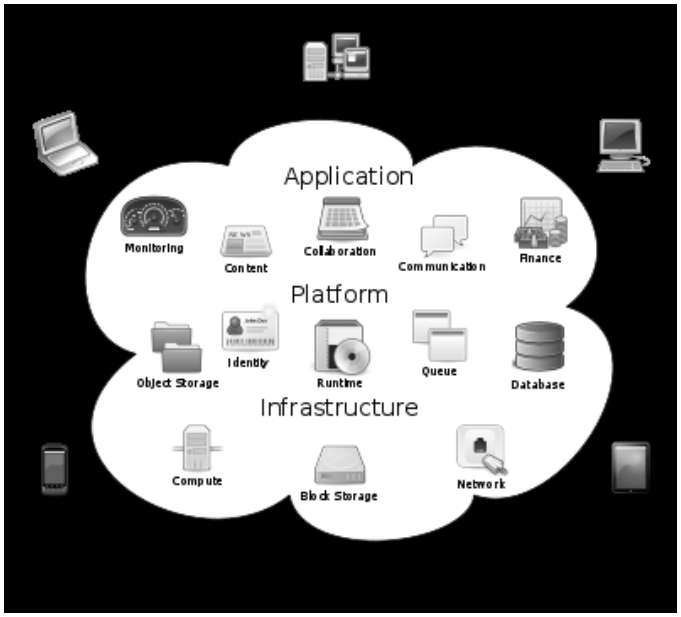

Fig.1 Overview of Cloud computing

The reminder of paper is organized as follows. Section 2 discuss about issues in cloud computing. Section 3 new security analysis in cloud computing. Section 4 discuss the comparison of security issues and Section 5 will conclude the paper.

II. ISSUES IN CLOUD COMPUTING

Before considering the cloud computing technology. It is important to understand the risks involved. You should carry out the risk assessment process before any control is handed over the to a service provider.

A. Data storage and security

Many cloud service provider provide storage as a service. They take the data from the user and stored on the large data centers, hence providing a user means of storage. Although these service provider says that data stored in a cloud is safe but there have been some cases where data is been modified or lost due to security holes. Various cloud provider adopt various technology to resolve the problem of cloud data storage. The virtualized nature of cloud make the traditional mechanism unstable for handling the security risks so these service provider use different encrypting technique to overcome these problems.

Another major issue that is mostly neglected is of data remanences.It refers to the data left out during tranfer.It cause minimal security threat in private cloud computing offerings,

however server security issues may emerge in case of public cloud offerings as a result of data remanence.

Virtualization increases the security of cloud enviroment.With virtualization a single machine can be divided into multiple virtual machine, thus provide better data isolation. The vms provide the security test bed for executing of untested code from entrusted user. An hierarchical reputation system have been proposed in a paper [9] for managing trust I n the cloud environment.

B. Application level security

Application level security refers to the usage of software and hardware resources to provide the security to application such as attackers are not make any changes in the application formate.Now a days attacker launched them as a trusted user and system consider them as trusted user and allow full access to attacking party. The reason behind this is using outdated network policies. With the technological advancement these security policies become obsolete as there have been instances when system security have been breached, but with the recent technology advancements it is quit possible to imitate a trusted user. The threat to application level security include sql injection attack ,dos attack ,captcha breaking , xss attack.

Hence, it is necessary to install high level security check to minimise these risks.Thes traditional method to deal with increased security issue have been to develop a task oriented asic device which can handle the specific task and provide high level of security[10].But with application level threat being dyanamic and adaptable to the security check in place, these closed system have to observed to be slow in compare to the open ended system.

C. Data intrusion

Another security risk that occurs in cloud computing enviroment, such as the google doc cloud service is a hacked password or data intrusion. If someone gain access to google doc password then they will able to gain all account instance and resources .The stolen password allow the hacker to modify ,erase the full data and even disable the services. Furthermore there is a possibility of hacking email [11] (google doc user name) to be hacked and since google allow the lost password to be reset by email, the hacker may still able to access the account after receiving the new password.

D. Single to multicloud

The use of cloud computing have increase in many organization. The cloud computing provide a many benefit in terms of cost and avalability.The pay per use model know as cloud computing. One of the prominent service offer by cloud computing is cloud data storage, in which subscriber don't want to store their data on their own server, instead of that there data stored in cloud service provider. This service don't provide only flexibility and scalability for data storage but it also provide the customer with the benefit of only for the amount of data they need to store for the particular period of time. In addition to these benefits customer can access their data from anywhere as long as they are connected to internet. Since the cloud service provider is the different market entities, data integrity and privacy are the most common issues that need to be address in cloud computing. Even thought the cloud service provider have standard regulation and power infrastructure to ensure the customer data privacy and provide a better availability. The political influence might become an issue with the availability of the service.

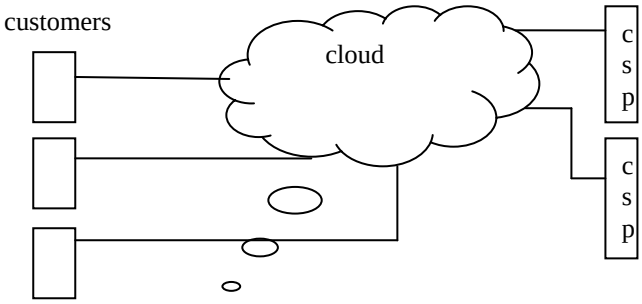

Fig. 2. Cloud computing architecture

In this work we observe that relaying on single service provider for his out sourcing data is not very promising. The availability of the data is not up to the mark. if suppose the cloud service provider goes down due to any technical reason, then no one will access the data from any where this means high availability violated as shown in fig 2.To address this issue we are switching from single service provider to multiple service provider where we can store the customer data into multiple service provider so that if any service provider get down even then user can access their data as shown in fig 3.

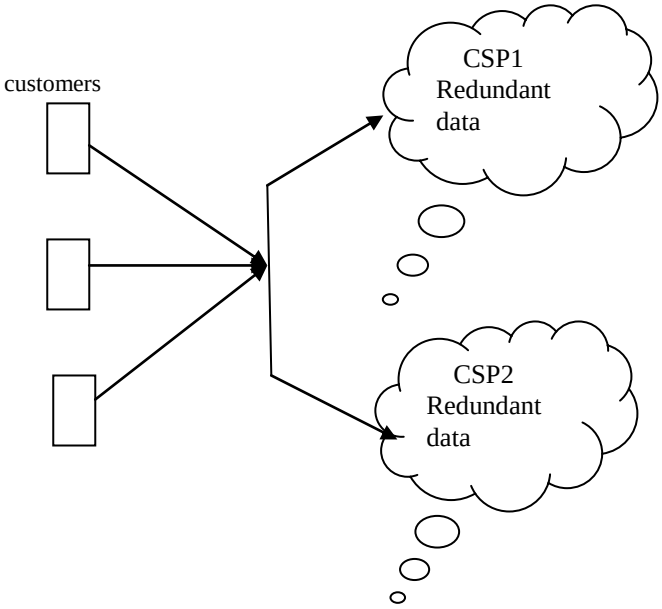

Fig. 3 Multi. cloud computing architecture

E. Data integrity

In cloud computing, data move to remotely cloud server [12].cloud remotely store the data and get back to owner whenever it needed. But there is no guarantee that the data stored is not alter by cloud or third party auditor(TPA).In order to overcome the threat of data integrity , the user must be able to use the assist of TPA.The TPA have experience about checking the integrity of a data, that cloud user do not have, and that is difficult for the owner to check.

Data integrity is one of the important issues in cloud computing. Because data integrity ensure that data is of high quality, correct, consistent and accessiable.After moving the data to cloud, user thought that there data are secured. The hope may be fail some times, the user data may be alter or deleted.

In this scenario it is important to verify the tempered or deleted data

F. Cost

Cost is also the one of the major issue in a cloud computing. As the size of data increase the cost of data also increases, this means cost is directly proportion to size of data. But there is different cost in term of single cloud and multi cloud. Because data stored in the multi cloud is to achieve high avalability,so redundant data are store in multiple service provider then the cost will be calculated by adding the cost of all service provider that contain the redundant data that will be the total cost[2]. There is one more factor by which cost will be increase, i.e. algorithm, as the algorithm complexity increase cost of service provider will also increase, which mean algorithm complexity is directly proportional to cost.

III. NEW SECURITY ANALYSIS IN CLOUD COMPUTING

In this section we analyze the security mechanism related with data integrity, data inrusion, and service availability.

A. Homomorphic token technique

In the cloud data storage system, users store their data in the cloud and no longer possess the data locally. Thus, the correctness and availability of the data files being stored on the distributed cloud servers must be guaranteed. One of the key issues is to effectively detect any unauthorized data modification and corruption, possibly due to server compromise and/or random Byzantine failures. Besides, in the distributed case when such inconsistencies are successfully detected, to find which server the data error lies in is also of great significance, since it can always be the first step to fast recover the storage errors and/or identifying potential threats of external attack.

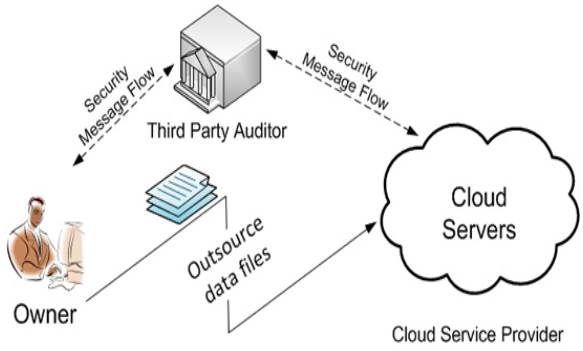

Fig. 3Towared secure storage multi. cloud computing architecture

To address these problems, our main scheme for ensuring cloud data storage is presented in this section. The first part of the section is devoted to a review of basic tools from coding theory that is needed in our scheme for file distribution across cloud servers. Then, the homomorphic token is introduced. The token computation function we are considering belongs to a family of universal hash function, chosen to preserve the homomorphic properties, which can be perfectly integrated with the verification of erasure-coded data. Subsequently, it is shown how to derive a challenge response protocol for verifying the storage correctness as well as identifying misbehaving servers. The procedure for file retrieval and error recovery based on erasure correcting code is also outlined. Finally, we describe how to extend our scheme to third party auditing with only slight modification of the main design.

B. File division technique

In order to achieve secure, storage and access on outsource data in the cloud we exploit the technique of multiple division to protect the data files. Proposed model has enabled us to store data easily and securely. As in this method dividing the data into multiple parts and as the number of part increase the security of data also increase because it is difficult for intruder to check all file to match the content as shown in fig.2. Here we are not focusing on using any technique for multiple division we can use any basic mechanism to divide file to reduce the cost.

To illustrate this model we use example there are three clients represented as a C1 and C2.And they stored there data in two different cloud service provider its represent as CSP1 and CSP2. client store there data in the CSP that data will be divided in the form of multi division technique in the client side and that multiple data stored in an redundant form into both the cloud service provider simultaneously such that if any cloud service.

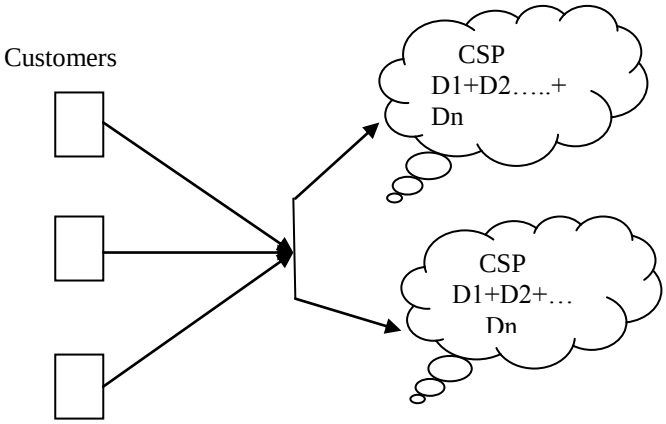

Fig. 4 A cost effective multi. cloud computing model

C. Depsky model

This section will explain the recent work that have been done in the area of multi cloud. A virtual cloud storage system is called depsky.It address the issue like data integrity , availability in multi cloud.

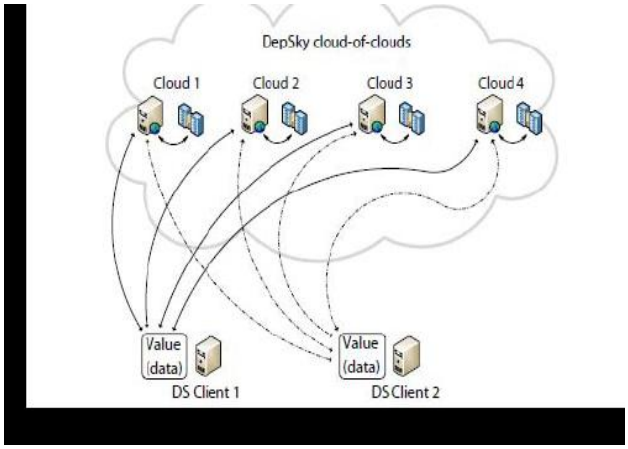

Fig. 5 A depsky architecture [3]

A depsky architecture [3] consist four cloud and each cloud uses its own particular interfaces. The depsky algorithm exist in client machine as a software library to communicate with cloud as shown in fig.5.These four cloud are storage cloud, so there are no code to

be executed. The depsky library allow only reading and writing permission with the cloud storage.

D. Privacy protocol

Data and software process protocol steps executed by cloud customers to add the privacy enforcement structure to the software and data before transferring them to the cloud.

Privacy feedback protocol describe essential component that should be considered and planned through when designing privacy aware cloud service .The main aim of this protocol to inform user for the various privacy mechanism applied on their data and make them to aware of risk.

IV. COMPARING THE SECURITY ISSUES IN CLOUD COMPUTING

Ref	Year	Data integrity	Data availability	Single cloud	Multi cloud	Security mechanism	Cost		
							Low	Medium	High
[1	2012	Follow	Follow		Follow	Homomorphic token technique		Follow	
[2	2011	Follow	Follow		Follow	File division technique		Follow	
[3	2011	Follow	Follow		Follow	Depsky algorithm			Follow
[4	2011	Follow survey		Follow			Follow		
[5	2010				Follow	RAID like technique		Follow	
[6	2010			Follow			Follow		
[7	2009	Follow		follow		Privacy protocol	Follow		

Table 1 Comparison based on issues in cloud computing

Table 1 illustrate the advantage of single cloud model over multi cloud model. It also address some specific issues in single cloud as well as multi cloud and give the comparison between them. It is clear from the table that there are more research have been done in the past in single cloud as well as in multicloud. Multicloud can address the issues like data integrity, data availability and data intrusion. and in addition most of the research focus on providing the secure storage such as in depsky.Therefore providing the cloud data base storage system instead of normal storage system is a significant role in order to run queries and deal with database. Table 1 also illustrate that in 2010 80% of the research are based on single cloud and about 20% of research are based on multi cloud .It is clear from the past that the more research has been conducted in the area of single cloud in comparison to multi cloud

Cost is the one of major issue in multi cloud model because as the data redundancy increase among the service provider cost will increase and as the data store redundantly security of data also needed, so moving to complex algorithm also charge cost of implementation .The cost increase as the complex algorithm increase .To overcome these problem some author used some technique like token, file division method to reduce the cost. By applying these technique the cost will be reduce as compare to algorithm. But this scheme is not fully secure they just balance the security risks and cost. in future they need to go for more secure scheme to make their user data more secure.

V. CONCLUSION

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 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 SP for his outsourced data is not very promising, so we are switching toward multi cloud. The cloud computing security is still a major issue in cloud computing enviroment.in addition the loss of service availability and data integrity are the major problem for the customer.Furthermorte data intrusion increase so many problem to the user of cloud computing.

The purpose of this work is to focus on the security issue and cost related with single cloud as well as multi cloud. Much research has been done on the single cloud and more research are going in the area of multi cloud to overcome these cost and security issue as well. we support the migration on multi cloud.

REFERENCES

[1] Cong Wang,student member,ieee,Qian Wang,student member,ieee, Kui Ren,member,ieee,Ning Cao,student member,ieee and Wenjing Lou,senior member,ieee,"Towared secure and dependable storage in cloud computing" 2012.

.

[2] Yashaswi Singh,Farah Kandah,Weiyi Zhang," secure cost effective multi cloud storage in cloud computing"2011.

[3] A.Bessani, M. Correia, B.Quaresma, F.Andre and P.Soura "Depsky:dependable and secure storage in cloud computing."2011.

[4] F.Rocha and M.Correia "lucy in the Sky without Diamond: stealing Confidential Data in the Cloud", Proc 1stIntl . Workshop od Dependability of Clouds, Data Centres and Virtual Computing Environments, 2011.

[5] Computing, 18(5), 2006, pp. 387-408. H.Abu-Libdeh, L.Princehouse and H.Weatherspoon, " RACS: a case for Cloud storage

diversity",SoCC '10: Proc. 1stACM symposium on Cloud Computing,2010.

[6] E.Grosse, J.Howie, J.Ransome, J Reavis and S.Schmidt, " Cloud computing roundtable", IEEE Security & Privacy,8(6),2010.

[7] W.Itani, A.Kayssi, A.Chehab, "Privacy as a Service: Privacy-Aware Data Storage and Processing in Cloud Computing Architectures" Eight IEEE International Conference on Dependable, Autonomic ans Secure Computing,Dec 2009.

[8] R.Gellman, "Privacy in the cloud: Risks to privacy and confidentiality from cloud computing",Prepared for the World Privacy Forum Feb 2009.

[9] B.R.Kandukuri, R.V.Paturi and A.Rakshit, "Cloud Security Issues," 2009 IEEE International Conference on Service Computing, 2009.

[10] Scalable Security Solutions, Check Point Open Performance Architecture, Quad-Core Intel Xeon Processors,"Delivering Application-Levels Security at Data Centre Performance Levels,"Intel Corporation, 2008.

[11] S.L.Garfinkel," Email-based identifcation and authentication: An alternative to PKI? ",IEEE Security and Privacy.

[12] Identifying the data integrity in cloud storage IJCSI International Journal of Computer Science ISSUES, Vol.9, Issue 2,No 1,March 2012.

.