International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue 13
October 2017

A Strategy of Methodology for Multi-Cloud Storage security in Cloud Computing

Chanaveni Chaithanya
Assistant professor, Department of CSE Siddhartha College of Engineering and Technology, Hyderabad, Telangana, India

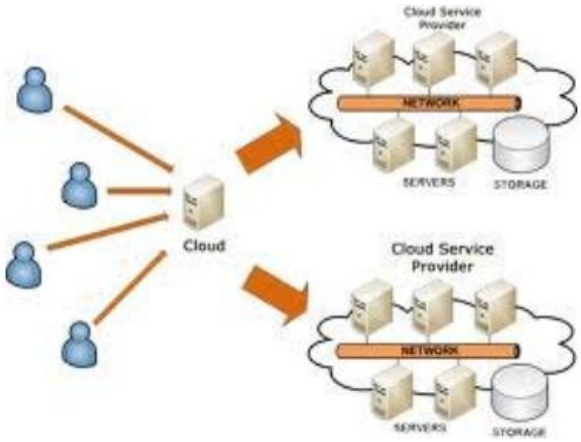
ABSTRACT: *As new storage model, cloud storage has gainattentions from in cooperation the academics and industrial communities.Nevertheless along with variant advantages, it also carries newchallenges in maintaining data integrity and highly available reliable data storage facility.In addition,provided that better privacy as wellas make sure data availability,can be accomplish by dividing the user's data block into data pieces and distributing them among theavailable Service Providers in such a way that no less than a threshold number of Service Providers can take part in effectiveretrieval of the whole data block.In this paper,we propose a secured cost-effectivemulti-cloud storage(SCMCS)model in cloudcomputing which holds an economical distribution of data among the available Service Providers in the market,to provide customers with data availability as well as secure storage.*

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

I. INTRODUCTION

One of the outstanding offerings provided in cloud computing isthe cloud data storage, wherein subscribers do now not need tostore their data on their very own servers, in which as a substitute their data could be stored at the cloud service company's servers.In cloud computing, subscribers need to pay the servicevendors for this storage service. This service does no longerhandiest presents flexibility and scalability for the data storage,it additionally offer clients with the gain of paying only forthe quantity of data they want to shop for a selected periodof time, without any uncertainties for efficientstorage mechanisms and maintainability troubles with huge quantities ofdata storage. In addition to these benefits, clients caneasily get access to their data from any geographical region wherethe Cloud Service Provider's network or Internet may beaccessed. Data storage additionally redefines the security troublescentered on client's outsourced data (data that isn't alwaysstored/retrieved from the clients very own servers). Sincecloud service providers (SP) are separate marketplaceentities, data integrity and privateness are the maximum crucial problemsthat need to be addressed in cloud computing.

Fig1: distribution of data over several SP'sIn addition, providing better privateness in addition to make sure informationavailability, can be executed via dividing the facts amongseveral SP s to be had in the market, based on his availablefinances. Also we offer a choice for the consumer, towhich SP s he ought to selected to access data, with admire to data access great of service offered via the SP's on the area ofdata retrieval.



In this survey we additionally offer the consumer with better guaranteeof availability of data, by using maintaining redundancy in recordsdistribution. In this situation, if a service issuer undergoesservice outage or is going bankrupt, the user nonetheless can get access to his data by means ofretrieving it from other service vendors. From the commercial

enterprisefactor of view, due to the data that cloud data storage is a subscriptionprovider, the higher the data redundancy, the better could be thecost to be paid by means of the user. Thus, we provide an optimizationscheme to address the tradeoff between the price that a cloudcomputing user is inclined to pay to achieve a particular stageof security for his data. In different words, we offer a schemeto maximize the security for a given finances for the clouddata.

II. RELATED WORKS

Before considering the cloud computing technology. It isimportant to understand the risks involved. We should carryout the risk assessment process before any control is handedover the to a service provider.

A. Data storage and security: Many cloud service provider provide storage as a service. They takethe data from the user and stored on the large data centers, henceproviding a user means of storage. Although these service providersays that data stored in a cloud is safe but there have been somecases where data is been modified or lost due to security holes.Various cloud provider adopt various technology to resolve theproblem of cloud data storage. The virtualized nature of cloud makethe traditional mechanism unstable for handling the security risks sothese service provider use different encrypting technique toovercome these problems.

B. Application level security: Application level security refers to the usage of software andhardware resources to provide the security to application suchas attackers are not make any changes in the applicationformate.Now a days attacker launched them as a trusted userand system consider them as trusted user and allow full accessto attacking party. The reason behind this is using outdatednetwork policies. With the technological advancement thesesecurity policies become obsolete as there have been instances whensystem security have been breached, but with the recent technologyadvancements it is quit possible to imitate a trusted user. The threatto application level security include sql injection attack ,dos attack,captcha breaking , xss attack.

C. Data intrusion: Another security risk that occurs in cloud computingenviroment, such as the google doc cloud service is a hackedpassword or data intrusion. If someone gain access to googledoc password then they will able to gain all account instanceand resources .The stolen password allow the hacker tomodify ,erase the full data and even disable the services.

D. Single to multicloud: The use of cloud computing have increase in manyorganization. The cloud computing provide a many benefit interms of cost and avalability.The pay per use model know ascloud computing. One of the prominent service offer by cloudcomputing is cloud data storage, in which subscriber don'twant to store their data on their own server, instead of thatthere data stored in cloud service provider. This service don'tprovide only flexibility and scalability for data storage but italso provide the customer with the benefit of only for theamount of data they need to store for the particular period oftime. In addition to these benefits customer can access theirdata from anywhere as long as they are connected to internet.Since the cloud service provider is the different marketentities, data integrity and privacy are the most commonissues that need to be address in cloud computing. Eventhought the cloud service provider have standard regulationand power infrastructure to ensure the customer data privacyand provide a better availability. The political influence mightbecome an issue with the availability of the service.

III. APPROACH

We 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 pricedon two factors, how much data is to be stored on the cloudservers 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 periodof time. We consider p number of cloud service providers (SP),each available cloud service provider

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue 13
October 2017

is associated with a QoSfactor, along with its cost of providing storage service per unitof stored data (C). Every SP has a different level of quality ofservice (QoS) offered as well as a different cost associated withit. Hence, the cloud user can store his data on more than oneSPs according to the required level of security and their affordable budgets.

Threat Model: Customers' stored data at cloud service providers is vulnerable to various threats. In our work, we consider two typesof threat models. First is the single point of failure [7], whichwill affect the data availability that could occur if a server atthe cloud service provider failed or crashed, which makes itharder for the costumer to retrieve his stored data from theserver.

Availability of data is also an important issue which could beaffected, if the cloud service provider (SP) runs out of business.Such worries are no more hypothetical issues; therefore, acloud service customer can not entirely rely upon a solo cloudService Provider to ensure the storage of his vital data.

To illustrate this threat we use an example in Fig. 1. Let usassume that three customers (C1, C2 and C3) stored their dataon three different service providers (CSP1, CSP2 and CSP3)respectively. Each customer can retrieve his own data fromthe cloud service provider who it has a contract with.

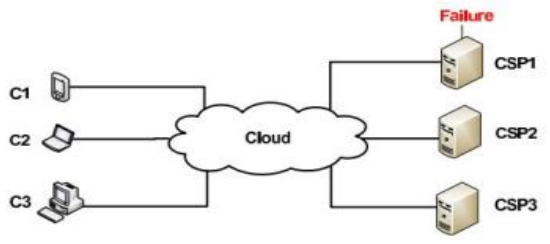


Fig2. CSP failure

If a failure occur at CSP1, due to internal problem with the server orsome issues with the cloud service provider, all C1's datawhich was stored on CSP1's servers will be lost and cannot beretrieved. One solution for this threat is that, the user will seekto store his data at multiple service providers to ensure betteravailability of his data. Our second threat discussed in thispaper is the colluding service providers [8], in which thecloud service providers might collude together to reconstructand access the user stored data.

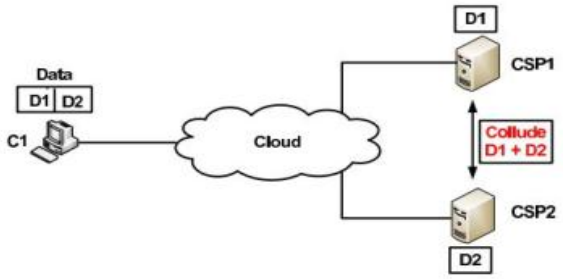


Fig.2 Colluding Service provider

We illustrate the colludingservice providers' threat in Fig. 2. (SCMCS) seeks a distribution of customer's data pieces among the available SPs in sucha way that, at least q number of SPs must take part in data retrieval, while minimizing the total cost of storing the data onSPs as well as maximizing the quality of service provided bythe SPs.

In this work we observed that, from a customer's point ofview, relying upon a solo SP for his outsourced data is notvery promising. In addition, providing better privacy as wellas ensure data availability, can be achieved by dividing theuser's data block into data pieces and distributing themamong the available SPs in such a way that no less than athreshold number of SPs can take part in successful retrievalof the whole data block.We proposed an economical distribution of dataamong the available Service Provider to provide customers

with data availability as well as secure storage. In our model,the customer divides his data among several SPs, based on hisavailable budget. Also we provide a decision for the customer,to which SPs he must chose to access data, with respect to dataaccess quality of service offered by the SPs at the location of
data retrieval. This not only rules out the possibility of a SPmisusing the customers' data, breaching the

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue 13
October 2017

privacy of data,but can easily ensure the data availability with a better qualityof service.

This approach will provide the cloud computing users a decision model, that provides a better security by distributing the data over multiple cloud service providers insuch a way that, none of the SP can successfully retrieve meaningful information from the data pieces allocated at their servers. 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 serviceoutage or goes bankrupt, the user still can access his data byretrieving it from other service providers.

In this section we describe the setup for the linear programming assignment problem (LP-Assignment) that describes our proposed model. Each cloud customer is providedwith p cloud service providers, where each of them offers aQoS level for storage services and required a cost C be paid bythe customer per storage unit of data.
One of the objectives is to minimize the cost of storage of the datapieces over p service providers. If di is the number of data piecesstored on ith provider which has a per unit cost of storing thedata as ci.The total cost the customer has to pay is given below:
$C = \sum^{a}_{i} d_i c_i$ …… (1.1)

In our model, we consider yi,j as a binary variable, which is set to1 if the jth data piece on ith service provider becomes a candidatein the current data retrieval. Since the Quality of Service factordepends on the physical location of information retrieval, the Quality of Service achieved in retrieving the data can be computed as given in following equation (1.2).

$$Q_{net} = \sum_i^a \sum_j^{d_i} y_{i,j} * Q_i \quad \ldots\ldots\ldots\ldots\ldots\ldots \quad (1.2)$$

Therefore, the total cost of storing the dis-tributed customer dataon a number of service provides must be minimized, and theQuality of Service achieved at the time of retrieval must be maximized. The objective is:

Minimize [C] and Maximize[Qnet] ……. (1.3)
Maximize [Qnet – C]…… (1.4)

Constraints: Since d_i is the data pieces allocated to stored atith Service provider, this implies:
$\sum_{j=1}^{a} d_i$=N…… (1.5)

Referring to the (k, N) threshold and the (b,a) threshold discussedbefore, the minimum number of pieces that must be chosen fordata retrieval is k, for which at least b service providers are required. Thus, we have

$\sum_{j=1}^{a} y_{i,j} \geq b$…… (1.6)
and
$\sum_{j=1}^{a} \sum_{i=1}^{d_j} y_{i,j} \geq k]$…… (1.7)

where, N ≥ k and a ≥ b. Now, to make sure that a single ServiceProvider can not retrieve any meaningful information, the number of data pieces allotted to each Service Provider must be lessthan k

$0 < d_i < k$…… (1.8)

Solution: Since we have multiple optimization objectives as wellas a set of variables di with non-definitive bounds, it seems to bevery complex Linear programming problem. The model can besimplified with the help of lemma 1.

IV. CONCLUSION

In this paper, we proposed asecured cost-effective multicloud storage (SCMCS) in cloudcomputing, which seeks to provide each customer with a bettercloud data storage decision, taking into consideration the userbudget as well as providing him with the best quality of service (Security and availability of data) offered by availablecloud service providers.

REFERENCES

[1] M. Armbrust, A. Fox, R. Grifth, A. D. Joseph, R. Katz, A. Konwinski,G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia. Above theclouds

:Aberkeley view of cloud computing. Technical report,University of California at Berkeley, February 2009.

[2] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic. Cloudcomputing and emerging it platforms: Vision, Future GenerationComputer Systems, 25(6):599– 616, 2009.

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

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

[5] M Arrington,GmailDisaster:Reports of mass email deletions"Onlineat http://www.techcrunch.com/2006/12/28/gmail-isasterreportofmass-email deletion/,December,2006

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

[7] N. Gruschka, M. Jensen, "Attack surfaces: A taxonomy for attacks oncloud services", Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on, 5-10 July 2010.

[8] J. Du, W. Wei, X. Gu, T. Yu, "RunTest: assuring integrity of dataflowprocessing in cloud computing infrastructures", In Proceedings ofthe 5th ACM Symposium on Information, Computer and Communications Security (ASIACCS '10), ACM, New York, NY, USA,293 304.

[10] Scalable Security Solutions, Check Point Open PerformanceArchitecture, Quad-Core Intel Xeon Processors,"DeliveringApplication-Levels Security at Data Centre Performance Levels,"IntelCorporation, 2008.

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

[12] Identifying the data integrity in cloud storage IJCSI InternationalJournal of Computer Science ISSUES, Vol.9, Issue 2,No 1,March2012.

Biodata:

Chanaveni Chaithanya working as Assistant professor, Department of CSE in Siddhartha College of Engineering and Technology, Hyderabad, Telangana, India. I have completed my M.Tech from Vivekananda College Of Engineering & Technology