International Journal of Advanced Technology in Engineering and Science
Vol. No.5, Issue No. 03, March 2017
www.ijates.com
ijates
ISSN 2348 - 7550

# AN APPROACH OF MOBILITY OF DATA AMONG CLOUDS

**K.Bhargavi[1], Somashekahr[2], M.Manohar[3]**

**ABSTRACT**

*Providing the data for sectors like public and private is the motto of cloud computing. Cloud computing not only stores the data but organizes and arranges the data, with a high security. In this paper we are focusing on accessing the data only from public cloud and hybrid but also from private cloud considering the security and privacy issues. We have discussed the concept of sharing the data in both public and private cloud. However, there exists many such procedures but we have tried a mechanism of sharing the information.*

## I. INTRODUCTION

***"We change our behaviour when the pain of staying the same becomes greater than the pain of changing. Consequences give us the pain that motivates us to change" – Dr. Henry Cloud and Dr. John Townsend***

Successful businesses require the ability to change and increasingly to adapt quickly, to be agile to new approaches and technologies and be flexible to the needs of the business and customers.IT needs to keep up with the speed of business and support the needs to be successful and no longer be constrained by contractual boundaries, shortage of localized skills or existing platform limitations. The need to build agility into decisions you make is going to become increasingly part of the selection process.

Change is never easy where you have to conform to policies, security requirements, standards, decision processes and budgets and it is going to get harder with the ever higher demands and expectations of users and customers. Resisting change or finding reasons not to do it will carry less and less weight. Businesses are going to have to become agile and to find ways to offload workloads to others to allow themselves to focus on the needs of the business, to become unconstrained and more flexible.

To serve users and customers in a way they want and expect to be serviced is going to be key and being open to utilising new technologies such as cloud, mobility, big data and to changing again and again where needed will be critical in the new economy.This paper aims at providing a method of sharing the data with simplest at ease methods considering the security aspects of the broker and company. We have tried a theoretical method of sharing the data among clouds.

## II. PROBLEM

Sharing the data among the cloud is the major problem in industry, but it is the worth fetching factor for the cloud brokers. Virtualization technology is at the heart of any public or private cloud datacenter. It allows providers to get more out of physical resource by allowing multiple instances of virtual cloud resources to run concurrently. Each virtual resource believes it has its own share of hardware resource.

The private cloud datacenter area is dominated by vendors such as VMware, which manages datacenter resources using ESX virtualization technology and vCloud API access to the hypervisor.

Public cloud providers, such as Amazon and Microsoft, have adopted KVM, Hyper-V, and Xen virtualization technologies for managing their datacenters.Sometime it becomes difficult either to the company owner or to the public to know the details or upcomings , if cloud data center doesnot reveal the information. Because providers might update this information without notifying users, it can be difficult to manually obtain service configurations from cloud providers' websites and documentation (the only sources of information).

## III RISKS INVOLVED

One side effect of the lack of interoperability among cloud providers is vendor lock-in, which also means lack of ability to migrate application components and associated workload from cloud provider A to cloud provider B. This article investigates the technical challenges from the user-to-multiple cloud interoperability perspective.

## IV. NEED

In this cloud integration model, application owners are responsible for provisioning their application components over resources belonging to multiple providers. In this scenario, owners typically implement or use an application provisioner software program (such as RightScale [www.rightcale.com] or CloudSwitch [https://home.cloudswitch.com]), which distributes application components across multiple resource providers to meet the SLAs in an optimal way. This article covers the challenges inherent in the cloud-to-cloud interoperability perspective—that is, the cloud integration model consisting of multiple cloud providers that cooperatively integrate (via federated middleware software) their datacenter resources to support seamless migration of application workload and components across each other.

## V. MODEL

To access the data from public cloud is very easy [fig1]as it does not require much authenticated information neither from client side nor from company's side. Where as to access the data from private cloud requires many such authentication.

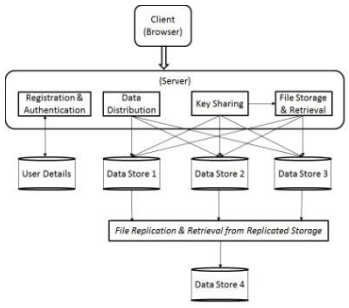


Fig1

We have discussed a small module apart from existing API's and management tools .The method involves proper identification of both client and company owner technically.

1) If the person requires the company's private cloud data, the login module must contain the relevant position of the client in the company with password (HTTP )
2) Depending on the position or role of the client in the company the cloud broker is going to provide the accessibility of database to client, with OTP provided to the client from company. Matching of the

client OTP with company's OTP and cloud broker's OTP and communication of cloud broker with company's head the cloud broker will give access to the a part of the database.

3) Database accessing is further divided depending on the roles of the employee. Even though there exists all the authentication details the cloud broker will be denied to access the whole database.
4) Situation where the client is not a part of the company but still want to access the database then there exists a different scenario

1) The user will be identified in login module –details like

-> company of the client where working

->Role of client in company

->Need of the data to the client

Company details

2) After the authentication, the user will be verified by the cloud broker and company's head for authentication
3) If found correct then the user will be given a virtual database environment to work with.
4) No data is allowed to carry by the user-only evaluations and statistical calculations can be done.

> Roles and privileges are to be given specifically to the employees while interacting with the cloud or cloud environment.
> Session Time out password must be assigned to only those employees who are sharing the cloud environment
> To have the approval of the company's owner the module should be designed in such a way that no other hacking mechanism could break it like digital signature, thumb or eye retina scanning.

If we implement this a normal user can have an access to the some part of the company's private data. This may reduce work on company's product marketing strategy. This can even provide a good strategy on the user for accessing only that company's product. Providing videos of manufactured goods and manufacturing goods may be known by the customer for their future reference.

The figure below defines the flow of data from client identification module to company's head identification module.

## VI. CONCLUSION

It is clear that use of data sharing in clouds is rapidly increasing; client wants to have access data from multiple sources . Due to this, people or customers prefer storing the data in multiple clouds . Thus this paper implements a solution to provide data to client from multiple clouds with high level of security and authentication constraints. It also supports the migration to multi-cloud environment due to its ability to decrease security risks that affect the cloud computing user.The method proposed in this system will overcome the client problem of accessing the data from multiple clouds .

**REFERENCES**

[1] Mohammed A. AlZain, Eric Pardede , Ben Soh, James A. Thom, "Cloud Computing Security: From Single to Multi-Clouds", 2012 45th Hawaii International Conference on System Sciences, pp. 5490-5499

[2] Nikhil Shrivastva, Ajay Survase, Poorva Andurkar, Shubhada Bhandare, "Cloud Computing Security using Multiple Cloud", International Journal of Emerging Trend in Engineering and Basic Sciences (IJEEBS), Volume 2, Issue 1

[3] Francisco Rocha, Miguel Correia," Lucy in the Sky without Diamonds: Stealing Confidential Data in the Cloud", IEEE 2011, pp. 129-134.

[4] Mukesh Kant, Tripathi Jaypee, "Enhanced Cloud Computing Security with the help of Inter-Clouds", IEEE transaction on Service Computing, 2012, pp. 122-127

[5] B.Arun, S.K.Prashanth," Cloud Computing Security Using Secret Sharing Algorithm", paripex -indian journal of research, March 2013, pp. 93-94.

[6] B.Srinivasulu, S.V.Sridhar, U.Narasimhulu, K.Ramakrishna, "Cloud Computing Security potential for migration from a single cloud to a Multi-Cloud Environment", International of Advanced Research in Computer Science and Software Engineering Research, Volume 3, Issue 5, May 2013, pp. 919-925 .

[7] M.A. AlZain and E. Pardede, "Using Multi Sharesfor Ensuring Privacy in Database-as-a-Service", 44th Hawaii Intl. Conf. on System Sciences (HICSS), 2011, pp. 1-9.

[8] H. Abu-Libdeh, L. Princehouse and H. Weatherspoon, "RACS: a case for cloud storage diversity", SoCC'10:Proc. 1st ACM symposium on Cloud computing, 2010, pp. 229-240

[9] K. Birman, G. Chockler and R. van Renesse,"Toward a cloud computing research agenda", SIGACT News, 40, 2009, pp. 68-80

[10] C. Cachin, R. Haas and M. Vukolic, "Dependable storage in the Intercloud", Research Report RZ, 3783, 2010

[11] G. Brunette and R. Mogull (eds), "Security guidance for critical areas of focus in cloud computing", Cloud Security Alliance, 2009

[12] H. Takabi, J.B.D. Joshi and G.-J. Ahn, "Security and Privacy Challenges in Cloud Computing Environments", IEEE Security & Privacy.