



HYBRID CLOUD EXPLOITING THE ASSETS OF BUSINESS VALUE

Mr. Sadigale Parimal Ravindra¹, Mr. Chavan Aniruddha Shrimant²,
Mr. Shinde Khandu Dhondiram³

^{1,2,3}Professor, Dept. of Computer Technology, Karmayogi Polytechnic College, Shelve-
Pandharpur, Dist-Solapur, State - Maharashtra, India

ABSTRACT:

Cloud is kind of centralized database where numerous clients accumulate their data, recover data and possibly adjust data and it is a representation where user is made available services by Cloud Service Provider on the basis of pay per use. Numerous organizations are now taking most important steps in the direction of cloud computing. A hybrid cloud is a grouping of both public and private clouds which are bound mutually by either harmonized or proprietary knowledge that facilitates data and application portability. Hybrid clouds present the benefits of outlay and scale of public clouds although also offering the security and organizing of private clouds. Hybrid clouds can be measured an intermediary stage as enterprises organize to progress for the most part of their workloads to public clouds. All along with the characteristic security concerns associated through private clouds, there are several additional factors one should regard in a hybrid environment. Hybrid environments entail both on-premise and public cloud providers, several additional infrastructure security considerations come into the view which is normally related with public clouds.

Keywords: *Cloud, Hybrid environment, Public cloud, Private cloud.*

1. INTRODUCTION:

Cloud computing construct on established trends for motivating the cost out of the delivery of services while growing the speed and agility with which services are deployed. Companies are obtaining technology services as they are necessary and paying only for the resources they get through to a certain extent than maintaining their personal capital intensive

IT infrastructure [4]. For all the excitement and hyperbole that has enclosed the cloud, contrasting other passing technology tendencies, cloud computing is certainly no fad. Significantly, it's a progress that is altering the way IT delivers value. The advantages of cloud computing include on-demand self-service, ubiquitous network admission, location autonomous resource pooling, fast resource elasticity, usage-based charge, transmission of risk. Organizations are normally finding that the

services of public cloud and private cloud have potencies but also limitations which can provide as barriers to adoption [8]. The most excellent business solutions will frequently be built by means of integrating a grouping of two or more applications running on the systems of private and public. The financial benefits offered by means of public clouds are striking enough for numerous organizations to move forward some of their workloads of non-critical to such services although using private clouds for their needs of mission-critical. Such deployments of hybrid cloud have confirmed to be beneficial not just in terms of enhanced economics however also in terms of business agility. A hybrid cloud shown in fig1 is a grouping of both public and private clouds which are bound mutually by either harmonized or proprietary knowledge that facilitates data and application portability. It may possibly be a combination of a private cloud within an organization with one or additional providers of public cloud or a private

cloud hosted on third-party premises with one or additional public cloud providers [12]. The key difference between private and hybrid clouds is the extension of service provider-oriented low cost cloud storage to the enterprise [1]. That is remote cloud resources are perfectly consistent & integrated in the private cloud, and thereby create a hybrid cloud [1]. Hybrid cloud infrastructures have to factor in the setup and operating cost for a data center (e.g. hardware, power, cooling, and maintenance) as well as the usage-based costs of the cloud provider. Depending on utilization, data center cost and the costs of the cloud provider, businesses have to decide whether or not moving to the cloud is profitable. An environment of hybrid cloud can assist meet their requirements.

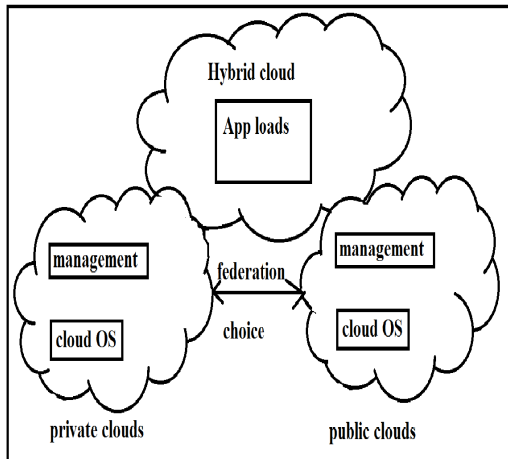


Fig1: An overview of hybrid cloud

2. CATEGORIZATION OF CLOUD SERVICES:

In order create the illusion of infinite resources and elasticity, virtualization technology is needed. Depending on how abstracted resources are, different service models are differentiated as [2] [3] [7]: Software as a Service (SaaS): at the highest level of abstraction, users are mostly unaware of the fact that are using cloud-enabled applications, and are hence not able to control the underlying resources. Instead, they simply use client

interfaces such as web browsers. A popular example is the salesforce.com CRM system [5]. Platform as a Service (PaaS): users are able to develop and deploy applications within the provider's hosting environment, e.g. a Java application framework. Low-level resources are not controlled by the cloud user. Prominent example is the Google App Engine [4]. Infrastructure as a Service (IaaS): at the lowest level of abstraction, cloud users have access to virtualized resources such as processing time, networking or storage. They are provided virtual machines and can run arbitrary software. Famous example is Amazon EC2 [6].

3. ALLEVIATING THE RISKS CONNECTED WITH HYBRID CLOUD DEPLOYMENTS:

Hybrid clouds can provide as a transitional approach and assist businesses fine tune their schemes for upcoming public cloud adoption. Hybrid clouds present businesses a protected shell from which they can attempt out public cloud services, whereas still maintaining susceptible data in a more guarded private cloud. There are several best practices that will assist alleviate the risks connected with hybrid cloud deployments. VM-level security: The boundary of the hybrid cloud surroundings is not only elastic however also spans multiple clouds together with on-premise private clouds. This entitle for self defending defence at the level of virtual machine which moves all the way through on-premise data centre, in the cloud and among providers of multiple clouds. Multi-layered defence: By means of tools such as firewall, log inspection and so on geared on the way to virtual machines is significant. The traffic among the virtual machines should be constantly monitored by means of setting policies aptly. Traffic control: An on-premise entrance should be used to manage incoming traffic to the

public cloud relatively than providing undeviating access. Data and encryption: Data in the cloud have to be encrypted. A solution of encryption should have well-made encryption key management policies to make sure data integrity. In addition, the business has to preserve encryption-key ownership to uphold separation of duties among the business and the provider of public cloud service. This also permits the business to concern their encryption across its clouds of private and public moreover prevents vendor lock in, permitting the organization to progress between cloud vendors [14].

4. ADVANTAGES OF HYBRID CLOUDS:

Hybrid clouds present the benefits of outlay and scale of public clouds although also offering the security and organizing of private clouds. Hybrid clouds can be measured an intermediary stage as enterprises organize to progress for the most part of their workloads to public clouds. Hybrid clouds reduce capital expenses as component of the requirements of organization's infrastructure are outsourced towards public cloud providers. Hybrid cloud improves resource allotment intended for temporary projects at a greatly reduced outlay since the use of public clouds eliminates the requirement intended for investments to perform these projects and also helps to optimize the infrastructure spending throughout various stages of the lifecycle of application [10]. Public clouds can be tapped for expansion as well as testing and can be used to move applications, which might be no longer essential because of the progress to SaaS, at greatly minor costs than committed on-premise infrastructure whereas private clouds can be used for production. Hybrid clouds offer mutually the controls obtainable in a private cloud deployment

all along with the ability to quickly scale by means of public clouds. Supplies maintenance for cloud bursting, tapping the public clouds intended for an unexpected requirement for added compute resources and moreover provides extreme improvements in the overall organizational alertness, as a result of the aptitude to leverage public clouds, leading to augmented opportunities hitherto unavailable in conventional infrastructure or pure private [13].

5. SECURITY NEEDS OF A HYBRID CLOUD ENVIRONMENT:

As organizations make use of hybrid clouds for their business requirements, they must comprehend the new security needs of a hybrid cloud atmosphere. Any businesses planning to organize hybrid clouds should recognize the different security requirements and follow the industry best practices to alleviate any risks. While hybrid clouds suggest the security benefits of private clouds, there are several exceptional security challenges that take place as the perimeter extends further than the organization's limits [15]. All along with the characteristic security concerns associated through private clouds, there are several additional factors one should regard in a hybrid environment such as Perimeter extension: As a hybrid cloud enlarges the IT perimeter exterior to the organizational limits, it opens up an outsized surface area intended for attacks with a segment of the infrastructure of hybrid cloud under the organizing of the service provider [11]. Identity and access management: An easier advance to solving the identity requirements of hybrid clouds is to extend the existing identity of enterprise and access management towards the public clouds. This opens up unease regarding the approach influencing the identity of enterprise and its impact on the organization's safety. Management tools: When organizations administer intricate

hybrid cloud environments by means of a management tool, moreover as a part of the cloud proposal or as a tool of third-party of organizations should regard the security allegations of using such a tool [9]. The management tool has to be able to hold the identity and put into effect security consistently across environments of hybrid cloud. Data migration: A hybrid cloud makes the information flow from a private setting to a public cloud to a great extent easily. There are concerns of privacy and integrity connected with such data movement since the privacy controls in the public cloud surroundings differ considerably from the private clouds. Security policies: There are risks related with the security policies spanning the environment of hybrid cloud.

6. CONCLUSION:

Hybrid clouds present a superior flexibility to businesses while offering selection in terms of keeping control and security. Hybrid clouds are frequently deployed by organizations prepared to push part of their workloads to public clouds moreover for cloud bursting purposes. Since hybrid clouds differ based on company requirements and structure of functioning, there is no one-size-fits-all solution. Hybrid environments entail both on-premise and public cloud providers, several additional infrastructure security considerations come into the view which is normally related with public clouds. Any businesses planning to organize hybrid clouds should recognize the different security requirements and follow the industry best practices to alleviate any risks. Once protected, a hybrid cloud environment can assist businesses transition more applications into public clouds, providing added outlay savings.

REFERENCES:

1. Steve Lesem. Cloud Storage for the Enterprise - The Hybrid Cloud. <http://cloudstoragestrategy.com/2010/01/cloud-storage-for-the-enterprise---part-2-the-hybrid-cloud.html>, January 2010.
2. Peter Mell and Tim Grance. The NIST Definition of Cloud Computing, Version 15. <http://csrc.nist.gov/groups/SNS/cloud-computing/>, October 2009.
3. Michael Armbrust, Armando Fox, Rean Grith, Anthony D. Joseph, Randy H. Katz, Andrew Konwinski, Gunho Lee, David A. Patterson, Ariel Rabkin, Ion Stoica, and Matei Zaharia. Above the Clouds: A Berkeley View of Cloud Computing. Technical Report UCB/EECS-2009-28, EECS Department, University of California, Berkeley, Feb 2009.
4. Google, Inc. Google App Engine. <https://appengine.google.com/>.
5. salesforce.com. CRM Software & Online CRM System. <http://www.salesforce.com/>.
6. Amazon, Inc. Amazon Elastic Computing Cloud. <http://aws.amazon.com/ec2/>.
7. Kevin Lee. Cloud Computing Lecture, December 2009.
8. Ganguly Uttam, "An Approach to Data privacy in Cloud Computing: Keep Sensitive Data Private", International Conference on Computing and Systems 2010, The University of Burdwan.
9. John Harauz, Lori M. Kaufman, Bruce Potter, "Data Security in the World of Cloud Computing", Proceedings of the IEEE Conference on Security and Privacy, July/August 2009, pp 61-64.
10. Balachandra Reddy Kandukuri, Ramakrishna Paturi V, Atanu Rakshit, "Cloud Security Issues", Proceeding of IEEE International Conference on Services Computing, 2009, pp 517-520.
11. Borja Sotomayor, Ruben S. Montero, Ignacio M. Llorente, and Ian Foster. Virtual Infrastructure Management in

- Private and Hybrid Clouds. IEEE Internet Computing, 13(5):14{22, September 2009.
12. Microsoft Corporation. Windows Azure Platform Now Generally Available in 21 Countries. <http://blogs.msdn.com/windowsazure/archive/2010/02/01/windows-azure-platform-now-generally-available-in-21-countries.aspx>, February 2010.
13. Alexander Lenk, Markus Klems, Jens Nimis, Stefan Tai, and Thomas Sandholm. What's inside the Cloud? An architectural map of the Cloud landscape. In CLOUD '09: Proceedings of the 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing, pages 23{31, Washington, DC, USA, 2009. IEEE Computer Society.
14. Steven Fraser, Robert Biddle, Scott Jordan, Kate Keahey, Bob Marcus, E. Michael Maximilien, and Dave A. Thomas. Cloud computing beyond objects: seeding the cloud. In Shail Arora and Gary T. Leavens, editors, OOPSLA Companion, pages 847 {850. ACM, 2009.
15. Constantino Vazquez Blanco. Execution of SGE Clusters on top of Hybrid Clouds using OpenNebula. [http://www.opennebula.org/_media/constantino_vazquez_-_opennebula_-_executing_sge_clusters_on_top_of_hybrid_clouds_using_opennebula.ppt](http://www.opennebula.org/media/constantino_vazquez_-_opennebula_-_executing_sge_clusters_on_top_of_hybrid_clouds_using_opennebula.ppt), September 2009.