Perlustration of Risks and Quality Analysis Tools in Multi-Cloud Environments

Mr. Harsha A C
M.Tech, CSE Department
Dr. Ambedkar Institute of Technology
Bangalore-560056

Prof. Praveena M V
Asst. Professor, CSE Department
Dr. Ambedkar Institute of Technology
Bangalore-560056

***Abstract*—This paper emphasis on multicloud over other cloud deployment models in cloud environment. Since multiple clouds are utilized to deploy multicloud environment, there are various options of cloud vendors with different SLA's. This paper gives an idea on how the cloud vendors can be chosen before adopting by an enterprise by analyzing quality of a cloud and associated risks. The tools like CORAS, PREDIQT and others are used to predict risk and quality of cloud.**

Keywords— multicloud; CORAS;PRIDIQT

I. INTRODUCTION

Cloud computing is not a new technology anymore. Most of us are facilitated by its services over many applications that we are using, but still it's the hot topic to discuss because it has lot new things popping up.

According to NIST (National Institute of Standards and Technology) Cloud computing is defined as "A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."[1] where as Wikipedia defines cloud computing as:"The delivery of computing as a service rather than a product, whereby shared resources, software and information are provided to computers and other devices... Cloud computing provides computation, software, data access, and storage services that do not require end-user knowledge of the physical location and configuration of the system that delivers the services."[2].

Cloud computing is of more concern as nowadays it is difficult to manage business environments using the traditional IT infrastructures as we face tremendous growth in applications in the market, even the data content is growing exponentially, likewise the computational or processing capabilities are required and many newer architectures are being defined which we need to indulge in the infrastructure to meet the growing business standards. Few characteristics of cloud computing defined by NIST[1] addresses the solution to above scenarios, they are:

- On demand self service
- Broad network access
- Resource pooling
- Rapid elasticity
- Measured service

On demand self service: A cloud consumer would access the cloud resources such as storage, computational capabilities, software services etc. when necessary without service provider's interaction.

Broad network access: cloud computing services are available over network and are accessible by even thin platform devices across the globe with proper credentials.

Resource pooling: since the global customers requirement of resources keep changing the resources are pooled over feasible locations so that the services need not always be availed from a single source. Hence we can obtain request and response independence.

Rapid elasticity: the main advantage of cloud computing is elasticity. There is always a variable fluctuation in the consumers' resource requirement. Cloud service provider need to sustain availability of cloud to his customer to meet SLA. and cloud features resource scale up and scale down so quick that will meet such fluctuation in requirement.

Measured service: cloud system also includes a metering mechanism to charge the consumer for the amount of resource he has consumed.

Cloud Providers offer services that can be grouped into three categories.

1. *Software as a Service (Saas)*: service provider would offer his client a complete application or software at customer's ease of use on demand.

2. *Platform as a Service (Paas)*: customer can run his application on cloud without worrying much in implementing the required environment for his application, which will be provided by service provider as a service.

3. *Infrastructure as a Service (Iaas)*: the basic storage and computing capabilities are made available to customer s over the network. Resources (Servers, storage systems, database management etc.) are pooled and offered to customer to meet his workloads.

Cloud is deployed through following models [1],

A. Private cloud model: in this model the cloud infrastructure is operated and designed for a particular organization only. So such clouds are oriented to help improve performance of that enterprise. And they are designed very carefully as they need to deploy from scratch.

B. Public cloud model: in this deployment model the cloud service will be availed over the network for public access. And that does not mean it is free for all, it will have it is own security terms and condition implied.

C. Hybrid cloud model: it is a composition of two or more clouds (private, community or public) that remain separate elements but are bound together, so that the benefits of multiple deployment models are offered together. Multiple clouds feature is aggregated and their capabilities and capacity are combined and served together.

TABLE 1 Summary of the various features of cloud deployment models

Deployment Model	Managed By	Infrastructure Owned By	Infrastructure Located At	Accessible and Consumed By structure
Public	Third party provider	Third party provider	Off-premise	Untrusted
Private	Organization	Organization	Off-premise	Trusted
			Off-premise	
	Third party provider	Third party provider	Off-premise	
			Off-premise	
Hybrid	Both organization and third party provider	Both organization and third party provider	Both on-premise and off-premise	Trusted or Untrusted

Other deployment models [3],

D. Community cloud : infrastructure is shared among several organizations which have common concerns (security, compliance, jurisdiction, etc.), and the services can be accessible for few organizations for which it is availed like in public cloud but less in number than the latter but definitely higher than private cloud.

E. Distributed cloud: Machines distributed over different locations can also provide cloud computing service through a single network such attempt is named as distributed cloud.

F. Multi cloud: multiple cloud computing services are served through a single architecture to reduce dependence on single vendors, increase flexibility, and improve robustness and recovery in case of disasters, etc. It differs from hybrid cloud as it refers to multiple cloud services, rather than multiple deployment modes.

Benefits of multi-cloud

Autonomy – it enables you to deploy your applications on different cloud providers hence reduces dependency on a single vendor. So it provides us with the option to choose vendors who have much more better SLAs. Also it benefits you the liberty of switching among vendors.

Hybridity – applications deployed on a cloud which is geographically near to location of the enterprise results in better response time hence better performance thus we can choose clouds around the globe which favors in improving performance.

Security- in terms of storage services if the data is shared among multiple clouds the data will be much safer from the intruder attacks according to *Shamir's secret sharing algorithm.* [4]

Extended capabilities – in case of a cloud failure the cloud can be replaced without interrupting the customers application hence it can provide higher fault tolerance, also in case of intense applications the load can be shared among remaining clouds than letting a single cloud handle and thus it provides load balancing.

II. ISSUES AND CHALLENGES OF CLOUD COMPUTING:

The cloud computing though has lot of advantages for the enterprises; it also suffers few issues and challenges. According to the survey by International Data Corporation (IDC), Security, Performance and Availability are the three biggest issues in cloud adoption.

- *Security, privacy and availability*

According to the survey by International Data Corporation (IDC), Security, Privacy and Availability are the three biggest issues in cloud adoption. Privacy issues arise as the data flow if out of organizations control there could be serious consequences of trust if the service provider reveals the data or alters it. Availability is important as the cloud adopted should help in maintaining the organizations performance sustained all the time, in case the cloud fails the organizations work flow will be hindered. Security issues can be further classified into

Data integrity: One of the most important issues related to cloud security risks is data integrity. The data stored in the cloud may suffer from damage during transition operations from or to the cloud storage provider, example to such issues faced by Google docs, red hat[5]

Data intrusion: by gaining one's login credentials by an hacker he can cause a greater threat of altering data or erasing it completely such intrusions were faced by Amazon [6][7].

- *Performance*

The cloud must provide improved performance when a user moves to cloud computing infrastructure. Performance is generally measured by capabilities of applications running on the cloud system. Poor performance can be caused by lack of proper resources. Many times users prefer to use services from more than one cloud so that they can have efficient provision of resources. The data intensive applications are very challenging for single cloud service provider to provide proper resources.

- *Reliability and Availability*

Reliability denotes how often resources are available without denial and how often they fail. One of the important aspect that creates serious problems for the reliability of cloud computing is down time. One way to achieve reliability is redundant resource usage. Availability means possibility of obtaining the resources whenever they are needed considering the time it takes for these resources to be provisioned. Some data intensive applications running real time need high availability of resource.

1) Risks and challenges of multicloud

Though multicloud is designed in order to provide maximum benefits out of all the available cloud vendors it has few risk factors too which are the following,

Lack of replacement: a certain cloud service of a vendor may not meet requirements of customer, or requirements may be altered based on situation. So there would be need of a different service is preferable but it may not be possible to find a new service provided by another vendor which meets those requirements and still maintain Interoperability with other clouds in multicloud environment.

Security breaches: since multicloud is a complex system and often the services are provided by many vendors and the data has to flow through many components hence the risk of security breach exists, this can be avoided by shared security agreement to vendors in the multicloud environment.

Data incompatibility: in most cases it happens that the data transferred from a system to other not necessarily feasible with the latter, hence there would be a need of data transmission required, in case of a data intensive applications might ask for data transmission often. Hence the over head of data transmission might increase.

Complexity in cost estimation: by using services from different providers, it may become more and more complex to predict costs.

III. CLOUD SERVICE PROVIDERS

Since we have been addressing cloud service providers who provides cloud services to his customer in reliable means, lets get to know few such cloud vendors. According to *skyhighnetworks*[8] top twenty enterprise cloud services include Amazon web services, office 365, salesforce, ciscowebex, box, yammer, ServiceNow, SuccessFactors, Adobe Echosign, LivePerson, concur, workday, MSDN, SAS On Demand, Github, zendesk, Informatica cloud, Ariba, Host Analytics, Infralinks,Rackspace, Google cloud engine, Windows azure, Softlayer, Hp cloud are few vendors and the list does not end here.

But we need to notice that all these cloud services are not developed equally of course they have different agenda of deploying. *Toptenreviws.com*[9] gives a comparison among few cloud services shown in figure 1.

From Fig 1, we can notice that each service provider provide something good in their unique way. For example consider streaming a video, we need to have higher resolution videos streamed and streamed at higher speed but we want it to consume less data. Though we know the fact that higher resolution images consume more data and the lower resolution images with less data per frame could be streamed at faster rate in an fixed bandwidth. So we will have to extract good from all those cloud services, which is possible by adopting multicloud deployment model.

Deploying multi cloud over traditional infrastructure is not that easy, it needs enterprise to go under a decision making process[10] where in the analyst will have to measure the cloud quality and risks associated, following are few tools which are used to measure.

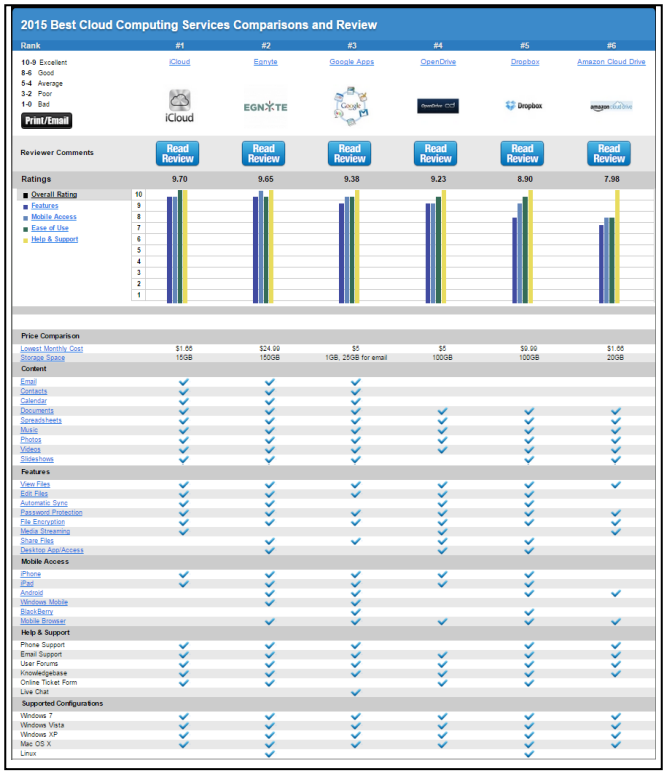

Fig 1. Cloud comparison and reviews

The *Service Measurement Index(SMI)* [11] is a standardization effort from the *Cloud Services Measurement Index Consortium* (CSMIC) consisting of academic and industry enterprises. The Service Measurement Index (SMI) uses characteristics and measures to create a common means to compare different services from different cloud vendors. SMI is a hierarchical framework and divides measurement space into seven characteristics. The characteristics are categorized as Usability, Security, Performance, Agility, and Privacy, Financial assurance and Usability. Then within those attributes KPI's(key performance indicators) are defined that prescribe data to be collected to measure. This is depicted in the following table

TABLE 2 Cloud service-level categories and KPI's table

Service-level category	KPIs	Unit of measurement
Availability	Service window	Time range
	Service/System availability	%
	MTBF	Time units
	MTTR	Time units
Performance	Response time	Seconds
	Elapsed time	Time units
	Throughput	Transaction or request count

Capacity	Bandwidth	Bps
	Processor speed	MHz
	Storage capacity	GB
Reliability	Service/System reliability	%
Scalability	Service/System scalability	Yes/No, or description of scalability upper limit

PREDIQT [12] is a tool which specifies quality characteristics and their indicators, combining indicators into functions for overall quality levels and dependency analysis. The main objective of a PREDIQT-based analysis is by identifying different quality aspects, evaluating these aspects and results in prediction of system quality. The PREDIQT method produces and applies a multi-layer model structure, called prediction models, which represent system design, system quality and the interrelationship between the two.

CORAS [13] is a tool used to analyze risk factor which maintains ISO 31000 risk management standard. Unlike other tools like *CRAMM* [14] and *OCTAVE* [15] rely on text and tables, CORAS uses diagrams as an important means for communication, evaluation and assessment. The core risk analysis segment of the CORAS risk management process are three sub-processes ('identify risks', 'analyze risks', 'risk evaluation'), grouped together at the top layer of the figure. It employs modeling technology for three main purposes:

- to describe the target of assessment at the right level of abstraction.
- as a medium for communication and interaction between different groups of stakeholders involved in risk assessment.
- to document risk assessment results and the assumptions on which these results depend.

Real Option Analysis (ROA)[16], which is a decision support technique in the area of capital investment by means of mathematical models to evaluate financial options. Other approaches to cost estimation in the setting of security investments are *Net Present Value* (NPV) [17], *Return on Security Investment* (ROSI) [18], *Architecture Trade-Off Analysis Method* (ATAM) [19], *Cost Benefit Analysis Method (CBAM)* [20] and the Security Solution Design Trade-Off Analysis [21].

CONCLUSION

This paper emphasis on the multicloud and its advantages over the available single cloud helps in understanding the importance of using multicloud architecture and also provides risks and challenges associated with multicloud adoption. This paper also gives a brief look over few quality and analysis tools to measure the cloud quality and risks associated with it.

ACKNOWLEDGMENTS

Would like to thank my guide Mr.Praveena M V and the anonymous reviewers and friends for their valuable comments.

REFERENCES

[1] The The NIST Definition of Cloud Computing (Draft), accessible: csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf.
[2] http://en.wikipedia.org/wiki/Cloud_computing (April-14)
[3] http://en.wikipedia.org/wiki/Cloud_computing#Deployment_models(April-14)
[4] Adi Shamir, How to Share a Secret, Massachusetts Institute of Technology,1979
[5] C. Cachin, I. Keidar and A. Shraer, "Trusting the cloud", ACM SIGACT News, 40, 2009, pp. 81-86.
[6] S.L. Garfinkel, "An evaluation of amazon's grid computing services: EC2, S3, and SQS", Technical Report TR-08-07, Computer Science Group, Harvard University, Citeseer, 2007, pp. 1-15.
[7] S.L. Garfinkel, "Email-based identification and authentication: An alternative to PKI?", IEEE Security and Privacy, 1(6), 2003, pp. 20-26.
[8] https://www.skyhighnetworks.com/cloud-security-blog/the-20-totally-most-popular-cloud-services-in-todays-enterprise/ (may 5)
[9] http://cloud-services-review.toptenreviews.com/ (april 20)
[10] Aida Omerovic, Peter Matthews, Peter Matthews," Towards a Method for Decision Support in Multi-cloud Environments", IARIA, 2013.
[11] Cloud Services Measurement Index Consortium, "CSMIC," accessed: January 2013. [Online]. Available: http://csmic.org
[12] A. Omerovic. PREDIQT: A method for model-based prediction of impacts of architectural design changes on system quality. PhD thesis, University of Oslo,2012
[13] M. S. Lund, B. Solhaug, K. Stølen: Model-Driven Risk Analysis – The CORAS Approach, Springer, 2011
[14] B. Barber, J. Davey: The use of the CCTA risk analysis and management methodology CRAMM in health information systems. In 7th International Congress on Medical Informatics, MEDINFO'92, pp. 1589-1593, 1992
[15] C. J. Alberts, J. Davey: OCTAVE criteria version 2.0. Technical report CMU/SEI-2001-TR-016. Carnegie Mellon University, 2004
[16] M. Amram, N. Kulatilaka: Real Options: Managing Strategic Investment in an Uncertain World. Harvard Business School Press, Cambridge, Massachusetts, 1999
[17] M. Daneva: Applying Real Options thinking to information security in networked organizations. CTIT Report TR-CTIT-06-11, University of Twente, 2006
[18] W. Sonnenreich, J. Albanese, B. Stout: Return on Security Investment (ROSI)-A Practical Quantitative Model. Journal of Research and Practice in Information Technology, 38(1), 45-56, 2006
[19] R. Kazman, M. Klein, P. Clements: ATAM: Method for architecture evaluation. Technical report CMU/SEI-2000-TR-004, Carnegie Mellon, 2000
[20] R. Kazman, J. Asundi, M. Klein: Making architecture design decisions: An economic approach. Technical report CMU/SEI-2002-TR-035, CMU/SEI, Carnegie Mellon, 2002.
[21] S. H. Houmb, G. Georg, R. France, J. Bieman, J. Jürjens: Cost-benefit trade-off analysis using BBN for aspect-oriented risk-driven development. In 10th International Conference on Engineering of Complex Computer Systems (ICECCS'05), pp.195-204, IEEE Computer Society, 2005.