International Journal of Enhanced Research in Management & Computer Applications
ISSN: 2319-7471, Vol. 5 Issue 1, January-2016

Analysis and Applications of Risk Management in Cloud computing

Laxmi Devi

ABSTRACT

Cloud computing offers its customer's reliable service at flexible prices that do not break the bank. However, as good and innovative as cloud computing may be, it does not necessarily mean that cloud computing is good for all businesses. By researching the cloud computing services available, I will explore the benefits, as well as the drawbacks of cloud computing within the business realm. First of all I will give an introduction to cloud computing. Secondly I will try to define the value preposition. Furthermore I will describe the web services which are delivered by cloud computing. Moreover I will describe the deployment models and about managing the cloud. I will also describe a scenario of migrating to cloud for a small business company. Finally, looking to the future of cloud computing, I will comment on the role that cloud computing can play in businesses in the future.

Keywords: Cloud computing, Service, Cloud Management, Value preposition, Deployment models, Service consumer, Cloud provider, Service developer, Cloud migration

INTRODUCTION

The biggest challenges that companies will face as they move into the cloud are secure data storage, high-speed access to the Internet, and standardization. Storing large amounts of data in centralized locations while preserving user privacy, security, identity and their application specific preferences, raises many concerns about data protection. These concerns, in turn, lead to questions about the legal framework that should be implemented for a cloud-oriented environment. In the second section Assessing the Value Proposition, I will describe the various attributes of cloud computing that make it a unique service. These attributes—scalability, elasticity, low barrier to entry, and a utility type of delivery-completely change how applications are created, priced, and delivered. I will describe the factors that have led to this new model of computing. Early adopters of these services are those enterprises that can best make use of these characteristics. To get a sense for the value of cloud computing, I will try to compare it to on-premises systems. From this perspective, a number of benefits for cloud computing emerge, along with many obstacles. I describe these factors in some detail. Aside from technological reasons, behavior considerations associated with cloud adoption are discussed.

As technology has migrated from the traditional on-premises model to the new cloud model, service offerings have evolved almost daily. I will provide some basic exposure to where the technology is today, and where it will likely be in the not too distant future. In the fourth section Deployment models I will try to illustrate the most typical cloud deployment models. These models demonstrate the performance and economic benefits of cloud computing. They are based on the needs of the widest possible range of consumers. Security, governance, and standards, for example, are all critical aspects. Some parts of cloud computing management which I will explore are: definition of cloud management, management responsibilities, managing desktops and devices in the cloud, lifecycle management, emerging cloud management standards and managing the risks. I will also try to explain how companies should make the move, what are the most important steps to get there, what should their cloud strategy and cloud road map look like etc. Some of the steps are: define adoption approach, select cloud provider, upgrade the organization, and revamp tools and processes.

The Term - Cloud

The term cloud has been used historically as a metaphor for the Internet. This usage was originally derived its common representation in network diagrams as an outline of a cloud, used to represent the transport of data across carrier backbones to an endpoint location on the other hand. This idea started early in 1961 when Professor John McCarthy suggested that computer time-sharing technology might lead to a future where computing power and even specific application might be

sold through a utility-type business model1 . It become very popular in the late 1960s, but in the mid- 1970s the idea faded away because it was clear that the IT-technology in those days was unable to sustain such a futuristic computing model. Since the turn of the millennium, the concept has been revitalized. This concept denotes a model on which a computing infrastructure is viewed as a cloud, from which businesses and individuals access applications from anywhere in the world on demand. The main principle is offering computing, storage and software as a service.

There are many definitions defined for cloud computing. Buyya et al.2 has defined it as ―Cloud is a parallel and distributed computing system consisting of a collection of inter-connected and virtualized computers that are dynamically provisioned and presented as one or more unified computing resources based on service-level agreements (SLA) established through negotiation between the service provider and customer. Vaquero et al.3 have stated ―Clouds are a large pool of easily usable and accessible virtualized resources (such as hardware, development platforms and/or services). These resources can be dynamically reconfigured to adjust to a variable load (scale), allowing also for an optimum resource utilization

A LITERATURE REVIEW

Several researches have been done in the area of SLA and risk management in cloud computing environments. Some of these researches tend to provide new SLA risk management models or frameworks to overcome security issues associated with the SLA in the cloud. This research focuses on an SLA-based risk analysis in cloud computing environments by examining three different SLA factors, which are the risk factor associated with the service, the service cost factor, and the response time factor. The related work in this area lacks research that concerns the SLA-based risk analysis and this may happen because the cloud computing security area has been one of the emerging research areas recently. The following parts discuss different research that has been done in the areas of SLA and risk management in the cloud computing environments.

In term of SLA-based work in cloud computing, Alhamad et al proposed various models in this area such as an SLA-based trusted model for cloud computing. The model helps cloud consumers to evaluate the cloud resources and decides, which resources are more reliable to use. Moreover, Alhamad et al also provided SLA framework for cloud computing. This framework provides good criteria that helps to build a good SLA in cloud computing and it discusses negotiation strategies between the cloud providers and other parties such as a cloud consumer, cloud broker, or SLA's monitoring agent. Hammadi and Hussain proposed a monitoring framework for SLA.

Chi et al. Offered a data structure called "SLA-tree" to support SLA-based decisions in cloud environments. This structure contains two different data sets such as a waiting list of queries to be executed and the other set is an SLA for each query, which points out different queries profits for modifying response times for each query. Jahyun Goo proposed a framework for structuring SLA in IT outsourcing arrangements. This framework provides detailed descriptions of SLA measurement development and accurate statistical validations. This framework covers 11 SLA contractual factors and their relationships with three more sub-factors. This paper produced a benchmarking tool for SLA structuring efforts. Hedwig et al proposed an SLA design for enterprise information systems. This design consists of different state-of-the-art concepts from system management and balances the risk with the process cost.

Bhoj et al [introduced architecture for SLA management in federated environments. This architecture uses SLAs to share selective information within different administrative boundaries. This helps federated clouds' consumers to share, measure, monitor, and ensuring the SLA specifications of the shared services. All those models and frameworks include and describe different SLA factors and metrics. The research chooses two of the most important factors: the response time and service cost. Those two factors have high impacts on making the decision about choosing the cloud service providers.

In term of risk management in the cloud computing environments, similarly, many papers proposed different frameworks in this area. Zhang et al presented an information security risk management framework in cloud environments. This framework presents good insights in understanding the critical areas in cloud environments. It helps to identify threats and vulnerabilities and their impacts in the cloud environments. Furthermore, this framework discusses the possible actions needed to mitigate the risks. Yuqin and Helgesson offered a modified risk management model by integrating the SLA to a pre-existing risk management model.

Morin et al presented several issues and challenges of SLA and risk management in cloud computing. In this research, a risk management framework such as this framework is used to identify and quantify risks in cloud computing environments. In term of SLA-based risk assessment and analysis in cloud computing environments, the European Network and information Security Agency presented a thorough report about risk assessment in cloud environments indicating that

the SLAs force better risk management in cloud computing environments. Likewise, the Cloud Security Alliance (CSA) indicates in its cloud security guide that cloud consumers should engage security departments in the establishment of the SLA so they can enforce some security requirements in the SLA. Research has been done in risk analysis in the area of cloud computing and SLA, in general.

Yeo and Buyya analyzed the resource management policing while accomplishing obligated objectives such as, meeting SLA, reliability and profit. This research uses two different methods for risk analysis: separate and integrated to identify the effectiveness of resource management policies in accomplishing the required objectives. Similarly, Waldman and Mello discussed a framework for risk analysis of non-compliance with SLA requirements.

Moreover, Battré et al presented a risk management process that can be used by grid providers to support SLA provisioning. The risk management process in this paper uses FERMA standard . Also, risk analysis has been done to examine the relationship between the network availability and availability SLA specification and this paper provides methods to control the risk and define availability SLA.

Yang et al presented a patch management framework based on SLA-driven patch applicability analysis, which allows automated analysis and risk assessment for business impact during the patch process. Patel et al [19] provided a mechanism to manage SLAs in cloud computing environments using Web Service Level Agreement (WSLA) framework to monitor and enforce the SLAs and they provided a real world scenario to evaluate their proposal.

Moreover, Hovestadt et al offered a workflow for selecting the best cloud resources according to the assessed risks and they provided some measurements to calculate different factors to support this workflow. Previous research did not relate or analyze information security risk against SLA metrics and specifications as this research intends to do. In term of the different techniques that have been used in the previous research, several researches in the area of SLA risk management in cloud computing are just providing general frameworks and models to implement the risk management process.

Furthermore, most of the risk analysis researches did not implement the research scenarios and they did not even simulate them such as Hovestadt et al which presented risk analysis based on assumptions. Also, Yeo and Buyya focus on the grid environments and they have simulated their environment using GridSim and for cloud environments, it would be better to use CloudSim to simulate cloud environments.

Correspondingly, Waldman and Mello used the state of art model and assumptions to evaluate the risk of non-compliance with SLA requirements. However, this research does not match or relate the risk factor with other SLA factor such as the cost or response time. Yeo and Buyya claim that the work was able to determine the performance difference in resource management policies against a single SLA object or combination of the objects. Moreover, this paper presents decent workflow to select resource according to assessed risks and it provided good methods to do the measurements and this could be used to calculate the risks and decide the best cloud resource. Waldman and Mello state that risk of lack of availability is an essential parameter for the elaboration of SLAs.

THE VALUE PROPOSITION

Cloud computing is based on the paradigm of shared multitenant utility. This paradigm creates new opportunities to the users and developers. The approach of cloud computing, that provides shared resources on a pay-as-you go basis, changes the economics of information technology and creates new types of access and business models. Many applications or processes that have benefit from economies of scale, commoditization of assets and conformance to programming standards will have benefits also from the applications of cloud computing. If they want to have a customized solutions, a high degree of specialization and access to proprietary technology they will expose the limits of cloud computing much more quickly.

Cloud computing represents a combination of the infrastructure of a datacenter with the ability to provision hardware and software. Depending of the service requested, there can be different models implemented. If the service concentrates on hardware then the Infrastructure as a Service (IaaS) model is implemented. An example of this model is Amazon Web Service. If the service requests software stack then the model shifts to the Software as a Service (SaaS) model. An example of this model is Microsoft's Windows Azure Platform.

When the service concentrates on different types of stacks, such as hardware/software/application, then the appropriate model which needs to be used in this case is the Platform as a Service (PaaS) model. Examples of a PaaS offering are SalesForce.com and The Google App Engine. Additionally to the different service models implemented through cloud computing there are also different type of deployment models which can be implemented. If the cloud is available to the

public and it is utilized on a pay-as-you-go basis then the public cloud model is used. If the cloud is used in an organization's infrastructure (network), it is referred to as a private cloud. The mix of these two models is represented as a hybrid cloud. Any analysis of the potential of cloud computing must account for all these possibilities.

The ability of cloud computing to virtualize pooled resources optimizes these investments and allows the cloud provider to pass along these economies to customers. This can blur the difference between a small and large deployment since it becomes tied only to demand. As I described above, scalability is one of the main advantages of cloud. Because of that cloud can provide high performance parallel batch processing that was not done before. Now, if some company wants to perform complex analysis, with the use of cloud this can be done much faster than before when it needed to take days or moths.

Processor-intensive applications that users currently perform on their desktops such as mathematical simulations in Mathematics and Matlab, graphic rendering in Renderman, and long encoding/decoding tasks are other examples of applications that could benefit from parallel batch processing and be done directly from the desktop. The economics must work out, but this approach is a completely new one for most people and is a game changer. Another attribute that makes cloud computing unique is its presents everywhere. This can be used as data storage for the large array of sensors, diagnostic, and mobile devices, all of which both generate data and consume data. After that it is easier to use these data for further researches.

BUSINESS APPLICATIONS OF CLOUD COMPUTING

With a strategic approach to cloud computing, including managing the integration, business process and security obstacles mentioned, cloud opens up fundamentally new ways of doing business. Ways that are not just more efficient and lower cost, but would be impossible without cloud. Ways that enable companies to keep pace with ever increasing consumer expectations, competitive pressures and capture business value in new ways. The true promise of cloud isn‘t just about rethinking IT; it‘s about reinventing business. The value of cloud computing can be seen in these areas:

IT without boundaries

Removing the barrier enables cloud to deliver tasks and workloads with great economies of scale and by best capable experts, whether they are in the company or out.

Speed and Dexterity

Another value of cloud is that it helps the companies to deliver their offerings much more rapidly and gives them end-to-end visibility into the business data.

Creating new business value

Cloud enables collaborations, and this helps companies to cooperate and innovate collectively. Computing in the cloud is done in a different way, and its goal is to be delivered to the consumer in such a way that he will not even thought of.

Cloud computing obstacles

As many things also cloud is not perfect. It may not be practical for any applications. There is also the risk that cloud can deviate from its basic principles. An obstacle is also the resource limitation which appears during the peak conditions. As the power 36 utilities suffer brownouts and outages the same can happen to the cloud computing. Additional obstacle is the pricing method used by some provider. It may not be linear and if that at the entry it is low, it may happen that later it grows and can lead to vast costs. Cloud computing vendors run very reliable networks. Often, cloud data is load-balanced between virtual systems and replicated between sites. However, even cloud providers experience outages. In the cloud, it is common to have various resources, such as machine instances, fail. Except for tightly managed PaaS cloud providers, the burden of resource management is still in the hands of the user, but the user is often provided with limited or immature management tools to address these issues.

Table 1: Challenges and Obstacles to Cloud Computing

Subject Area	Captive	Cloud	Challenge
Accounting Management	Chargeback or Licensed	Usage	In private systems, costs associated with operations are fixed due to licenses and must be charged back to accounts based on some formula or usage model. For cloud computing, the pay-as-you-go usage model allows for costs to be applied to individual accounts directly.
Compliance	Policy-based	Proprietary	Compliance to laws and policies varies by geographical area. This requires that the cloud accommodate multiple compliance

Deployment Models

A deployment model defines the purpose of the cloud and the nature of how the cloud is located. Cloud computing architects have to consider many things before moving from standard enterprise application deployment model to one based on cloud. There are different types of deployment models offered by cloud. They can deploy their applications on public, private or hybrid clouds. This does not dictate the location. Even that it sounds that public cloud is hosted out there on the Internet and private cloud is located on premises, it can happen that also public cloud is hosted at a facility. This gives to companies many opportunities to decide which type of deployment model they will choose. They can choose more than one model to fulfill their requirements. If the application is need for a temporary time then the best solution might be to use a public cloud because it does not require buying additional equipment. For a permanent application the best solution will be private or hybrid cloud since they offer specific requirements on quality of service or location of data.

End User to Cloud

This is one of the most spread models. Its essence is that the end user accesses the data or applications on the cloud through Internet. Some of examples of this model are email hosting and social networking sites. The end user can access their services from any browser on any device. An important fact is that the end user is not aware of this model actually works. They only need a password other data is stored and managed in the cloud.

Enterprise to Cloud to End User

This deployment model allows enterprises to use the cloud to deliver data and services to the end user. When the end user wants to access the data in the enterprise, the enterprise accesses the cloud to retrieve the data and sent to back to the end user. The end user may be someone out of the enterprise but also someone inside it.

Risk Analysis Approach

To ensure that there all security risks are eliminated, cloud service providers are trying to implement different security mechanisms. There are two important questions regarding the security risks: How to estimate data security risk before placing data in the cloud? How to assure customers that their data is safe with the service various providers within the cloud network? With the help of a proper risk analysis approach, the cloud service providers can gain trust from their customers. Current security technology such as Secure Socket Layer (SSL), digital signatures and authentication protocols lack effective trust management. Figure 1 represents a risk analysis approach using a Trust Matrix. For the trust matrix two variables, namely Data Cost and Provider‘s History are considered. Data cost is considered as one of the variables because

the users can assign a cost to the data based on the data's criticality. Provider's History is considered as another parameter since it includes the record of the past services provided by the provider to the customers. The variable parameter _Data Location' is used to provide details about the data located in sensitive sites. A trust matrix can be generated with the variables represented along the axes. x axis represents the data cost. y axis represents the service provider's history. z axis represents the data location. The trust matrix consists of areas representing the Low Risk/ High Trust Zone and High Risk/ Low Trust Zone. A common cloud computing scenario is considered with some past statistics from the service providers. Thus the trust has been measured and can be used for all the future transactions.

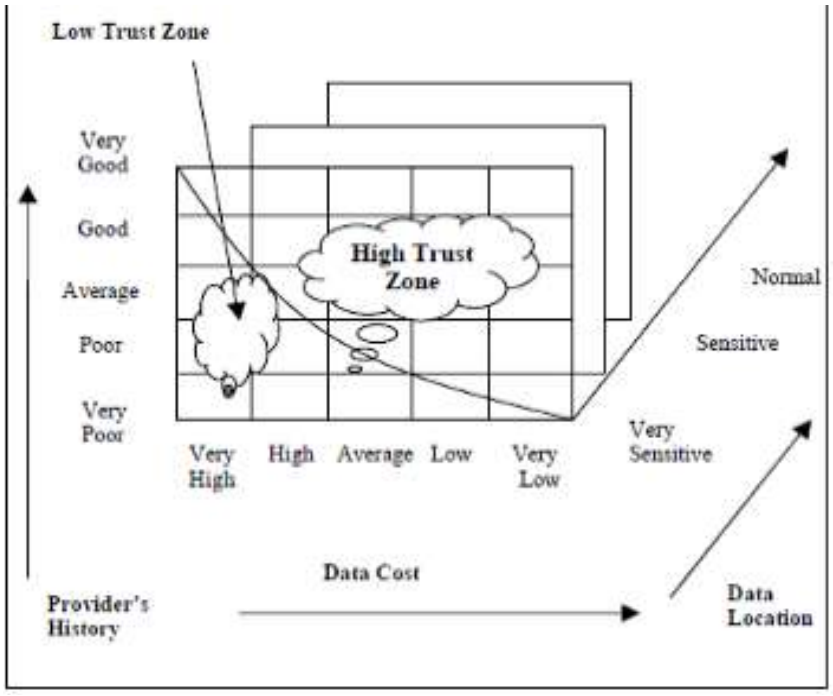

Figure 1: A trust matrix for risk analysis

CONCLUSIONS

Cloud computing has numerous benefits. Although, like all technologies, cloud computing services have many drawbacks as well, it can be seen that the benefits of cloud computing outweigh its negative aspects. Making use of cloud computing correctly and efficiently in a business can not only increase profits for a company by allowing fewer employees to work remotely, but it can also increase the productivity of a company. With the stage-driven migration approach, we can resolve all the financial, technical and social-political concerns. Deciding to invest in a cloud computing can prove extremely valuable.

REFERENCES

[1] Learn what Windows Intune can do for your organization [online], available at: http://www.microsoft.com/en-us/windows/windowsintune/explore.aspx
[2] About DMTF [online], available at: http://www.dmtf.org/about
[3] White paper: Cloud Computing: Analysing the risks involved in cloud computing environments
[4] P. Arora, R. Biyani and S.Dave , To the Cloud: Cloud Powering an Enterprise, 2011
[5] Liladhar R. Rewatkar, Ujwal A. Lanjewar, Implementation of Cloud Computing on Web Application‖, International Journal of Computer Applications, Volume 2, 2010
[6] B.Peng, B.Cui and X. Li, Implementation Issues of A Cloud Computing Platform, Department of Computer Science and Technology, IEEE 2009.
[7] P. Mell and T. Grance, The NIST Definition of Cloud Computing, National Institute of Standards and Technology, Information Technology Laboratory, Technical Report Version 15, 2009.
[8] B. Sotomayor, R. S. Montero, I. M. Llorente, and I. Foster, Virtual infrastructure management in private and hybrid clouds, IEEE Internet Computing, 13(5):14_22, September/October, 2009.
[9] Jon Oltsik, White paper: What's needed for cloud computing? 2010, p 5
[10] J. Rittinghouse, J.Ransome Cloud Computing: Implementation, Management and Security 2010, p 28
[11] Amazon Simple Storage Service (Amazon S3), [online], available at: http://aws.amazon.com/s3, retrieved 5 Jan 2009.