Risk Management Analysis and Applications of Cloud computing in business sector

Khushi Ram

Email id: **khushiram.chauhan@gmail.com**

ABSTRACT

Cloud computing offers its customer‘s reliable service at flexible prices that do not break the bank. Cloud computing can be particularly beneficial to small businesses since it can decrease the total cost of ownership for IT systems. Unfortunately, one of the major barriers to adoption of cloud services is the perception that they are inherently less secure, exposing the organization to unacceptable risk. There are standard processes for managing security risk that can help businesses make trade-off decisions, but these processes currently cannot be applied to cloud computing since the security details of cloud services are not typically available to small businesses. This lack of information leads to a lack of trust: small businesses cannot evaluate the security of cloud services. Finally, looking to the future of cloud computing, the author discussed on the role that cloud computing can play in businesses in the future.

Keywords: Cloud computing, Service, Cloud Management, Service consumer, Cloud provider, Cloud migration.

INTRODUCTION

Managing risks is of paramount importance for enabling a widespread adoption of cloud computing. Users need to understand the risks associated with the process of migrating applications and data, so that appropriate mechanisms can be taken into consideration. However, risk management in cloud computing differs from risk management in a traditional computing environment due to the unique characteristics of the cloud and the users’ dependency on the cloud service provider for risk control. 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, Cloud computing security is a broad research domain with a large number of concerns, ranging from protecting hardware and platform technologies to protecting clouds data and resource access (through different end- user devices). Although the advantages of cloud computing are tremendous, the security and privacy concerns of cloud computing have always been the focus of numerous cloud customers and impediment to its widespread adaptation by businesses and organizations. 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.

Cloud computing has gained considerable attention in the scientific community. Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort. This definition describes cloud computing as having five characteristics i.e., on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. Although there are many benefits to adopting cloud computing, there are also significant barriers to adoption. One of the most significant barriers to adoption is security. As cloud computing represents a relatively new computing paradigm, therefore the most important concern is its security from both the perspective of cloud customer and Cloud Service Provider (CSP).

Migrating critical applications and sensitive data to cloud environment is of great concern for organizations that are moving beyond their data centers. To mitigate these concerns, a CSP must ensure that customers will continue to have the same security and privacy controls over their applications and services and provide evidence to customers that their organization are secure and they can meet their service level agreements. Since the emergence of cloud computing in 2006, a lot of review papers based on cloud computing are available in the current literature but to date no systematic review of cloud computing risks has been published. Therefore, the primary goal of this research is to systematically select and review published research work and provide an overview of risk analysis, risk severity and impact of these risks on cloud users and providers.

LITERATURE STUDY

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.

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.

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.

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.

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.

APPLICATIONS OF CLOUD COMPUTING IN BUSINESS SECTOR

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.

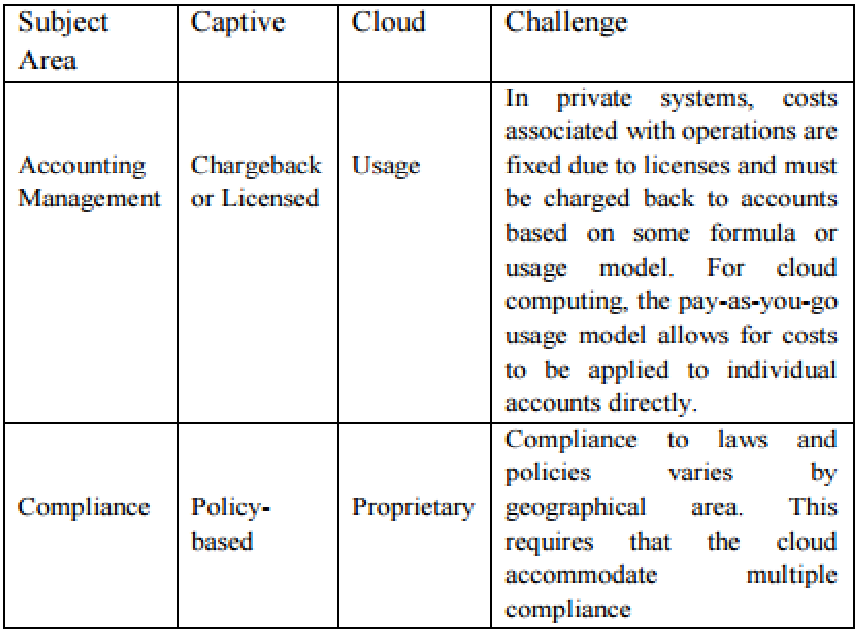
Creating new business value

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

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

It is clear that the security issue has played the most important role in hindering Cloud computing. Without doubt, putting your data, running your software at someone else's hard disk using someone else's CPU appears daunting to many. Well-known security issues such as data loss, phishing, botnet (running remotely on a collection of machines) pose serious threats to organization's data and software. Moreover, the multi-tenancy model and the pooled computing resources in cloud computing has introduced new security challenges [6] that require novel techniques to tackle with. For example, hackers are planning to use Cloud to organize botnet as Cloud often provides more reliable infrastructure services at a relatively cheaper price for them to start an attack.

As with any technology, such benefits are partly offset by the existence of risks, and in particular for cloud computing, security tops the list of concerns for most organizations. Risk-based security analyses are a widely-adopted method for making security decisions and are required for federal systems covered by FISMA and health-care related systems covered by HIPAA. A risk-based analysis of cloud services would allow a small business to make cost-benefit decisions about whether to deploy cloud services since they explicitly weigh the impact of potential security problems against the cost of mitigating those problems. Processes for managing security risk have been developed by a number of organizations, but these processes are of limited applicability in cloud computing, since cloud vendors do not supply risk information about their services. One risk analysis process is the Risk Management Framework (RMF) which is outlined in detail in NIST's documentation and involves understanding the impact of a loss of Confidentiality, Integrity, or Availability (CIA) to an organization's data or systems. The impact of such a loss is categorized as low, moderate, or high, depending on the reputation, financial, and human costs of an event. Furthermore, the cost savings of cloud computing can be offset by the level of risk it imposes. Therefore, a small business's cost/benefit analysis should include a risk analysis of those systems before moving the organization's data to them. 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.

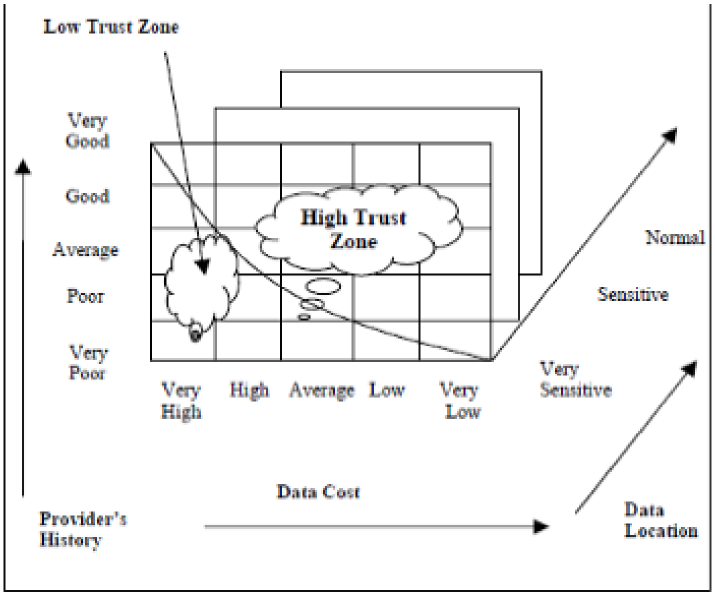


Figure 1: A trust matrix for risk analysis

CONCLUSIONS

Cloud computing has several 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 output 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.

This paper studied about both the value and the vulnerabilities of the shift to cloud computing and argues for a new practice in cloud business arrangements: the Security Risk Agreement. Such agreements will provide both parties with a clear understanding of their roles and accountabilities to one-another.

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.

[12] National Institute of Standards and Technology. 2010. Guide for applying the risk management framework to federal information systems (SP 800-37).

[13] ObReiman. 2009. Kernel vulnerability affects EC2: NULL pointer dereference. AWS Developer Forums https://forums.aws.amazon.com/message.jspa?messageID=142144.

[14] Saaty T. L. Decision making with dependence and feedback: The analytic network process. Pittsburgh: RWS Publications, 1996.

[15] Saaty T. L. The analytic hierarchy process. New York: McGraw Hill Publications. 1980.