STUDY OF BUSINESS RISK MODEL IN CLOUD COMPUTING

Vibha Sahu[1], Dr. S.M. Ghosh[2], Praveen Kumar Shrivastava[3]

[1, 3]Ph.D Scholar, Dr.C.V.Raman University, Kargi Road Kota Bilaspur, (India)

[2]Associate.Professor, Rungta College of engineering &Technology Bhilai C.G. (India)

ABSTRACT

Cloud computing is a hopeful technology for development of large-scale, on-demand, flexible computing infrastructures. The trend of adopting this technology by the businesses automatically introduced new risk on top of existing risk. Study of cloud business Risk purpose is to guide IT managers and decision makers regarding what to look for and things to consider when making a business decision about cloud. The Business Risks Framework reviews and illustrates the five most important business factors mentioned here. The simulations and process provided here are small illustrations about how to evaluate cloud availability and costs. The qualitative aspect of this research is to assist IT managers in coping with the uncertainties of IT transformation and the business decision of adopting cloud technology.

Keywords: Cloud Computıng,Cloud Securıty,Cloud Securıty Rısk Model

I. INTRODUCTİON

Cloud computing is currently one the most valued IT innovations. The research focuses on helping IT managers in their ongoing risk tradeoff efforts, which must always balance the demands of the business, constant regulatory changes that must be met, and escalating security threats. As cloud computing becomes more pervasive, many corporations are considering moving mission-critical workloads to cloud computing offerings. However, hesitation and barriers to adoption persist due to concerns about security, compliance, and business risks, as well as the lack of a functional model to rationalize and quantify IT risks in cloud computing services. The purpose of this research is to bring clarity and to create a better understanding of the security, business, and compliance risks associated with cloud computing, and to align perceived risks with actual risks. The goal of this research is to create a model that can guide IT professionals in the understanding of security, compliance, and business risks associated with cloud offerings, and tradeoffs that could mitigate these risks. Most IT companies planning to the cloud computing prototype. we have seen a rapid evolution of a cloud computing security discipline, with ongoing efforts to handle with the individual requirements and capabilities regarding privacy and security issue. Clouds have created new surfaces for attacks.

II. SECURITY CONCERN

Some security concerns are listed and discussed below:

2.1 Cost Factor

Cost is one of the main factors that experts agreed on its positive effect for lowering business risks. The experts seemed to have faith on the significant benefits that the cloud model brings to businesses. They highlighted

their own experiences building clouds for innovative model associated with cloud computing. As discussed earlier, this cloud model reduces the need for large capital investment, reduces operational cost, and provides payment flexibility since pay only for what you consume. The skills and training required to maintain cloud VMs is significantly lower than the expertise and necessary to support traditional IT. This point has been supported not only by the experts consulted but in many other sources also. The flexibility of payment based on paying for usage is evident simply by visiting any of the cloud provider websites like Amazon, cloudsigma, Gigenet, and Rackspace. But all clouds providers are different, there is no standard unit of measurement for VMs. Some clouds like RackSpace and GoGrid use RAM as the basic unit of measurement, while others use CPU units and others have invented their own unit of measurement. there is so much confusion about cloud costs and which cloud to use. First, we discuss how to estimate cloud cost. The fastest way is to use the cost estimate tool from cloud provider. After that you probably want to compare prices with other cloud services to ensure you are getting the best price. there are many open source cloud calculators already available. the research findings were not surprising, but instead very consistent with expectations of workloads with variable or "bursty" demand pattern. The "bursty" pattern can be a collection of unpredictable peaks that result, for example, from flash crowds responding to an advertising campaign, or a special sales offer on eCommerce website, or any activity on a social networking site. The "bursty" pattern can also be created by predictable peaks caused by differences in demands due to time-offday, day-of-the-week, or cyclical patterns like tax season. we can see that predictable peaks for time-of-day variations like those experienced by banks usually have a peak-to-average ratio (PAR) of about two or three.When a burst in traffic comes we can quickly deploy as many VMs as we need to support the volume. The advantage of the cloud is not just the low cost per VM, but the automation scripts that enable "bursty" workloads to quickly deploy, in a matter of minutes, thousands of VMs to handle very high volumes.

some of the key cost advantages of cloud over traditional IT are-

2.1.1 Power

The cost of electricity is becoming a significant cost of running a data center. This is why new cloud data centers are located in areas where the cost of electricity is lower, and where it can utilize water sources or air to minimize cooling costs. Because of their large consumption of power, clouds are able to negotiate wholesale block prices for electricity at much lower cost than smaller. most cloud data centers operate with minimal lighting. Some clouds use mega data center providers turn their lights off.

2.1.2 Operations and Labor Cost

Cloud providers have the advantage that data centers are heavily automated and one operator is able to handle thousands of computers. Contrast this with traditional IT, where one system administrator is usually responsible for 150 servers or perhaps less, and we can easily recognize a significant advantage for cloud environments. The combination of high automation and substantial number of servers per operator in clouds results in significantly lower costs for labor and operations.

2.1.3 Buying Power

When it comes to buying power the big cloud providers have tremendous Influence. For example, the top clouds (Google, Apple, Amazon, Microsoft, eBay) consumed five percent of the entire worldwide x86 spending in 2010. With this kind of buying power, discounts are significant. Some suppliers provide parts at minimum profit margins because the volumes are very high.

2.1.4 Commoditized Hardware

Another aspect that provides great advantage to cloud providers is that most clouds are built with "white boxes." The term white box means the computer is assembled with parts provided by independent vendors. The cloud provider becomes the assembler of the final computer, which is built from parts representing the lowest possible cost of hardware.

2.1.5 High Utilization

Clouds have the advantage of being able to choose from many workloads to maintain their systems at high capacity. where lack of virtualization, no multitenancy, and a small number of instances works against optimizing workloads to maintain high utilization. Automation and virtualization technology facilitates the move of VMs to aggregate complementary workloads, which maximizes the usage of IT resources.

2.2 Efficiency

The main motivation to move to a cloud is to save money on capital expenditure and operational expenses, but a very close second reason is to support faster deployment of nnm,.,/applications and improve the overall agility of the enterprise. Lead times to create a data center can be very long. They include the lead times to obtain capital approval, purchase hardware, configure systems, and deploy a solution. The quality assurance verification tests for a data center can range from several weeks to several months. The scalability of clouds because of their natural elasticity is one of the aspects that mitigate cloud risks associated with efficiency, availability, and cost. Standardization and automation create enormous efficiencies for clouds through substantial reduction in configuration options, limited software images supported, and automatic movement of VMs to optimize the cloud IT resources. There are some disadvantages to standardization and automation. As, standardization limits the number of operating systems and software levels available in the cloud, resulting in a dramatic reduction on the diversity of VMs. This lack of diversity helps facilitate the penetration of viruses and other malicious software across the cloud. Automation reduces cost and complexity if done correctly, but if a mistake is made on the automation script, it can cause an incredible number of problems. Automation mistakes can spread quickly, perhaps affecting the entire cloud pod before being contained. Clouds are very efficient at performing automation workflows, and automation is a known culprit in creating IT "storms" in the clouds.

2.3 Control Factor

One of the disadvantages mentioned by CIOs and CTOs during the interview process for this research was the lack of transparency that cloud providers maintain regarding operations procedures. A good mitigation for this lack of transparency is a detailed set of requirements,expectations, and assurances described in SLA contracts with the cloud provider. Contracts can protect users by providing penalties when loss of income is caused by lack of service, but this doesn't mitigate possible lock-in risks. IT professionals are accustomed to controlling their IT resources, and it takes some time to get accustomed to new management processes and tools to manage IT resources at the VM level (IaaS), or platform level (PaaS), instead of at the physical level. After IT managers get new cloud processes in place that generate good availability at lower cost, many experts have observed that most of the resistance and concern about diminished IT control quickly fades.

2.4 Availability Factors

cloud environments, which behave very differently. Failures in the cloud are easy to recover from within a couple of minutes because of automatic scripts and instantiation of VMs. Events that are catastrophic in a

traditional data center are an everyday occurrence in the cloud environment, but with no tangible significance to the user. This is a paradox because failures are more common in clouds. Services offered by cloud providers to automate the recovery process help reduce the recovery time to only a couple of minutes. But why do clouds have more failures than traditional IT? These failures are the result of massive amounts of systems and storage running at 95 percent utilization in mega data centers. Clouds provide the illusion of "always available," despite the constant failure of systems, because of the large redundancy and automation they possess. Automation enables very fast recovery, which helps minimize the amount of time the system is down. A review of the availability equations listed bellow helps illustrate that the shorter the recovery time the better the availability, and that the more redundancy a system has the better its availability. In addition to recovery automation, a recovery strategy should also be created when moving workloads to the cloud. No cloud system is immune to a possible catastrophic event, and a disaster recovery plan is of key importance, whether a business uses clouds or traditional IT. In the case of the cloud, it is recommended that a different cloud provider be used, or at a minimum, ensure that the disaster recovery configuration is in a separate location, with different network providers and substantial redundancy. Another unique aspect of cloud computing is its ability to sustain significant denial of service (DoS) attacks. This ability is the result of the cloud's elasticity and the ample resources from which more capacity can be drawn. This capacity can be used to maintain the services until the source of the attack can be shut down. However, this capability requires automation. If cloud users don't invest in the automation and allocation of additional resources, the few standard allocated VMs can certainly tip over with the exces demand created by a DoS attack. Cloud users are not immune to DoS attacks, but instead have more resources available to them to defend against an attack. Cloud providers are using significant technology to enable early detection of DoS perpetrated on their customers. They are monitoring outliers on service requests and communicating to customers to address the attacks as well as possible. Availability is one of the factors that affect the reputation of a business. The general perspective of is that IT availability is one of the factors under the control of IT managers that can make a great impact on preserving and enhancing the reputation of a business. If availability is of great importance, the IT budget is not significant, and the solution doesn't use confidential data that requires strict regulatory compliance, hosting the solution in the cloud could provide some significant advantages over traditional IT.

2.5 Legal Complexity

From a legal perspective there are many issues with cloud contracts. These issues include unclear and restrictive laws, frequent trans-border operations, and lack of precedents to guide litigation. Most standard cloud contracts are based on "as is" warranties, which means the service is provided with no promises of any kind. There is no guarantee that the cloud service will be appropriate or that it will meet the customer's expectations. Not all cloud providers offer SLAs, and those that specify assurances are usually based on limited obligation and availability. This is measured by the cloud portal uptime, instead of by the customer's service reliability and actual performance. Also, lack of standards is a problem for cloud contracts because there is no unified way to offer cloud services and there are no standardized benchmarks to help quantify the quality of service. Trans-border data flows are common when data is resident in multiple countries and cloud service and customer are located in different countries. Data flow that crosses a country's borders is subject to the jurisdiction of multiple countries, and can create costly litigation fees because of unclear and contradictory law. Trans-border data flow has many potential legal issues that can arise because of inappropriate handling of data, disparities between IT

regulations depending on country, and ambiguity about obligations. T managers should fully negotiate cloud contracts to ensure the agreements satisfy the needs of the business and avoid ambiguity about roles, responsibilities, and processes. The process of negotiating a contract should include specifications about the location of the data at all times, security and performance assurances, and country jurisdiction and litigation processing in the event of a dispute.

III. SOLUTION FOR CLOUD BUSSINES RISK MODEL

As we discussed earlier Cloud BUSINES risk model is based on- (1) cost (2)Efficiency (3)Control (4) Availability (5) legal complexity.

This solution strategy can assist IT managers in coping with the uncertainties of IT transformation and the business decision of adopting cloud technology.

3.1 Solution for Cost

a) Create long term strategy- Move to a cloud should instead be viewed as a long-term business transformation. A long-term plan can help identify workloads that are expensive for the corporation to maintain in-house, and cause them to evaluate a lower-cost alternative. A plan can help prioritize the workloads that are best suited for clouds, and accelerate that transformation. This plan should perform a deep analysis on the security and cost tradeoffs when making the decision to move workloads to a cloud.

b) Estimate cloud migration cost – Moving a workload to a cloud can be a great opportunity to lower capital expenditure (capex) and operating expense (opex). However, not all workloads move easily to a distributed and virtualized environment. Some modifications might be necessary to achieve a successful cloud

c) Calculate current cost- Before moving to any cloud it is important to know the cost of your current traditional IT. Analyze which applications; services are the main cost drivers.

d) Compare cloud providers- Before committing to a cloud provider make sure to compare prices across many clouds because the price differences between clouds are significant. Since clouds tend to optimize their configurations by different workloads, types of VMs, and network configurations, every cloud service is different.

e) Automate – To achieve the lowest possible cost in clouds, you need to make sure to automate your workloads to use the optimal amount of VMs for your workloads, and remove VMs you are not going to need. Keeping VMs running unnecessarily is a waste of money in clouds, because you pay for what you use.

3.2 Solutions for Efficiency

a) Optimize your cloud solution – There are many cloud management tools that are able to monitor and optimize workloads hosted on virtual environments, and that can greatly facilitate the management of VMs. Cloud elasticity is fantastic at providing the capacity necessary on demand, but keep in mind that the requests for additional resources should be managed to optimize your business and not necessarily the IT service.

b) Use the right tool for your workload - Each cloud solutions has different IT requirements and it is important to use the right tool for the job. Many cloud solutions use new programming languages like Python, PHP, and Ruby on Rails.These types of programming and scripting languages require management and development tools designed to be used with them, and extensions that facilitate the usage of cloud APIs and services

c) Create a Disaster Recovery Plan – It is out of your control to prevent “cloud storms,” and since sooner or later there will be some type of unfortunate mistake that could affect your solutions, it is best to prepare for a disaster.

A disaster recovery plan should include data centers from multiple cloud providers. However, if a single cloud provider is used, a minimu Configuration should include two data centers in different locations, with significant network redundancy, including at least two different network suppliers. Clouds provide good availability, but still can't be assured 100 percent, and business solutions running on clouds still need a disaster recovery plan.

d) Patch Often – To mitigate the lack of diversity of operating systems and middleware versions and types, it is recommended that users and cloud providers follow a process to continuously update software to the latest level. Stay informed.On vulnerability reports and make sure your cloud provider uses the latest operating system versions and patches.

e) Reconfigure and redesign for the clouds – Moving workloads "as is" sometimes is not the most effective way to utilized cloud resources. For a workload to achieve the maximum economic benefit and scale horizontally automatically, it needs to be redesigned with cloud scaling in mind. Workloads need to be adjusted to interface with the cloud APIs and web services to automatically instantiate VMs.When required, delete unnecessary resources to avoid needless charges, and achieve an effective load balance across VMs. Without effective configuration and adoption of the cloud provider APIs and services for optimization, solutions won't run as efficiently as possible.

3.3 Solution for Control

a) Demand Transparency – you must know how your data and workloads will be managed. To mitigate this concern, request inspection of the Physical data center facility, and audit the IT processes associated with your workloads before signing a long-term contract with the cloud provider.

b) Create Isolation Layer – Avoid cloud lock-in by keeping customization related to cloud APIs and automation scripts encapsulated in a few modules to facilitate movement to other clouds if necessary.

c) Educate IT Managers about Cloud Benefits – If IT managers understand the reasons and business benefits for moving to the cloud, less pushback and resistance can be expected from IT personnel.

d) Control by the Numbers – The control points on IaaS and PaaS moves from the physical layer to the VM layer. Appropriate cloud tools should be utilized to ensure cloud services are optimized. The more data you collect, the better analysis you can make and more control you can exert on the utilization of the VMs.

e) Create Clear Contractual Agreements – If you plan to run a considerable amount of work in the cloud, it is advisable to create a contract or SLA stating your expectations and requirements. Don't accept the standard contract you get on the web when you first register with a credit card. Those contracts are written for the benefit of cloud providers, and usually include indemnification clauses.

3.4 Solution for Availability

3.4.1 Automate Recovery Process

To benefit from higher availability in the clouds an investment must be made in automating the recovery process. Moving a workload to a cloud without investing in automating the recovery process would not provide any availability benefits, and could in some instances provide inferior availability.

3.4.2 Monitor for Outliers

Be proactive in defending against DoS attacks. If request loads are substantially higher than expected, consult your cloud provider to validate network activity and the origin of possible attacks. Cloud providers constantly monitor the network volumes for possible DoS attacks and can help block attacks coming from external servers, or within the same cloud.

3.4.3 Create a Disaster Recovery Plan

Clouds don't protect against catastrophic events and it is necessary to build a solid disaster recovery plan using data centers in different locations, with plenty of redundancy.

3.4.4 Calculate Availability

It is important to understand the current availability as well as the possible future availability with new IT configurations. Before moving to the cloud constructs a realistic view about the current probability of system failure and overall availability. When moving to the cloud, include in the SLAs the availability expected, and dedicate a budget to automate the recovery process. After the service is in the cloud, test the Availability by stressing the service. Simulate a DoS attack to ensure the solution will work correctly when an actual DoS attack happens.

3.5 Solution for Legal Complexity

3.5.1Negotiate Contracts

The standard cloud contract won't likely satisfy enterprise needs. It is recommended that contracts be fully negotiated to add the assurances, desired operational processes, and the specific country that has jurisdiction in case of a dispute.

3.5.2 Avoid Ambiguity

Define concepts carefully, in a way that can be measured or quantified consistently to avoid ambiguities and misconceptions. Since there are no standard benchmarks and precedents to help describe important concepts.

3.5.3 Cyber Forensic Support

For court proceedings it is important to have evidence to prove our innocence or to demonstrate wrongdoing by an attacker. However, without support by the cloud provider, and the enablement of cyber forensics on the cloud services, the user might end up with insufficient evidence. Lack of support for cyber forensics is one of the key risk factors listed under the compliance framework.

3.5.6 Specify Roles and Responsibilities

Cloud systems consist of multiple layers of services, some created by the cloud provider and others provided by external vendors. Most clouds have a rich ecosystem of vendors to ensure delivery of services. To guarantee the quality expected, a mitigation strategy is to negotiate directly with the vendor providing the subservices.

3.5.7 Follow Best Practices for IT Contracts

Because of a lack of benchmarks and precedents, cloud contracts should be more specific about the expected results and services provided. However, IT contracts best practices should be feollowed to avoid common pitfalls. Because the expected trend is for prices to drop until further maturity of the cloud market, most enterprises should set flexible contract agreements that enable them to take advantage of falling prices, but also to protect themselves against unexpected price hikes.

IV. CONCLUSION AND FUTURE WORK

Cloud computing is the future of IT industries It helps the industries to get efficient use of their IT Hardware and Software resources at low cost. This paper discuss about the cloud business risk Challenges. this research illustrated the way financial benefits of the cloud can fluctuate depending on the kind of workloads. In the case of "bursty" workloads, the potential financial benefits could be significant, since substantial reduction in IT cost can be achieved by utilizing the lowest possible configuration and dynamically provisioning VMs to support

demand peaks. New cloud compliance risks related to cyber forensics, data segmentation, and data remnants are a few of the many new risks associated with clouds, and described under the Cloud Compliance Risks. Since the pace of technology is very fast in the area of cloud computing, it would be interesting to do an evaluation of cloud risks in several years to show how risk vectors, identified by this research, have changed with new technologies.

V.REFERENCES

[1]. M. S. Mimoso, "Cloud Security Alliance releases top cloud computing security threats", http://searchcloudsecurity.techtarget.com/news/1395924/Cloud-Security- Alliance-releases-top-cloud-computing-security-threats, 2010, Accessed November 4.

[2]. C. McMonigal and P. S. Levy, "Cloud Storage Usage Models and Reference Architectures", Intel Developer Forum, San Francisco, CA, 2011.

[3]. S. Marston, Z. Li, S. Bandyopadhyay, J. Zhang, et al., "Cloud computing — The business perspective ", Decision Support Systems, vol. 51, no. 1, pp. 176-189,April 2011.

[4]. Cross-VM Side Channels and Their Use to Extract Private Keys http://www.cs.unc.edu/~yinqian/papers/crossvm.pdf

[5]. Multi-Tenant Data Architecture http://msdn.microsoft.com/en-us/library/Aa479086

[6]. Cross-VM Side Channels and Their Use to Extract Private Keys http://www.cs.unc.edu/~yinqian/papers/crossvm.pdf

[7]. Security Considerations", Report No.G00210095, Gartner, March 7, 2011.

[8]. IDC, "Data Center and Cloud Computing Survey", Report, January 2010.

[9]. Perfecting the unknown: Cloud Computing http://www.mysanantonio.com/business/article/Perfecting-the-Unknown-Cloud-Computing-4157844.php

[10]. Pirate Bay Ditches Servers and Switches to the Cloud http://news.cnet.com/8301-1023_3-57534707-93/pirate-bay-ditches-servers-and-switches-to-the-cloud/

[11]. Insecure API Implementations Threaten Cloud http://www.darkreading.com/cloud-security/167901092/security/application-security/232900809/insecure-api-implementations-threaten-cloud.html