THE RISK MANAGEMENT IN CLOUD BANK IN INDIA AND THE ROLE OF CHANGING FUNCTION AND NEED OF THE BANK

[1] S.Veniswari, [2] Dr. B. Revathy
[1] Research Scholar, [2] Professor & Head
[1] Department of Commerce,
[1] Manonmaniam Sundaranar University, Abishekapatti, Tirunelveli – 12, TamilNadu.

Abstract: This paper presents issues risk management in cloud bank-based computing. The computing industry is witnessing a paradigm shift in the way computing is performed worldwide. There is a growing awareness among consumers and enterprises to access their information technology (IT) resources extensively through a "utility" model, a development broadly called "cloud computing." Today's, the boom in cloud computing has brought lots of cost, efficiency, reliability, security, policies as key challenges for the banking sector to provide better service for their customer. In this talk we consider the issues that need to be addressed first before making the move to the cloud. Testing and researching cloud environment and are intensely interested in seeing what cloud concepts might accomplish for their banking and finance industry. In addition, this paper takes a look to some open issues related to cloud platform e.g. deployment, elasticity and mobility.

Index Terms **- Banking Sector, Cloud-based Computing, Finance industry, Issues, Utility model.**

I. INTRODUCTION

Cloud computing has experienced a fast growth during the last years, and it is expected to keep developing more and more. Cloud services will be profitable in business application, which will transform services in cloud-based services. This change is needed especially for application like ERP (enterprise resource planning) or CRM (customer relationship management). Banks are an important segment of business area that cloud computing is targeting in the next few years. Due to this type of business needs, cloud services must be similar with a "silver bullet". There are many advantages that cloud provides for banks as customers. First of all, cost savings, using cloud-servers instead of personal servers, will save a lot of money. Moreover, cloud provides: usage-based billing, business continuity, business agility, green IT. Thus, nowadays cloud computing services has some disadvantages that stops banks to adopt the cloud, such as security, confidentiality of the data, and also quality of services.
The main contribution of the present research is an empirical study of the risk and control analysis in relation to the prospective adoption of public cloud services by a sample of Swiss companies. The participants in the study are professionals who attended a course in Business Risk Management (Gestion des Risquesd'Entreprise) at the Geneva School of Business Administration (Haute Ecole de Gestion de Genève). They worked in groups and submitted five reports each dealing with a specific company. The purpose of this study is to establish whether cloud computing risks are well understood and whether proper mitigation practices have been studied and proposed. In short, we find a sufficient degree of risk awareness and the ability to focus specifically on those risks and controls that are relevant to the particular IT function to be migrated to the cloud. The recommendations of whether to adopt cloud services depend on the company's size, technological expertise, and corporate culture but not on the type of process or data to be migrated. To our knowledge, this is the first study of this kind to be conducted in Switzerland. Nevertheless, the inferences we make should be viewed in light of the small sample size (only five reports) and underline the need for broader and more detailed studies in the future.
1.1 What is cloud computing The US National Institute of Standards and Technology (NIST) defines cloud computing 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" (Mell & Grance, 2011). According to NIST, the cloud computing model comprises five essential characteristics, three service models and four deployment models (Mell &Grance, 2011).

II REVIEW OF THE STUDY

The three service models are Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) (Mell &Grance, 2011). IaaS denotes resources, such as processing, storage, networks, and other fundamentals, on which the customer can deploy operating systems and applications. Examples of such cloud solutions include Amazon's Elastic Compute Cloud (EC2), GoGrid's Cloud Servers, and Joyent (Sultan, 2011). PaaS builds on top of IaaS and offers an operating platform enabling the deployment of customer-created or existing applications that use the programming tools and libraries of the provider. Products in this category include Google App Engine, Microsoft Azure, Amazon Web Services (AWS) and Force.com (by Salesforce.com) (Sultan, 2011).

SaaS builds on top of IaaS and PaaS and provides a range of applications, such as word processing, spreadsheets, customer relationship management (CRM), HR management, enterprise resource planning (ERP) systems, etc., running on cloud infrastructure. SaaS has the lowest degree of customization with only limited control over some of the applications' configuration settings for off-shelf solutions such as Yahoo! Mail, Google Apps, Salesforce.com, WebEx, and Microsoft Office Live (Sultan, 2011). But users can also customize the products by developing specific components based on Application Program Interfaces (APIs) made available by cloud providers (Sultan, 2010). As a rule of thumb, the Cloud Security Alliance (CSA) (2011) explains that "the lower down the stack [IaaS, PaaS, SaaS] the cloud service provider stops, the more security capabilities and management consumers are responsible for implementing and managing themselves." In other words, in an IaaS architecture, the consumer is responsible for the security of the software deployed on it. At the other end of the spectrum, in a SaaS solution, the provider ensures the security of the applications they offer.

In terms of deployment, NIST distinguishes between private clouds, public clouds, community clouds and hybrid clouds (Mell &Grance, 2011). In private clouds, the cloud infrastructure is provided only for the use of a single organization. Private clouds give organizations more control over security, transparency and compliance but require substantial capital and operational expenditures and a highly proficient IT team (Carroll, van der Merwe, &Kotzé, 2011).

Heiser and Nicolett (2008) add that a single storage device may contain data and logging from multiple customers which poses challenges to understanding the access and deletion of files, and further from a privacy point of view. The data may also be located in different, often changing, data centers. Moreover, conducting forensic investigation even on an enterprise's own infrastructure is difficult, time-consuming and expensive.

As Sultan (2011) points out, Salesforce.com was unavailable for 6 h in February 2008, followed by Amazon's S3 and EC2 clouds only several days later. Amazon's S3 was unavailable again for 8 h later that year. The list of similar accidents extends to more recent years as well with the multi-day failure of Amazon's EC2 in April 2011. As ENISA's (2009a) survey shows, 28 out of 66 SMEs consider availability of service and data as an issue of critical importance. On the other hand, the availability of service in many cases, and in particular with respect to SMEs, surpasses the availability that an in-house IT department can maintain.

METHODOLOGY

- Five BBA Cloud Working Group sessions were held where the roadmap prepared by Pin sent Masons was considered and debated.
- The paper should be collection of report and books, journal, web site.

III RISK OF CLOUD BANKING;

As Hawser (2009) notes, cloud computing provides small and medium enterprises (SMEs) with access to software, services and infrastructure normally beyond their reach. In a survey of more than 70 SMEs conducted by the European Network and Information Security Agency (ENISA), 68.1% point to avoiding capital expenditures on hardware, software, IT support and information security as a reason for possible adoption of cloud services (European Network and Information Security Agency [ENISA], 2009a). One Stop Click's (2011) December 2010survey of more than 3200 SMEs from 16 countries reveals that 40% plan to purchase cloud services in the next three years. Cloud computing, however, presents significant risks and challenges as well. In a survey of nearly 1800 US businesses and IT professionals by the Information Systems Audit and Control Association (2010), 45% consider the risks of cloud computing as outweighing the benefits. The sections below review the main topics of concern with an emphasis on their interpretation from a management point of view. They are not ordered by severity but rather represent specialists' views regarding the major risks of cloud computing and the relevant mitigation practices.

3.1 Costs and potential risks

Transitioning from a traditional to a cloud computing environment entails switching costs that can be very high. For example, a dedicated workforce would need to be established to prepare, manage and execute the switching to the cloud, with the task of possibly replacing applications that are not compatible with the cloud providers' platform with new ones. Other switching costs include the network bandwidth needed for moving the data, any upload or download fees charged by the cloud provider,11 as well as any potential costs related to moving the data from one cloud provider to another. Booz Allen Hamilton has conducted sensitivity analysis based on multiple models of migration to the cloud, finding that the length of the cloud migration is one of the most influential factors driving economic benefits

3.2 Managing downside risks

Maximizing the benefits, while minimizing the costs and downside risks requires disciplined and comprehensive risk management. The tools that banks could use for this include conducting due diligence when selecting the provider, carefully crafting service level agreements and using severe penalty clauses covering any potential accidents, performing ongoing monitoring and audits, and developing and maintaining contingency plans for terminating relationships, etc. The primary obstacle to effectively using these tools is the size and power of the cloud computing providers. It would be very hard for a small community bank to effectively negotiate with or audit a behemoth like Amazon or Google, and even large banks can find it challenging, as the ENISA study has shown. One risk management strategy that has worked in other industries has been quasi-integration (minority control, strategic alliances), but this is likely not feasible even for the largest banks, again due to the sheer size of cloud computing providers. An alternative for banks would be setting up a community cloud for financial institutions, or at least coming to an agreement on universal requirements for cloud computing providers

3.2.1 Deployment Models

- Private cloud
- Community cloud
- Public cloud

- Hybrid cloud

3.2.2 Essential Characteristics

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

3.2.3 Service Models

- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

3.2.4 Private Cloud

- Provisioned for single organization
- May exist on or off site
- May be managed by organization or outsourced

3.2.5 Community Cloud

- Provisioned for exclusive use by a specific community
- May be managed by one or more of the community organizations
- May be managed by community organization or outsourced

3.2.6 Public Cloud

- Provisioned for general public
- Exists on the premise of the cloud provider
- May be owned, managed & operated by a business, academic or government organization or a combination

3.2.7 Hybrid Cloud

- Combination of two or more distinct cloud infrastructures
- Combines characteristics of private, public & community clouds
-

3.3 BUSINESS USE OF CLOUD SERVICES

3.3.1 Financial Savings

- Equipment
- Personnel
- Infrastructure
- Space & utilities
- Reduced obsolescence
- Reduced capital expenditures

3.3.2 Increased Flexibility

- Rapid deployment
- Ability to add or reduce capacity
- On-demand provisioning
- Disaster recovery
- Business expansion (across town or across the globe)

3.3.3 Streamlined business development

- Focus on innovation & research
- Reduced effort on management, maintenance & support
- Simplified entry into or exiting from business initiatives
- Increased access to technical expertise
- .

3.4 CLOUD SERVICE RISKS

3.4.1 Security

- Physical access to infrastructure, systems & data
- Physical location of systems, data
- Logical access to the network, OS, applications & databases
- Network & data segregation

3.4.2 Availability

- Cloud provider service interruptions
- Data location/availability for restoration
- Network/connectivity interruptions
- Failure of the provider to adhere to SLAs
- Service provider disaster recovery

3.4.3 Processing Integrity

- Adherence to change management procedures
- Incident management
- Failure of the provider to adhere to SLAs

- Timeliness
- Accuracy
- Authorization
- Completeness

3.4.4 Confidentiality

- Comingling of data & other assets
- Unauthorized access to sensitive

3.4.5 Privacy

- International laws affecting service provider location
- Regulatory compliance/legal liability
- Breach & incident management

IV FINDINGS

• The need to protect confidential business, government, or regulatory data
• Cloud service models with multiple tenants sharing the same infrastructure
• Data mobility and legal issues relative to such government rules as the EU Data Privacy Directive
• Lack of standards about how cloud service providers securely recycle disk space and erase existing data
• Auditing, reporting, and compliance concerns
• Loss of visibility to key security and operational intelligence that no longer is available to feed enterprise IT security intelligence and risk management
The need to protect confidential business, government, or regulatory data • Cloud service models with multiple tenants sharing the same infrastructure
Data mobility and legal issues relative to such government rules as the EU Data Privacy Directive
• Lack of standards about how cloud service providers securely recycle disk space and erase existing data
• Auditing, reporting, and compliance concerns
• Loss of visibility to key security and operational intelligence that no longer is available to feed enterprise IT security intelligence and risk management
• A new type of insider who does not even work for your company, but may have control and visibility into your data.

V SUGGESTIONS

a. The Cloud promises to revolutionize not just the Government but also industry as a whole. Further, the Cloud presents tremendous opportunities to fast track the healthcare and education sector in India. However, it will require careful development of a national Cloud strategy to ensure that maximum benefits of the Cloud accrue to the nation while minimizing the risks.
b. In essence, the Government needs to play a pivotal role in ensuring that Indian entities can take advantage of the Cloud revolution for economic growth without being encumbered by the challenges and risks arising from the Cloud. The Government needs to work on dual goals of protecting interests of Indian entities in relation to risks from Cloud adoption and accelerating the adoption of Cloud in India.
c. This will be possible only with cooperation between various government agencies and departments anchored by key ministries. The NTP-2012 also plans "to exploit individual strengths of organizations under Dot/DIT to their mutual benefit for ensuring these organizations to effectively flourish in the competitive telecom market while adequately supporting the security needs of the country."

VI CONCLUSIONS

Cloud bank computing presents some important risks which should be assessed by any enterprise considering engagement in this area. Our main contribution consists of an empirical study of a sample of Swiss companies which is aimed at analyzing the understanding of the risks that public cloud services present and how they can be managed. Even though the sample size is very limited, we can see sufficient awareness of both the risks and the management solutions. The authors of the reports have consulted the large volume of literature pertaining to cloud computing risks with some of the reports referring to the Swiss regulatory context as well. There is also a degree of originality in the reports as they have considered the risks in the specific context of the concerned companies and according to their needs and capabilities. The flexibility and cost-efficiency of the cloud should be more attractive to SMEs as compared to large companies. On the other hand, there may still be a certain level of mistrust in SMEs regarding the cloud as they lack sufficient expertise and risk management skills. Indeed, the reports suggest that large companies are better prepared toward the adoption of cloud services. Nevertheless, as this paper has shown, understanding, assessment and mitigation of the risks are vital when it comes to cloud computing. Once these steps have been properly addressed, where necessary with the help of external advice, the cloud may not look like such a dangerous place even for SMEs. Finally, we stress again on the limited nature of our study whose purpose was to serve as an introductory exploration of the risk analysis with regard to prospective adoption of cloud services. Our findings cannot be extrapolated to all Swiss companies, but allow us to devise a stricter and more rigorous methodology for further studies based on interviews, questionnaires or quantitative surveys.

REFERENCES

[1] Biswas, S. (2011b, January 26). Computing without borders – What works, what doesn't [Web log post]. Retrieved from (accessed on: January 25, 2012).

[2] Carroll, M., van der Merwe, A., &Kotzé, P. (2011, August). Secure cloud computing: Benefits, risks and controls
[3] Cloud Security Alliance. (2010). Top threats to cloud computing v1.0. Retrieved from (accessed on: December 12, 2011).
[4] Cloud Security Alliance. (2011). Security guidance for critical areas of focus in cloud computing 6, 2012).
[5] Cunningham, P. (2009, June). Three cloud computing risks to consider. Information Security Magazine. Retrieved (accessed on: December 5, 2011).
[6] Douglas, M., and A. Wildavsky (1983). Risk and culture: An essay on the selection of technological and environmental dangers. Berkeley; Los Angeles: Univ. of California Press.
[7] www.cloud bank.com.in