CLOUD RISK MANAGEMENT

P. Vidhyalakshmi*

ABSTRACT

Cloud computing is a highly automated efficient data center providing service-based access of IT resources such as computing, storage, network, platform, application and its related security. Cost cut and scalability of the cloud are the main reasons that attract the IT managers of any organization towards the cloud scenario while data sensitivity is the other reason that prevents them from migrating to the cloud scenario. The expectations for the consumer from cloud computing are availability of data irrespective of the consumer location, data security, high reliability and cost effectiveness. Any organization opting for cloud should have features like network dependency, IT skills, data import / export and handling risk from multi-tenancy. Cloud computing will undoubtedly benefit the organization if its providers are chosen with care. Cloud providers still have to prove that they can protect the data. To have a successful deployment or the migration to the cloud the main points to be considered are licensing, processing requirements and memory locks, bandwidth requirements, communication protocol and data security. This paper deals with the different risks involved in the cloud implementation. The solutions for data security, intrusion detection in the cloud, cloud auditing and cloud disaster recovery techniques are also discussed.

Keywords: *Virtualization, Hypervisor, Cloud Security Alliance (CSA), Cloud Control Matrix (CCM), potential risks, Service Level Agreement (SLA)*

***** Ansal Institute of Technology, Gurgaon.

INTRODUCTION

Cloud Computing is growing in popularity, providing businesses with more agility, efficiency and cost saving[1]. This comes into an organization when they want to add or increases their capability with the help of IT but without investing in infrastructure, training new personnel or buying new software. Infrastructure, applications and software could be used in cloud environment as pay-per-use method. Cloud computing combines the known technology such as virtualization in an ingenious way to provide IT services. Advent of cloud computing has changed the landscape of Information and Technology (IT). Cloud provides solution for the problems caused by exponential growth in volumes of data, device proliferation and the changes demanded by the fast paced business and technology. The full advantage of the cloud is taken by IT because of private, public or hybrid cloud model of Software as a Service (SaaS), Platform as a Service (PaaS) or Infrastructure as a Service (IaaS)[2].

Virtualization is the basis of IaaS cloud computing, which serves the business better with the help of efficient resources utilization by pooling and sharing IT resources. PaaS and SaaS are built on top of the supporting IaaS infrastructure. Virtualization saves costs but increase in virtualization brings in increased security risks. Consumers should be prepared for the cloud outages[1], which refer to the situation when the cloud services fail. The consumers could lose access to the data and they could not use the processing capabilities provided by the cloud. This will have a rippling negative effect on service to their customers. The potential risks of the cloud computing and the possible risk management measures are discussed in the succeeding sections.

CLOUD COMPUTING CHARACTERISTICS

US National Institute of Technology has laid out the essential characteristic of cloud computing as follows[3]:

On-Demand Self-Service – User can add or manage his services without any human intervention. Provisioning and de-provisioning of services occur automatically at the provider end.

Ubiquitous Network Access – Cloud services are accessed with the help of internet using standard mechanism and protocol and have to be available all the time. Denial of service due to network problem may result in business loss.

Resource Pooling – Computing resources that are used to provide cloud services are realized using homogenous infrastructure that's shared between all service users.

Rapid Elasticity – Resources should be scaled up and down rapidly and elastically.

Measures Services – Resources / services usage has to be metered, supporting optimization of resource usage, providing usage reports and should have pay-as-you-go business model[6].

Migration to the cloud has to be done carefully to enjoy the full benefits of the cloud. Moving an application, development or storage into cloud means a new paradigm of IT and security management. It moves the data from the purview of security analyst and network perimeter. A clear vision of how the data moves outside the organization, where it is stored and who has access to it has to be observed carefully. The organization should study their infrastructure and adjust their working and practices according to the cloud. This may increase the bandwidth requirement due to increased Internet connectivity. Key application will be reached through the network connection outside the system. Testing the network characteristics of these new connections is very important[8]. Some organizations may adopt virtual servers as a means of saving on hardware, increasing uptime or both. Migration of the virtual infrastructure to the cloud may have significant impact on the application performance for these organizations. As the Internet traffic increases with the cloud computing, load on the security devices like firewalls, VPN concentrators and IDS/IPS appliances also increases.

POTENTIAL RISKS IN CLOUD COMPUTING

Based on the deployment method the cloud could be categorized as private cloud, public cloud, community cloud and hybrid cloud[5]. Private cloud is maintained by the single organization. This is mostly sought by big organization and is at the least risk. A group of companies can build their own member-only cloud called community cloud. The clouds that are run by Microsoft, Amazon and Google are the public clouds where any one can place the data, use the resources or use the platform. These are high-risk clouds because of multi-tenancy[4].

Some of the potential risk factors are data security, reliability, down time, loss of control on data, cost and time to migrate to cloud, maturity of cloud market, lack of industry standard, resistance by IT managers and staff, integration with the existing system and service level agreements and guarantees. Of all these, security is considered as the most important substantial roadblock for cloud computing uptake. Enterprise security has to be viewed in terms of cloud. Most of the executives are concerned about the features, facility and functionality of the cloud services. The main point of concern is the control and integration of data (i.e.) the ability to migrate one's data to and from the cloud providers such as salesforce.com. The lack of clear vision about the location of data is also a concern for some

executives. These concern increases if they prefer to use services of cloud providers maintained by foreign firms.

Hypervisor security is critical and overlooked. Hypervisor is also called as virtual machine manager, is a program that allows multiple operating system to share single hardware host. It actually controls the host processor and resources by allocating what is needed to each operating system and also make sure that the guest operating systems (i.e. virtual machines) do not disrupt each other. Security problems may become worse if employees access the back office data with the help of mobile devices[8]. Mobile clouds will help to resolve these problems as they allow IT admin to centrally control security.

CLOUD SECURITY ALLIANCE

Cloud Security Alliance (CSA) is a non-profit organization that helps to formulate rules for the best practices to be followed while providing security in cloud computing. It also provides security guidance to the companies that are implementing cloud computing and also helps the vendors to adopt the security measures in their software delivery models. They also provide toolkits to assess the private and public cloud against the industry-established security rules. Cloud Control Matrix (CCM), a part of toolkit is a set of security controls created by CSA, which will help the consumers to assess the risks associated with the cloud service provider. CCM is aligned with different areas as such as data center operations, application security, access management, ISO 27001 / 27002, different industry standards and regulations that an enterprise should follow. Many cloud computing security requirements are solved by using cryptographic methods. Key management is the main point to be focused on using these methods. To ensure guarantee of the service, Service Level Agreement (SLA) will be done between the customer and the provider. This may vary from business to business. This includes details about the requirement, the agreed level and quality of service, security measures adopted and the service rates.

Risk Management Options

Do not entrust cloud for time sensitive data[8] Some applications are so time sensitive that their use cannot tolerate any interruption. Before venturing into the cloud, the effect of service interruption on company's operations should be assessed.

Encrypt and send the data. If data has to be sent to the cloud, then they can be sent after encryption with higher bit keys for extra safety which can be decrypted after receiving from the cloud. Key management has to be done at the customer end. This may invite extra processing time at the customer end so it has to be used only for critical data.

Digital signature for documents. Document tampering can be found out if they have been sent to the cloud with digital signature. If tenders and quotations are to be stored in the cloud, this may give a clue about tempering of data.

Conduct appropriate due diligence of the cloud provider. The customer should have clear understanding of the capabilities and stability of the potential cloud service provider. CCM will help them in this regard apart from this they can also take details from user group forum posting on web.

Document the cloud providers' commitment to provide uninterrupted services. Service Level Agreement (SLA) has the terms of contract about the actual commitment made with respect to the service and service levels between the customer and the vendor.

Prepare for the inevitable service interruption. Use backup or alternate services. Emergency plan should be ready to ensure smooth working of the company operation in case of cloud services interruption. Redundancy storage of critical data has to be made with different providers at different locations.

Understand the relevant clauses in the contract. SLAs should be well drafted and well negotiated to include the compensation for service interruption. The monetary compensation for service blackout has to be clearly specified. "Force Majeure" clause will be there in the SLA, which will entitle the provider to cease their contract in case of natural calamity. Any exception or addition to this clause has to be carefully studied[9].

Provider switch feasibility. If the customer is not satisfied with the service of the provider or if the provider discontinues his service, the provider switching cost and time has to be calculated and specified in SLA.

Secured data transition. Security aspects of the data in transition have to be clearly specified in the SLA. The safety measures and the protocols used should be mentioned in the SLA.

CONCLUSION AND FUTURE SCOPE

Already 55,400 firms use Salesforce.com to manage customer relations and logistics for 1.5 million customers. Still most of the enterprises are not ready to migrate to the cloud because of the security reasons. A highly quantifiable assessment of the providers could help to gain their confidence about the vendors. The customers can adopt encryption of critical data and not all data at their place as it will increase the processing time and the storage capacity of the data. Proper identification of critical data must be done. CSA provides cloud computing knowledge certification for professionals in the same way they have to device a certification for the providers, seeing which the customers can confidentially choose them. The future

scope of this report would be to design parameters of service assessment of the providers. The parameters cannot be the same all over the world as each country will vary in the information security law. Country wise and business wise laws can be defined.

REFERENCES

1. http://searchcloudsecurity.techtarget.com/tip/Cloud-risk-management-Managing-the-risk-of-cloud-outages
2. http://www.csaindia.in/
3. csrc.nist.gov/groups/SNS/cloud-computing
4. http://www.microsoft.com/privatecloud/
5. P. Watson, P. Lord, F. Gibson, P. Periorellis, and G. Pitsilis, “Cloud computing for e-science with carmen,” IBERGRID, 2008
6. http://news.zdnet.com/2100-9595_22-287001.html.
7. Wikipedia, “Cloud computing,” http://en.wikipedia.org/wiki/Cloud_computing.
8. Cloud Computing: Benefits, Risks and Recommendations for Information Security, Nov. 2009; www. enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment.
9. http://www.eetimes.com/design/embedded-internet-design/4217727/Data-security-in-cloud-computing---Part-1--Overview