Security Risks in Cloud Network Innovations in Industries

[1]Ajit Singh, [2]Chetan Sharma, [3]Shuchi Sharma
[1,2]Surya World Institutions of Academic Excellence, Rajpura, Punjab, India
[3]Dr. IT Group, Banur, Punjab, India

Abstract
For last many years the network was represented as a seven layer architecture. Since the year 2008 , several companies are on a cloud computing network. As an emerging technology SaaS, PasS and IaaS are being used at a higher rate. Cloud computing leads to more flexibility, better scalability, higher availability, shorter time to market and better cost control But as more and more information on companies are placed on cloud, concerns are being grown about the security of data placed on third party' local area networks. Keeping in view about the security risks the interest of using clouds is being slowed down. The academia and industry partnership group was formed in 2008 which sets up some rules to integrate various platforms and create some test beds for cloud computing security. The main security breach in this technology is putting your data, running your software on someone else' system. The Various security risks involved in it are phishing and botnet.
Cloud security is abstract and complex, however, and difficult to estimate and measure. This research paper includes a smaller case study of a company using IaaS, where large scale of data was on CSP's Server was used intentionally by an unauthorized personnel. In this research paper key security threats, risks and various security mechanisms which are currently faced and used in the Cloud computing are discussed. Cloud computing has the potential to become a frontrunner in promoting a secure, virtual and economically viable IT solution in the future. However, one must be very careful to understand the security risks and challenges posed in utilizing these technologies.

Keywords
Cloud Computing, Cloud Risks, Security Mechanisms

I. Introduction
This research paper proposes cloud computing from the provider's view as a hardware connected to support downtime on any device in the network, without the change in the users' application level and as well as a cloud risks from the consumers point of view. In cloud computing the processor time, servers, various platforms and software's are offered pay-per-use. As industries are moving towards clouds by increasing the abstraction level at their end but a fear of data location at another network is a prime security issue.

II. Layered Innovations
Traditionally, the organizations had all their resources in their own server rooms, 'on premise' [1]. Over the past few years, the servers were shared with other businesses in Shared Service Centers, while recently they have been outsourced to third parties. The Hosting of data at another server was the next phase in industries.. The shared hosting is provided with a control panel in contrast to a dedicated hosting where a server is non-sharable with any other consumer. The data location compliance in shared hosting is subject to the rules of the hosting company. Cloud computing is the next central innovation in this evolution of IT which has created a hype in the industries.

III. Compliance in Cloud Networks
The adoption and migration to cloud computing is associated with numerous challenges and risks because users are still skeptical about its authenticity. Logging out from the cloud session, the browser may be configured to delete cookies automatically and log files on the Cloud Service Provider's (CSP) side indicating which user accessed which data. This approach may be a small solution to client insecurity for the data stored on the vendor's side. When interviews with KPMG experts were conducted, it showed that private consumers are interested to use and implement the cloud services. However, businesses users are not adopting cloud services. Before organizations can move to the cloud, a number of requirements have to be met. One of the requirements is that the organizations still conform to all applicable regulations and legislation. An important aspect that hinders businesses users from going to the cloud is compliance to data location legislation [2]. Gartner's Magic Quadrant report has placed Amazon's cloud computing service in one of its lower tiers, saying that for all of Amazon's commercial success it is "visionary" but "unproven." [3].

IV. Security Risks and Mechanisms
The verification of the vendor should be a primary concern to prevent the risk of any frauds. What is the vendor's industry background and how long have they been around? These factors all play a role in a cloud infrastructure provider's approach to security. [4] Is the provider SAS70 Type II certified? Statement on Auditing Standards (SAS) No. 70 is the authoritative guidance that allows service organizations to disclose their control activities and processes to their customers and their customers' auditors in a uniform reporting format. [5]. If a service provider has weak firewalls and safeguard mechanisms then there can be more phishing and botnet attacks on the cloud.
A recent Chinese phishing attack on Google´s Gmail puts cloud computing at risk. This attack targeted influential journalists, senior military personnel and government officials in the White House. Along with the hack on Sony's Play station network a 44-day affair that cost the company an estimated $171 million.[6] The Kneber botnet, is the new form of malware has infected more than 74,000 computer systems across the world and is focused on stealing login credentials for e-mail systems, social networks, and banking sites, according to Netwitness. Kneber is incredibly hard to detect and has reportedly compromised data from nearly 2500 corporate and government networks [7].
Another problem with cloud computing is that you depend on servers and storage you don't manage and that could be insecure. Deletion or alteration of records without a backup of the original content is an obvious example. There exists a regulatory compliance for consumer. But both vendor and consumer are under the security risks. What service providers will do if their services are used to distribute stolen and classified information? As WikiLeaks had used Amazon servers for releasing certain confidential and sensitive government information [8]. The next major risk in migrating to cloud computing is how to get your data out of the cloud. If a consumer wants to move to another CSP due to some reasons i.e. what will be the exit strategy?

To prevent various data security breaches some mechanism can be followed:

- Categorization of the data will be the first step towards ensuring its suitability for the cloud.
- Before migrating, your application on cloud, a consumer should be sure about the safety of its data.
- Always use non-sensitive data and less risky applications to initiate cloud operations.
- Evaluate the CSP's agreements like Terms of Service (TOS), Acceptable Use Policies (AUP) and SLAs carefully.
- There should be an infrastructure transparency between the consumer and the provider.

Keeping in view of various risks involved in cloud computing a group named Open Cloud Consortium (OCC) was started by the universities and various companies looking forward to investigate ways of improving computing, storage costs and novelty of this field among different providers.

V. Market Views

The main market views of cloud computing services are divided into leaders, challengers, visionaries and niche players. According to Gartner the leaders are Savvis, AT&T, Rackspace, Verizon Business and Terremark Worldwide. Visionaries include Amazon, GoGrid, CSC, Joyent and IBM. The leaders, meanwhile, have proven they have staying power in the market, and customers should be comfortable signing two or three years contracts with them, Gartner say. The challengers, as defined by Gartner, have a track record of delivering good service capabilities, but they are trailing the market's evolution, while niche players are typically specialists with more limited product portfolios, or emerging vendors. The challengers who placed ahead of Amazon are SunGard, Datapipe, NaviSite and OpSource. Niche players who placed behind Amazon include Hosting.com, Carpathia Hosting, SoftLayer, Layered Tech, Media Temple, and NTT Communications. Amazon is ranked as front leader in providing extraordinary and innovative services to the market. It has the richest cloud IaaS product portfolio, and is constantly expanding its service offerings and reducing its prices [9].

According to critics Amazon's services are not managed. Amazon is the only evaluated vendor and it does not provide any standard options for colocation, dedicated non-virtualized servers. Amazon charges separately for the additional services which are normally clubbed with competitive offerings. It provides developer-centric services, rather than enterprise-oriented, whereas it has significant traction in large enterprises. Amazon is purely an infrastructure-as-a-service vendor, whereas rivals who place higher in Gartner's Magic Quadrant are in the business of hosting physical servers and managing the data centre infrastructure for clients.

Amazon spokeswoman Kay Kinton defended the company's service- level agreements. Kinton writes in an e-mail. " Amazon Web Services (AWS) is clear about how our SLA's are calculated, we do not [exclude] downtime, and our service health dashboard gives customers complete constant access to how the services are performing. What matters most is demonstrated performance, and ours has been strong" [10].

However, risks can be reduced by getting Service Level Agreements (SLA) that provides guarantees for privacy and data safety. As a consumer wants secured servers for their application, it is the responsibility of a consumer to publish the accurate data on the cloud.

Amazon removed whistle blowing website WikiLeaks from its servers amid pressure from federal lawmakers who were upset with WikiLeaks' recent release of certain confidential and sensitive government information. So there is an open risk in cloud computing for service providers also about the extent of their relationship with consumers and what the other web service providers like Amazon will do in the future to ensure that their services are not used to distribute stolen, classified information.

VI. Conclusion

Cloud computing is creating a hype in Industries but the 45% of IT professionals think the risks far outweigh its benefits. According to a survey done by ISACA's in 2010 on cloud computing adoption showed that although cloud computing is a mainstream choice but it is definitely not the primary choice.[11] There are many organizations which have adopted the cloud computing infrastructure but still there are many who haven't opted for it. Before migrating to a cloud, there should be a risk assessment framework for all the information assets. Consumers can only minimize their risk but rewards can be tremendous if the risks are well managed.

References

[1] KPMG,"Orchestrating the New Paradigm", White Paper 2011.
[2] KPMG,"From Hype to Future, Cloud Computing Survey".
[3] Jon Brodkin (2008),"Seven Cloud-Computing Security Risks", [Online] Available: http://www.networkworld.com/news/2008/070208-cloud.html
[4] Security risks of cloud computing [Online] Available: http://bizmology.hoovers.com
[5] [Online] Available: SAS 70 Overview http://sas70.com/sas70_overview.html
[6] [Online] Available: http://www.theamericaspostes.com
[7] Kneber' Botnet Attacks PCs Worldwide, [Online] Available: http://www.pcworld.com
[8] "What led Amazon Kick off WikiLeaks from Servers?", [Online] Available: http://www.ibtimes.com
[9] "Amazon in Media", [Online] Available: http://aws.amazon.com
[10] Gartner's magic quadrant disses Amazon cloud. [Online] Available: http://www.networkworld.com
[11] A Survey on Cloud Computing Adoption [Online] Available: http://www.isaca.org