International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 2 Issue 8
August 2015

Review on Risks and Risk Management in Cloud Platform

Anwesh Mishra[1], Tashi Mishra[2], Assouma[3],Shoney Sebastian[4]
[1, 2,3]PG Scholar Department of Computer Science, Christ University, Bengaluru,India
[4]Associate Professor, Department of Computer Science, Christ University, Bengaluru, India

Abstract: *Cloud technology is one of the hugely popular computing techniques and is growing rapidly. The platform is full of advantages and benefits. In fact almost all the major companies provide cloud services. Some small vendors too are jumping in the cloud industry to start a business. So cloud is the trend which is full of advantages for both the provider and the consumer. However since nothing in the world comes without a con, the cloud platform being no different also has some issues associated with it. The maintenance and security of the cloud services are some of the issues in cloud. This paper consists of the risks associated in cloud computing platform. It starts with the definition of cloud computing, the services being offered by the cloud and goes on to define the risks which are there. The steps to mitigate these risks are also included.*

Keywords: Risks, Risk Management, Cloud service model, Cloud Computing.

I. INTRODUCTION

Cloud computing is one of the fastest growing field in the computer industry. The reason being the fact that it is simple offers a number of services and makes computing easy and hassle-free for people. The cloud industry is growing at a great pace owing to its popularity amongst the companies and individuals. There are numerous companies which offer cloud benefits. Cloud computing is not only provided by the titans like Amazon, Google and Microsoft but also by smaller companies.

Cloud computing is expected to be the next natural step in the evolution of technology, because it'll be an on demand information technology technique[4]. Virtualization will be the technology most of the cloud computing will be based on.

However there are always two sides for a coin. Hence, with the rising popularity of the cloud platform, there are some shortcomings and risks which have been exposed. These shortcomings or risks, no matter how small they are, pose a threat to the security and bring down the overall efficiency of the cloud. These risks may arise due to any loophole in the cloud system, or due to the nature's way. The loopholes may give rise to the security threats, which are again a part of risks in the cloud computing. In this paper we have taken into account various risks in the cloud computing environment, and have tried to find and compare the available measures to mitigate those risks.

These risks and their management strategies we are taking are being taken from a number of research papers available on the same topic. These papers illustrate many risks which are posing trouble and strategies to mitigate them, in the cloud based scenario.

We have done a survey study of the above defined risks. Section one covers the basic introduction of the paper. Section II of the paper covers the basic definition of cloud computing, as in what cloud computing means and what are the benefits of cloud platform, as well as services of cloud. The III section talks about risks. We have included risks from all the papers we have referred to, some of the risks were overlapping so we have mentioned it only once. In the IV part of the paper, we have given the mitigation strategies for these risks, in a tabular form. Last part is the conclusion of the paper.

II. OVERVIEW

A. What is Cloud Computing?

The National Institute of Standards and Technology(NIST) [5] 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''. European Community for Software and Software Services (ECSS) [6] explains it as the delivery of computational resources from a location other than your current one.

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 2 Issue 8
August 2015

The reason that cloud is becoming popular at such a swift rate is because it offers a great number of benefits than traditional computing scenario. It allows the users to follow the principle of pay as you go.

In [7] there are four major reasons given as to why cloud technology is becoming more and more popular:

No up-front investment: No need to sped in infrastructure, pay as go.

Lowering Operating Cost: Rapid allocation and de-allocation, no need to adjust according to peak hour's traffic.

Highly scalable: Easy to expand service to large scales, to meet more demand in business.

Easy Access: Web based services, so easily accessible through variety of devices at any time.

B. Cloud Models

There are basically three types of cloud service models. These are defined [8] as:

Software as a Service (SaaS): deployed to run over internet or run behind a firewall. Widely popular in automation and CRM.

Platform as a Service (PaaS): Can make your own applications using the platform provided by cloud.

Infrastructure as a Service (IaaS): Virtualization is the popular technique for this. Instead of buying equipment, can do it over cloud.

Apart from that there are deployment models for clouds such as public, private, community and hybrid [1]. A public cloud is for multiple users, private is for single user/organization, community is shared one for organizations with common interests and hybrid is a combination of two or more types [1].

III. RISKS IN CLOUD PLATFORM

As mentioned in the previous parts of this paper, the world of cloud computing is not perfect. So there are risks which pose a threat to this computing style. A risk is a situation where danger is exposed to the subject being talked about. In [1]some of the risks mentioned are:

Data Security Administration and Control: Data leakage, privacy, ineffective protection of data in transit etc.

Logical Access: Public network access, i.e. internet exposes to a lot risks.

Network Security: Intrusion, hacking, mobile device attacks.

Physical Security: No data center perimeters so attacks are possible from anywhere in the network.

In[2], the risks mentioned are mostly from an industry perspective a few of the mentioned risks are:

Disruptive Force: It means breaking a tradition and forcing your peers to get into something new, which didn't exist earlier. It puts an undue pressure on the peers to adapt to this change.

Lack of transparency: A cloud service provider will like to maintain the secrecy of its organization.

Reliability and performance issues: The responsibility is to provide best performance and be available all the time for the customers so the customers can totally bank on the service provide for their needs.

Vendor lock-in and lack of application portability or interoperability: Applications once developed on some platform may or may not work on other platforms.

IT organizational change: Shifting from the traditional way of doing things to a new way might reduce performance at times.

In [3]the risks described are from the view point of the industry experts. Some risks thus defined are:

Organizational Risks: When a company moves to cloud it faces issues like compliance to industry standards, in house IT Experts and IT planning.

Operational Risks: Its existing daily working structure also changes.

Technical Risks: There are a lot many technical aspects both the cloud service provider and the consumer have to deal with.

Legal Risks: The service provider and the user both may fall in the trap of legal risks pertaining to intellectuality of the data and theft of data.

The paper[3]goes on to describe other scenarios which may be a risk in the cloud computing environment. We need to understand that risks are not only something which can hamper the working completely. There can be a number of small risks which do not exactly look like a threat but are. In fact when we are looking and paying for a service we want it to be perfect in all means. So technically even a tweak of jeopardy with the service is like making the whole service substandard. So we have talked about a lot of risks above and here too we are

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 2 Issue 8
August 2015

going to discuss some scenarios of risks, as mentioned in[3].

One such scenario can be when the cloud provider is charging hidden expenses for the services provided. Since the user is not totally aware of the charges he'll end up paying more than he should. Second condition could be a case when cloud services become temporarily unavailable. Thus the user can't access the provided service as and when desired. Both of these situations lead to a case where the user is left dissatisfied. This is a risk for both the user, and the provider, because due to the unsatisfied customer their market may downgrade.

Another situation is when at the end of the contract the user wants to move his data/application from the cloud. It could be a tedious job. Firstly the migration of data is exhausting both in the terms of cost as well as ways. Secondly there could be legal restrictions posed on the moving. Thirdly if it is an app built on cloud provided platform, it may not work at all in other platform. This can been seen as being glued to one provider you chose in the beginning, taking away the liberty to try out other providers.

One major risk, more appropriately a drawback to cloud is that the users are not adequately trained while moving to cloud. So they remain uninformed about a lot many facilities and provisions which the cloud service might be providing.

IV. MITIGATION STRATEGIES

There are measures which help in controlling and mitigating the risks defined above. These are taken from [1][2] and described along with the risks in the following:

S.No.	Risks	Mitigation Strategies
1	**Data Security Administration and Control:** These include data integrity, data control, availability of data and services, data privacy, data encryption etc.	Classified information, adequate equipment, third party audit are some of the strategies that can be used.
2	**Logical Access:** Lot of unauthorized access via internet. Weak authentication mechanisms also give rise to such issues.	Establishment of Trusted User profiles, mechanisms for proper security of data. Privileged access monitored, reviewedand revised regularly.
3	**Network Security:**Threat of hackers and unwanted intrusion. Denial of Service and SQL injection are major threats to security of the network through which data travels.	Network level control. Firewall. Only authorized users should be made to change the security settings.
4	**Physical Access:** Data hosted on a virtual location, difficult to guard it.	Network Security mechanisms like data encryption control.
5	**Disruptive Force:**The companies, both the provider and the user, are setting an example for their peers to join them. This disrupts the market, already existing.	Basically it comes down to morality. It is not right to force your peers and pose a threat and risk to their already existing business.
6	**Lack of transparency:** The customer is unaware of a lot of things which go on at the end of cloud service provider. The service provider is not transparent all the time.	The customers should be given a through follow up. Should be mentioned in the terms about what and how will the cloud provider assist in case of any theft or security breach.
7	**Reliability and performance issues:** Service shouldn't be interrupted, whatever may be the case. Possible only in ideal situations. Due to varying speed issues like latency arise.	Fast internet is a must. Both parties should agree and sign on a mutual kind and speed of delivery. Provide with adequate amount of compensation in case of poor performance
8	**Vendor lock-in and lack of application portability or interoperability:** Cloud providers like Google App Engine and IBM Bluemix provide a platform to build and host your own apps, however these are vendor specific and may not run on other cloud.	The platform provided should be more portable and machine independent. Also before signing up for any cloud provider the customer should do background check.
9	**IT organizational change:** The staff, type of committees and a lot of other IT organization related things may change. This may not give ample time to the staff and organization to adjust to new working scenario.	A few tutorial lessons can help. Also the movement to cloud shouldn't be abrupt and impulsive rather it should be one step at a time. Instead of moving everything on cloud, try moving in parts and test how it feels.

V. CONCLUSION

We feel that with some caution these risks can be mitigated to a great deal. New techniques are developing day by day. The cloud providers should follow the rules and laws enforced such as: Payment Card Industry Data Security Standard (PCI DSS), Geographical restrictions applicable to the transit and storing of data, Sarbanes Oxley Act (SOX), Gramm-Leach-Bliley Act (GLBA), Health Insurance Portability and Accountability Act (HIPAA). [1]

Although there are many risks yet it is impossible and incorrect to not move to cloud. Cloud is the next computing style, we need to understand it and adapt to it. It is seen very evidently that if done in a proper way it is not impossible to mitigate these risks. If proper security standards are introduced, and just some attention is paid to the moving data in cloud, the risks of security can be controlled. Abiding by the laws makes it easier for the cloud providers to run their business in a hassle-free manner. The world is moving to cloud, why shouldn't you?

REFERENCES:

[1]- Carroll, Mariana, Alta Van Der Merwe, and Paula Kotze. "Secure cloud computing: Benefits, risks and controls." Information Security South Africa (ISSA), 2011.IEEE, 2011.

[2] Horwath, Crowe, et al. "Enterprise Risk Management for Cloud Computing." COSO.[Online]. Available: http://www. coso. org/documents/Cloud\% 20Computing\% 20Thought\% 20Paper. pdf (2012).

[3] Dutta, Amab, G. C. Peng, and AlokChoudhary. "Risks in enterprise cloud computing: the perspective of IT experts." Journal of Computer Information Systems 53.4 (2013): 39-48.

[4] A Vouk, Mladen. "Cloud computing–issues, research and implementations." CIT. Journal of Computing and Information Technology 16.4 (2008): 235-246.

[5] Mell P, Grance T. Perspectives on cloud computing and standards. National Institute of Standards and Technology (NIST).Information Technology Laboratory; 2009.

[6] CSS, White paper on software and service architectures, Infrastructures and Engineering – Action Paper on the area for the future EU competitiveness Volume 2: Background information, Version 1.3, retrieved:15.08.2010,http://www.euecss.eu/contents/documentation/volume%20two_ECSS%20White%20Paper.pdf

[7] Zhang, Qi, Lu Cheng, and RaoufBoutaba. "Cloud computing: state-of-the-art and research challenges." Journal of internet services and applications 1.1 (2010): 7-18.

[8] Yang, Jianfeng, and Zhibin Chen. "Cloud computing research and security issues."Computational intelligence and software engineering (CiSE), 2010 international conference on.IEEE, 2010.