ISSN: 0975-766X
CODEN: IJPTFI
Research Article

Available Online through
www.ijptonline.com

SUSCEPTIBILITY IN CLOUD

Muthuprasanna B, Dhikhi T
UG Scholar, Saveetha School of Engineering, Saveetha University Chennai, India.
Email: muthuprasanna003@gmail.com

Received on: 02.10.2016 *Accepted on: 28.10.2016*

Abstract

Cloud is the platform for the IT world which has taken over the several technologies in this current scenario. Cloud majorly provides three major services such as Platform as a service, infrastructure as a service, and software as a service. Cloud is the most demanding platform used by every field in IT. Cloud computing relay on the internet as a basic platform for the user to access the data. However this technique is still in it's developing stage and it has some vulnerability and thread that makes this system as a susceptible. Various malicious activity are being performed by the hackers which influence the loss of data and much more. This paper focuses on the various vulnerability that is present in the cloud computing

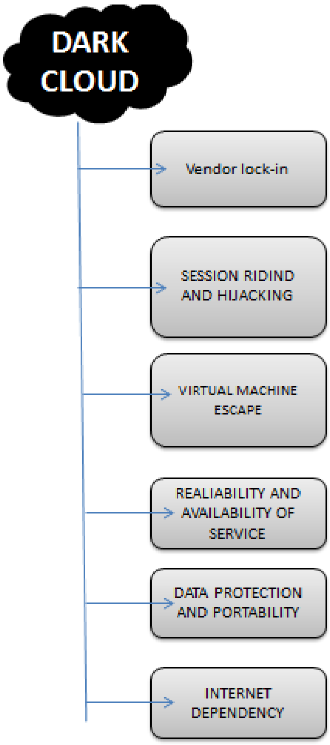
Introduction

As we talk about evolution of computer which started from the abacus devices (small computing devices) to a supercomputers and it has been evolved from single processing computer to distributed computer. The current technology which the computer revolution faces is the cloud. Cloud computing is the process of virtualizing the software, infrastructure and platform and provides the service based on the pay-per-use model. User no longer need to purchase the hardware, software or to manage the storage. In this technology the user are required to pay for the cloud service based on the personal consumption basis. Many service sector provides cloud service from a few cost to no cost. Cloud has the service providers such as the web-based email systems (e.g. Yahoo and Google) to exchange messages with others .social networking sites such as (eg: facebook, linkedin, myspace, twitter, instagram, snapchat) to share information with friends.

On-demand service such as (eg: netflix, hulu) to watch movies and shows. Some of the common storage are (eg: humyo, dropbox and zumodrive) to store personal photos, video, music etc. and online document editing tool such as (eg: google docs) and some of the online backup tool such as jungledisc, carbonite and mozy to automatically backup our data to the cloud server. Major companies started their business in cloud computing. Some companies rent services from the cloud service provider to reduce the management work load and operational cost for example: the social news website, reddit, rents Amazon Elastic Compute Cloud (EC2) for their digital bulletin board service. The digital photo sharing website, SmugMug uses amazon s3 for their photo storing service. Even some company uses cloud services for their advertising purpose.

The flexibility that the cloud services provides have changed our day to day life. However the security issue based on the cloud computing makes our private data into susceptible to the cybercrimes that happens every day. The hijacker uses a variety of technique to access the cloud without legal call authorization .According the DatalossDB, 1,047 data breach have been occurred in the first nine months in 2012 compared to 1,041 of the previous whole year. In this data breach, Epsilionleaked thousands of details from the customer databases. Stratfor's more than seventy thousand credit card numbers and more than eight lakh sixty thousand user names and passwords were stolen. Hijackers could also take gain of the huge computing power of clouds to fire attacks to users who are in the same or various networks. Therefore a good understanding of cloud vulnerable is need in order to provide a secure service to their user.

Here we will discuss the 6 most susceptible things present in the cloud. The vulnerable thread are referred to "DARK CLOUD". The dark cloud consist of various thread the six major thread listed according to their rate to effect.


DARK CLOUD
Vendor lock-in
SESSION RIDIND AND HIJACKING
VIRTUAL MACHINE ESCAPE
REALIABILITY AND AVAILABILITY OF SERVICE
DATA PROTECTION AND PORTABILITY
INTERNET DEPENDENCY

Earlier we mentioned, there are many distinct threads that must be noticed before using this cloud computing these thread are defined below.

A. Vendor Lock-In

One of the key problems of investing in an IT solution is lock-in. Wikipedia defines lock-in as the term of making a customer "dependent on a vendor for products and services, unable to use another buyer without different costs". There are various types of lock-in a company may have. For example, a vendor can interrupt a company's ability to replace their software with a challenging product (known as horizontal lock-in). They can impose technical requirements, forcing clients to use certain databases, operating systems, or hardware. They can pressure a company to purchase an entire suite of products, even if other best offerings are available, by offering huge discounts or taking that integrations or training on more than one products will be challenging. And finally, there is generational lock-in, which makes it very cumbersome – yet necessary – for a company to move a scale up at the product's end of life.

B. Session HI-jacking

It is the way of using an unauthorised way of finding a session key and using it for the identification of user information which is highly confidential and useful for checking the authorisation purposes but the hijackers use it for morphing it and changing them into non useful data. This is called the session hi-jacking. Though session riding is the hijackers giving actions to a web app for the particular user by giving the user an ID and tricking the user to visit a designed web page.

It removes data of users, online transfers like requests for orders, sends information to an internet and modifies system. Although the web techies brings new technologies which take most needed data, provide gain to safe web pages and gives fear.

C. Virtual Machine

Virtual machine escape is something where the hacker runs program on a VM that gives to communicate directly with the server. Such thing could give the hacker access to the host OS and all other virtual machines (VMs) running on that host. Though there are no issues, VM escape is the most important threat to VM security.

Virtual machines are designed to run in own controlled and independent platforms. Every VM should be, an individual system, separated from the host OS and several VMs running on the same system. The host is an intermediate between the server OS and client VM. It takes the host processor and gives resources needed by the customers as required to each guest operating system.

The explanation: "If the hacker can leave the virtual machines, they will likely have control of all of the guests, since the guests are hardly subsets of the program. Also, most virtual machines run with very high priorities on the host as a virtual machine needs access to the server's h/w so it can then match the real hardware into virtualized h/w for the guests. Thus, considering the virtual machine means not only that the guests are gone, but the host is also likely lost."

D. Reliability and Availability of Service

Here the cloud computing is not useful for eg: in February 2008 Amazon-s3 cloud storage was problematic for many hours causing data loss and access problems with various web2.0 With more services being held upon on top of cloud computing infrastructures, an outage can create a domino effect by taking low the huge cost of net services and apps.

E. Data Protection and Portability

Data portability is one of the most problematic in the draft Regulation, with Member States asking whether it would not be better addressed in consumer or competition law. There is concern that controllers to send data may require huge cost and effort - particularly in markets where there is no consumer "lock-in" - and priceless proprietary information and intellectual property. Other drawbacks that have been told by Member States' delegations include concerns around certain industries such as healthcare, where data portability may accuse on-going research.

F. Internet Dependencies

Cloud computing is an internet dependent technology that works only with the support of internet throughout its process of completion. Cloud computing is completely reliable on internet and hence makes it inefficient when there is less or no internet connection. The places like Africa where there is no much internet services provided it becomes harder to use such technology that is dependent on the internet. When there is slow or no internet the banking services and healthcare management becomes tiresome for the storage, processing and accessing of data with less availability of the internet.

Conclusion

Even though there is enough reasons for us to use this technology there are much more important reasons for us to consider why we cannot use this cloud computing on the long run. There are issues like what we have discussed so far. Security plays the most important role of all the other reasons and we have justified whether what are the issues faced in the cloud computing technology.

References:

1. Bernd GroBauer, ToBias Walloschek, and elmars Töcker “Understanding Cloud Computing Vulnerabilities” co published by the IEEE computer and reliability societies, March/April 2011.
2. MervatBarmia and Sarfraz N Brohi, “Seven Deadly Threats and Vulnerabilities in Cloud Computing“ Vol No. 9, Issue No. 1, 087 – 090, 2011 .

3. NarendranCalluruRajasekar, Chris O. Imafidon “Exploitation of Vulnerabilities in Cloud-Storage” International Journal On Computing, Vol.1, No.2, February 2011.
4. Te-Shun Chou “Security Threats OnCloud Computing Vulnerabilities” International Journal of Computer Science & Information Technology (IJCSIT) Vol 5, No 3, June 2013.
5. M. Jensen, C. Meyer, J. Somorovsky, and J. Schwenk, “On the Effectiveness of XML Schema Validation for Countering XML Signature Wrapping Attacks,” First International Workshop on Securing Services on the Cloud, Milan, Italy, September 2011.
6. S. J. Stolfo, M. B. Salem, and A. D. Keromytis, “Fog computing: Mitigating Insider Data Theft Attacks in the Cloud,” IEEE Symposium on Security and Privacy Workshops, pp. 125-128, San Francisco, CA, 2012.
7. A. S. Choudhary and M. L. Dhore, “CIDT: Detection of Malicious Code Injection Attacks on Web Application,” International Journal of Computer Applications, Vol. 52, No. 2, pp. 19-26, August 2012.
8. Symantec Internet Security Threat Report, 2011 Trends, Vol. 17, April 2012.
9. Kavitha. “A survey on security issues in service delivery models of cloud computing”. Journal of Network and Computer Applications, vol.34, pp.1-11, 2011. [10] G., Petri, “Vendor Lock-in and Cloud computing”,[Online],Available:http://clou dcomputing.syscon.com/node/1465147,20 10, [Accessed: 23-Jul-2011].
10. S., Brohi, M., Bamiah, “Challenges and Benefits for Adopting the Paradigm of Cloud Computing”, International Journal of Advanced Engineering Sciences and Technologies (IJAEST), vol. 8, pp. 286 - 290, 2011.