Study of security issues in cloud computing

[1]Krishna Chaitanya.Y, [2]Bhavani Shankar.Y, [3]Kali Rama Krishna.V, [4]V Srinivasa Rao

[1,2,3,4]V.R.Siddhartha Engineering College, Vijayawada, India

Abstract

This paper mainly provides the basic idea on Cloud Computing. It also deals with the Security Issue mainly faced in the Industry where Cloud Computing is implemented and necessary steps which can solve these problems to certain extent

Keywords

Cloud Computing, Security Issues

I. Introduction

Cloud computing provides the facility to access unlimited infrastructure to share business needs. The location of physical resources and devices being accessed are resources, store and execute data, offering services on demand over the network to perform operations that meet changing

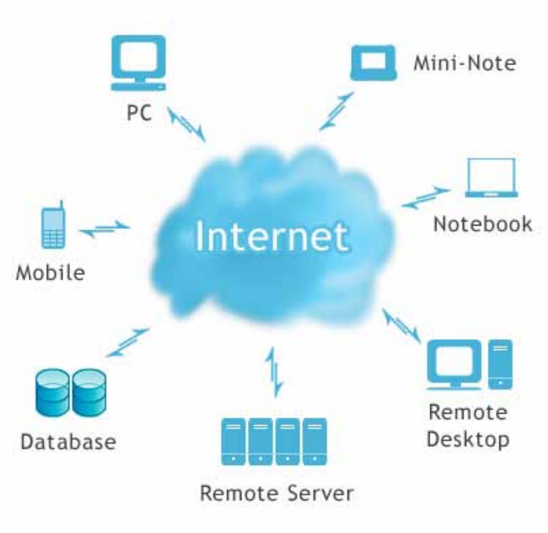


Fig.1: Cloud computing conceptual diagram

Cloud computing conceptual diagram typically not known to the end user. It also provides facilities for users to develop deploy and manage their applications 'on the cloud'. Cloud computing is the latest emerging trend in the field of Information Technology. Cloud Computing can be defined basically as Virtualization of the Technology and providing them as a service to the End user. Main aspects in Cloud Computing are

- Virtualization
- Utility Computing
- Scalability

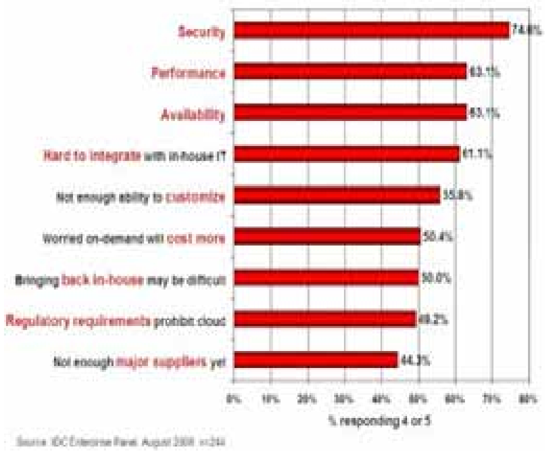
Virtualization means separating the Technology and Data from the Physical hardware. Virtualization is the heart of Cloud computing as it completely depends on it. Scalability feature provides the flexibility to the Cloud User and the provider. It makes the cloud to withstand any changes without affecting the performance of the entire system. Another aspect is Utility computing, where the Software, Infrastructure and platform are provided to Cloud computing Users as a Service. It is purchasing Computing Capacity just like Electricity, Telephone service. Cloud computing mainly provides three ways of Services

- SaaS – Software as a Service
- PaaS – Platform as a Service
- IaaS – Infrastructure as a Service

SaaS provides the Software as a Service to the Cloud Users. Now a days SaaS is like a boon where it worth a fortune to buy Original Software. You can pay depending on the usage of the Software. The PaaS provider provides the hardware, operating system, software upgrades, security and everything else related to the day to day hosting of an application. IaaS can be often referred to as Everything as a Service (EaaS) where user is free to choose anything he wants. IaaS provides CPU, memory, storage, networking and security as a package. IaaS is the virtual machine in the sky. You can choose any Operating system of your choice with desired size of data storage and hardware (like number of CPUs). Clouds can be broadly divided in to two categories. Public clouds and Private clouds. "Public Cloud" is one which is opened to public as a service. Anyone can utilize the services by paying to what they use. Top players in providing public Cloud are Amazon S3, Microsoft Azure, Google, Rackspace. Many business organizations make a Cloud and utilize it for the sake of their organization which can be called as a "Private Cloud". Even though

II. Security Issues in Cloud computing

Cloud Computing seems to be a boon for the IT and Business Industry, there are many Security Issues which may create a drastic damage to the users. We are now going to discuss various security issues such as Intruder Detection, Data segregation, Data Distribution, Hyper-Jacking attacks, Malicious Insider, Recovery.



Source: IDC Enterprise Panel, August 2008, n=244

Fig. 2 given stats confirm that the "Security" is the main Challenge in Cloud Computing.

A. Need more than one IaaS provider

All the data of the user is stored in the huge data storage space available in the cloud. Whenever a particular user wants to access his/her information the corresponding data of the user is retrieved and is presented before him/her. For storing these huge data, the cloud need large databases and hard disks. All this hardware is kept at a particular place in the cloud and proper measures are taken to protect them. Even then there is very much Fig.2 : Challenges/issues of the cloud computing "On-demand model" [3] chance of the damage to these hardware devices due to natural calamities like floods, earth quakes, cyclones etc or accidents. If this happens then all the user data that is stored on storage hardware devices are lost and the cloud computing is a failure. There may be cases where there is failure in the data centre of Service provider which may lead to the outage of data. Data once lost is difficult to retrieve. For example, Top Cloud IaaS provider Rackspace data center Power transformer was once hit by a Truck which resulted in the outage of data. So, maintaining more than one IaaS provider is always a better way. So, that if the data is spread into many places there may be chance of easy recovery in less time even in the time of Natural calamities.

B. Security Scan for Data leaving the Cloud

Cloud is a huge database of resources from various users around the world. All users may not be trusted. There may be intruders and cyber criminals who use the Cloud for Illegal activities and they may store malicious content in the cloud which may affect the common user. For example, if a Cyber criminal placed a data which may contain virus and Trojans such as autorun.inf and if the same data will be kept for access to may cloud users. This may cause a drastic damage to the users and their hard disks if that data is accessed. This can be prevented to some extent if the Data which is intended to leave the Cloud must be scanned with necessary Security devices. This may not completely eliminate the risk but can help to certain extent. Administrator must check the security for the Data which is entering and leaving the Cloud. If any suspicious data is found then the author's account must be deleted from the Cloud as soon as possible to keep the cloud clean.

C. Investigative Support

A single cloud consists of number of users in it. Each user will have an account and will be accessing through that account. There is a possibility that all the users may access their accounts simultaneously from the cloud at a time. Different users work on different applications as per their requirements in the cloud. Some users work sincerely and some users may work with the applications which may cause threat to the cloud. Such illegal activities may cause intense threat to the users private data. It also may lead to data loss stored in the cloud inside huge storage devices. The cloud provider must investigate through all the accounts from time to time to see whether such illegal activities are running in the environment of the cloud or not. If the cloud provider found any such activity, then he must be in a position to take necessary action against that illegal application and have to prevent the threat caused by the application to the cloud. But practically speaking this is difficult. It is very difficult to investigate each and every user in the cloud and each and every application being performed by the user, from time to time, in that huge cloud in which a lot of users and a lot of applications are present. Even then if you found that illegal application, you must take necessary action against it in no time which is very much difficult than finding the illegal application. The easy solution to the later problem is to delete that application and the user account as soon as possible. Therefore the cloud provider must be ready with a good Investigative support team and ensure users that they are safe from this serious security threat in cloud computing.

D. Data Segregation

Data segregation is one of the major risks in cloud computing. Users data can be kept in the shared mode or in private mode as per wish of the user in a cloud. Over all user's data and information in the cloud is in the shared environment. Due to this reason there is very much chance of the user's private data to be seen by other users. If the data and the information is not protected from other users then it is a major risk to the user to keep his/her private information, bank account numbers, secret codes, passwords so on in the cloud. If intense authorization and authentication is not provided to the users data in a cloud then this cloud computing is a failure. Hence the cloud provider must take intense care while segregating the data. The cloud provider must ensure the user that the cloud provided by him is very much secure from the external penetrations into private data of the user.

This segregation in the cloud computing environment can be provided through encryption and decryption methods. Generally there is huge storage area in the cloud and all the data of the users are kept in this place. Before storing all the information of a user, encryption must be done on the data of the user and then it is stored. Before retrieving the data by the user, decryption is performed on the data of that particular user and then the information is provided to the user. Authentication and Authorization provide more security to the user data.

E. Authentication includes:

- SSL authentication: An SSL authentication assures security during the online transactions.
- Certification Authorization: X.509 certificates can be used to provide authorization
- Kerberoes based Authentication: This type of authentication services include 3 steps: Firstly: The client and server should register their keys in the kerberoes server and Secondly: When the client wants to communicate with the service provider it sends the request to the Kerberoes server Finally: The kerberoes Server will generate a session key randomly and will allow the client and the service provider to communicate with each other.

Authorization includes:

It is a process that traditionally says the privileges to the user to access particular information or access a service.

F. Availability of Service:

It is the major issue of concern in the cloud computing area because Cloud computing is mainly an Internet based computing technology and there cannot be given any assurance for the 100% availability of Internet. It may vary according to the broadband speed and plans that are given by the service provider. Consider the website www.eyeos.com which provides a separate OS to run within it along with free space for storing some files within it. If a user wants to access the file that is present within it and has no internet connection then there is no access to the files present in there. If the user is viewing a file that is present with in the cloud and suddenly if the Internet connection fails then there will be no access to the file.

Also, this issue includes the long term viability of the cloud provider which says that if the cloud provider who is providing the services to a group is swallowed by a larger company will that organization provide a guarantee to the data that is present till now in the cloud.

G. Hyper -jacking Attacks:

As virtualization is the main theme of cloud computing the cloud are prone to hyper-jack attacks. To know about the guest hopping attacks we must know Hyper-jacking attacks. A hyper visor is a virtual machine that allows the user to run multiple operating systems concurrently. Hyper-jacking attacks mainly involves in the hardware manipulation. The hypervisor that attacks the system mainly operates underneath the system in stealth mode (secret) this causes main problem as the user cannot identify the hacker. If the hacker gets control over the main system then it is difficult to know from where the system got hacked as the OS will not be aware of the operating systems that the hacker system comprises of. If the hyper-jacking attacks are more then that leads to the guest hopping attacks. In order to perform the hyper-jacking attacks one should have the processor which supports hardware support virtualization. This has no solution as per the present knowledge and Microsoft is the leading organization that is performing the research on this Hyper-jacking attacks.

III. Conclusion

Cloud Computing is the beginning of the Internet based services. This is the new era in the Computing Industry. Pros and Cons are general for any Service. Along with the abundant uses in Cloud computing there are several Security threats that is being faced in the industry at present. Clients who are opting for the Services of the Cloud computing must beware of the Security concerns so that they may not be affected and lose their data.

References

[1] ENISA (2009) "cloud computing Benefits, Risks and Recommendations For Information Security".

[2] Siti Fatimah Abdul Razak, "Cloud Computing in Malaysia Universities", IEEE 2009 conference on Intelligent Systems and Industrial Applications

[3] "Gartner: Seven Cloud computing issues", InfoWorld.com [Online] Avaible : http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853

[4] "David Binning Top 5 Cloud computing issues. [Online] Avaible : http://www.computerweekly.com/Articles/2010/01/12/235782/Top-five-cloud-computing-security-issues.htm.

[5] "Cloud Computing may pose Serious threat", DigiTrends.com [Online] Avaible : http://www.digitaltrends.com/features/cloud-computing-could-pose-serious-security-issues.

[6] Srinivas Rao V, Nageswara Rao, N K E Kusuma Kumari, “Cloud computing: An overview”, (JATIT) Journal of Theoretical and applied Information Technology, 2009.