Policy for Security issues in Cloud Computing

[1]Jijo S. Nair, [2]Mukesh Kumar
Dept. of Computer Science &InfoTech
MANIT-Bhopal

Abstract
IT industry and organizations revolutionized with a staggering velocity in the last decimvir by the inlet of Cloud Computing Technology .Day by day more and more academicians, research scholars, IT industries, SME (Small and Medium Enterprises) gerents are drifting themselves towards the hot chocolaty flavored moorland of "Cloud Computing". As more and more enterprises, government agencies, and companies started to explore cloud computing, security issues came out as a gigantic gamut, as every individual preferred to work on a safe environment where privacy and security of their data is a major concern. This paper discusses cloud computing concepts, technical characteristics of cloud computing, analyses information security in cloud computing, security strategies and challenges that Cloud Service Providers (CSP) or vendors face during cloud engineering.

Keywords: Cloud Computing, Cloud Policy.

Introduction
Every enterprise and person wantsto explain "cloud" concept by their own words. If we gives a neutral definition, cloud computing is the resource delivery, it means get resources (hardware software) via network. The network of providing resources is called 'cloud'. Cloud computing has the potential to append the software industries entirely as application are purchased, license and run over the network instead of a user desktop. All the management is done on behalf of the cloud computing service provider. Cloud computing have main three service model. First is SaaS (Software as a Service) that refer to the software deliver to the client by cloud server, and user can access applications through network, SaaS eliminates the need to install and run applications on the customer's owncomputers/servers and simplifies maintenance, upgrades and support, resource allocation used to do in the multi tenant way. SaaS makes the utilization of the resources efficiently.

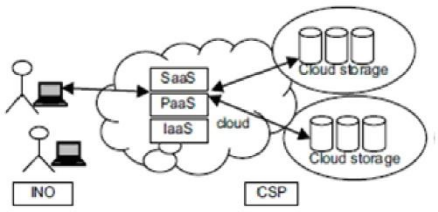

Fig – 1

Many companies provide SaaS services such as Google Apps, salesforce.com, officelive.com etc. Second is PaaS (Platform as a Service) provide facility to enable software and develop software to the user over the Internet. It also provides facilitate of development and deployment of applications Many companies provide of PaaS services like Azure, Google App Engine, force.com etc. Third is IaaS (Infrastricture as a Service) deliver a virtualization environment as-a-service rather than purchasing & configuring servers, storage and network equipment, The client can utilize these resources as a fully outsourced service. This service is typically billed on a utility computing basis and the amount of resources consumed. Many companies provide these facilities like Amazon, IBM, and EMC etc.

Types of Cloud
Public cloud, provide theservices to the multiple clients, and clients don't know many other users's running the application on the same server, network or disk. In Private Cloud, users can use it privately, and thus it become the most

Effective in control of data and secure. Companies have their own infrastructure and by this infrastructure, it can control the way to deploy applications. Server, network and disk can only be accessed by the authorized person, to use these infrastructures. Private clouds can be deployed in enterprise's data centers; it can also be deployed for hosting site. Private cloud can be built by the companies itself or by the cloud providers. The last is Hybrid cloud that contains the property of both public and private cloud.

Related Work in Cloud

The problem in thecloud is yet to be resolved by the IT industry, however, it is not perfect, some example are in February 2009, Google Gmail mailbox interrupt service for up to 4 hours, the fault is Owing Routine maintenance of data centers in Europe, making Europe overload another data center, and spread to other data centers eventually Google Gmail mail service interruption occurs worldwide. In mid-March, Microsoft's Azure stopped running about 22 hours. In addition, the 2008 Amazon S3 service was interrupted for 6 hours. All show that cloud computing is not that perfect, cloud computing services with its own security risks in the application is deepening gradually exposed. Despite the fact Cloud computing allows business users and individual user access many benefits, when the user start using cloud computing services, although there is a lot of security risks is evolving around cloud computing [2].

Fig - 2

The main problem of cloud security occurs in following way:-
A- Unsafe Application Programming Interface. B- Authentication mechanisms are weak.
C- Not correctly use the cloud computing.
D- Difficult to assess the reliability of suppliers. E- Share technical flaws.
F- Data loss / leakage.
As from the last years IT industry is adopting the business concept of cloud computing, major stress by

The industry is in the management & policy for security in cloud computing. Cloud requires only a system and a internet connection and user can get the data from the cloud where it is stores. Now the major issue is weather our data, which is present in the cloud will be secured or not. As data is in cloud authorization and security measures are to be adopted by the individual, also privacy of the data present in cloud is to be maintained. As data is in network (cloud) the data can be present any where irrespective of physical location (country) from where it is hosted. The customer need to make policy agreement so that the data will be present in specific jurisdictions as customers are fully responsible for the security and integrity of their own data, irrespective of their service provider. As data is present in a shared environment in cloud so data segregation is to be done by adopting powerful encryption technique which is tested and approved by the standard authorities. If at all collision occur on the cloud provider side then policy should assure that the client data is secured in any other place that is it should be able to recover the data in case a disaster or failure happens. Customer should assure if the current cloud service provider (CSP) merge with another cloud service provider then customers data should not be loss. Any inappropriate or illegal activity may take place in cloud computing then it should be able to chase out from where it occurred so as investigation can be done how activities took part.

Common Security Issue around Cloud Computing across Four main Categories:-
A – Data
B -Access
C - Compliance
D - Cloud infrastructure, platform and hosted code

Advanced Issue in Cloud Computing Security:-
A - Abstraction
B - Lack of execution controls C - Third-party control of data D - Multi-party processing [3].

Security Threats Presents in the Cloud -
There are various security concerns that prevent customers from taking benefits of the cloud. In this section, we have analyzed the security threats present in the cloud:-
A - VM-Level attacks
B - Abuse and Nefarious use of cloud computing C - Loss of governance
D - Lock-IN
E - Insecure Interfaces and APIs F - Isolation Failure
G - Malicious Insiders
H - Account or service Hijacking

I - Management Interface Compromise [5].

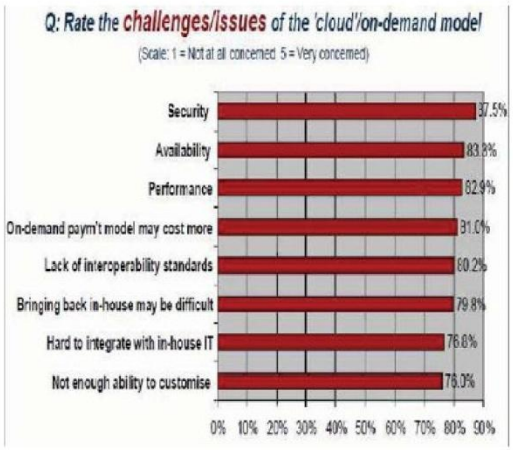

Fig – 3

Secure Cloud Architecture

Secure CloudArchitecture should be implemented in both physical and logical layers of the cloud as shown in fig (4)

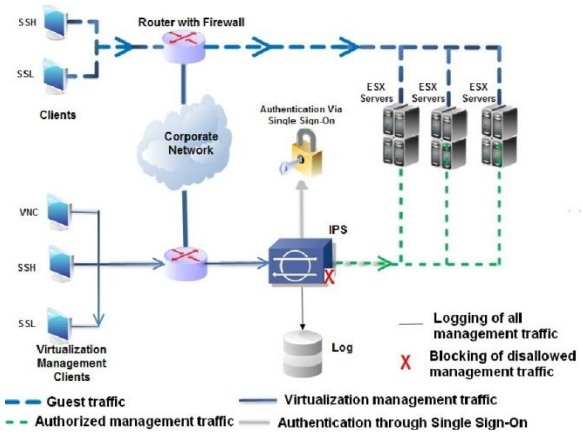

Fig - 4

Conclusion

In this paper we have focused on thebasic working, security issue of the cloud computing and future policy adoption for secure cloud computing. Cloud computing impact on the whole IT industry has been enormous, and compared with professional computing, cloud computing is more universal and extends to all corners of the world, which applied Commercial areas. With innovation and change in the same time, it puts forward higher requirements on security issues. It needs to establish a standardized system to solve problems triggered by a variety of security issues in cloud computingenvironment. Cloud

infrastructure relies on trusted computing and cryptography. Organizational data must be protected in a manner consistent with policies, whether in the organization's computing center or the cloud. No standard service contract exists that covers the ranges of cloud services available and the needs of different organizations. Having a list of common outsourcing provisions, such as privacy and security standards, regulatory and compliance issues, service level requirements and penalties, change management processes, continuity of service provisions, and termination rights, provides a useful starting point [10].

Future Work

These are all very importanttopics which will be certainly discussed in the upcoming years of cloud computing. Based on IDC(International Data Corporation) survey [11] the security and vulnerability market should exceed revenue of $4.4 billion by the end of 2013, with a climbing annual growth rate resulting in a compound annual growth rate (CAGR) of 10.8%. This survey shows that products that fall within the security and vulnerability management market will remain in high demand.

Reference

1. http://www.slideshare.net/liuliming/introduction-to-cloud-computing-presentation.
2. HaoyongLv, Yin Hu "Analysis and Research about Cloud Computing Security Protect policy" 2011 International Conference on Intelligence Science and Information Engineering.
3. ShubhashisSengupta, Vikrant Kaulgud, VibhuSaujanya Sharma "Cloud Computing Security - Trends and Research Directions" 2011 IEEE World Congress on Services.
4. IrfanGul, AtiqurRehman, M Hasan Islam "Cloud Computing Security Auditing".
5. AlokTripathi, Abhinav Mishra "Cloud Computing Security Considerations".
6. FarzadSabahi "Virtualization-Level Security in Cloud Computing"
7. Ramgovind S, Eloff MM, Smith E "The Management of Security in Cloud Computing".
8. Chenguang Wang, Huaizhi Yan "Study of Cloud Computing Security Based on Private Face Recognition"
9. Sang-Ho Na, Jun-Young Park, Eui-Nam Huh "personal cloud computing security framework".
10. Wayne A. Jansen, NIST "Cloud Hooks:
11. Security and Privacy Issues in Cloud Computing" [11]http://vulnerabilitymanagement.com/docs/IDC_MA_2009.pdf