Volume 3, Issue 7, July 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Security : A Major Concern in Cloud Computing

Priyanka Ora*
PAHER University, Udaipur
Udaipur, India

P. R. Pal
Lakshmi Naryan College of
Technology, MCA Department & University, India

Abstract—Cloud computing is an emerging trend in technical world . In today's scenario cloud computing used at major level any user can access its service and resources. It is the new term which is widely known in terms of IT .In this paper different types of clouds like Public, Private and Hybrid clouds are explained . Architecture of different service provider like SaaS,PaaS and IaaS is explained . Security is major concern in cloud computing as we are sharing our resources and data. In this paper various security issues and their improvement suggestions has been discussed.

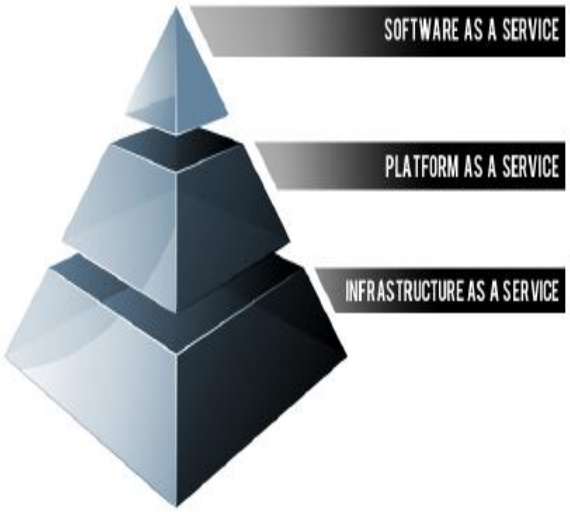
Keywords— Cloud computing , PaaS ,SaaS, IaaS ,Security

I. Introduction

Cloud computing is a new approach for delivering resources to users .It is a computing model which provides its service better than internet .It can be next higher level of internet .It is a collection of large number of server which transform information to its connected server .It provides platform to n number of server to use resources .In cloud computing main task is of clouds ,clouds are the entities which provides a platform to server for exchanging information and utilize services .This clouds are available in three forms public , private and hybrid .If we define all these clouds then in public anyone can transform the information and use resources ; whereas in private only authorized user can access information and hybrid is a combination of both public and private .

II .Cloud Computing Architecture

Cloud computing provide its services with the help of service providers which is known as cloud provider. This provider can provide availability of resources , storage and software to access . Basically there are three types of provider which are Saas(Software as Service),PaaS(Platform as a Service) and IaaS(Infrastructure as a Service).As we saw its service delivery model, which is based on this three server provider in which at the bottom layer Iaas(Infrastrucre as a service) is present it provides a flexible, standard, and virtualized operating environment that can become a foundation for PaaS and SaaS ; Next level is of PaaS (Platform as a service) which provides an efficient and lively approach to operate scale-out applications in a predictable and cost-effective manner. Last and the topmost level is SaaS (software as a service) which provides software application to user.



Although all these layers reduce cost data rates and leakages, they estimate and reduce software delivery time, highly availability of resources , easy scalability and condense license cost for users. In spite of all these facility cloud computing is having a severe concern regarding its security because user need to connect with unknown server and they

give right to share their hardware and software resources so chances of data loss get increase. In Cloud computing technology there are a set of important policy issues, which include issues of privacy, security, anonymity, telecommunications capacity, reliability, and liability among each other , But the most important among them is security and how cloud provider assures it. Generally, Cloud computing has several customers such as ordinary users, academia, and enterprises who have different motivation to move to cloud so security should be managed properly.

III. Literature Review

Cloud computing challenges and security discussed by various researchers Alok tripathi, Mishra [1] has discussed cloud computing security problems and has designed one security architecture model for organization. Mohamed Al Morsy[2] has described about cloud computing architecture and discussed some new techniques related with cloud computing security .[3] Farzad Sabahi has discussed some of the major Security concern which enterprise phases and suggest solutions related with that concern .[4] Takes a detailed look at cloud computing security risks and conclude that, as computing takes a step forward to cloud computing, security should not move backward. Users should not accept moving backward in terms of security, and computing technology and security both, must advance together.[5] Discuss the fundamental trusted computing technology.

IV. Security issues in cloud computing

In the last few years cloud computing has been mostly used by all organization. Any software company can just by tapping in the cloud can gain the flexibility and fast accessing of data, but the main drawback with cloud computing is data protection because our data ,resources is distributed among all server, Here is the question of security arises .Some security threats with their solutions has been discussed below:

(a)Despicable use of cloud Computing : The biggest drawback of cloud computing is anyone can register and use the resources of available server due to which probability of hackers and spammer of attacking the system would increase which create insecurity among users .

Mitigation: There are two approaches which can be done to overcome this situation
1. By implementing strict registration process.
2. By doing strict observation and inspection towards user's profile.

(b)Data loss & Regulatory compliance: This condition occurs when user is not sufficient with the current service provider in that situation user has to move to other cloud provider for resources which occur data lose. Customers are ultimately responsible for the security and integrity of their own data, even when it is held by a service provider . Traditional service providers are subjected to external audits and security certifications.

Mitigation:
1. We can use efficient provider which can fulfill all the requirement of cloud user.

(c)Data location and storage: When clients use the cloud, they probably won't know exactly where their data are hosted and transferred. Distributed data storage is a usual manner of cloud providers that can cause lack of control and this is not good for customers who have their data in local machine before moving from local to cloud.

Mitigation:
1. We can apply the system for user to store the data on their personal machines or system.

(d) Data Leakage: Data in the cloud is typically in a shared environment alongside data from other customers. Encryption is effective but isn't a cure all. Encryption and decryption is a classic way to cover security issues but heretofore it couldn't ensure to provide perfect solution for it

Mitigation:
1. Before moving your application to the cloud, do some attack modeling and consider the value of your assets to be stored in the cloud, versus the cloud service costs and custom security measures you may (or may not need) to implement.

(e) Recovery: If connectivity with cloud provider broke or some problems cause failure in cloud sever the system may lose user data. Cloud provider may or not be restore data completely, moreover clients prefer don't get permission to third-party companies to control their data. This issue can cause an impasse in security.

Mitigation:
1 .Cloud Provider has to provide some recovery software so that in case of system damage data can be protected up to some extent.

(f)Investigative support: Cloud services are especially difficult to investigate, because logging and data for multiple customers may be co-located and may also be spread across an ever-changing set of hosts and data centres.

Mitigation:

1. Each customer must know about where they are logged in and for how much time they are using resources.

(g) Long-term availability of Data : Ideally, cloud computing provider will never go broke or get acquired by a larger company .In that situation what will be the surety of data after such an event.

Mitigation:

1. Before log in the cloud provider they has to give data assurity and availability to the client so that they are well known about all the norms.

V. Conclusion

Although cloud computing is extensively used by many enterprises for optimization of new technology in a cost effective manner ,It provides several powerful resources and services to users at one hand but on the other hand it needs security . Enterprises that are implementing cloud computing should be aware of the security issues related with cloud computing. Proactive enterprises must follow the above mentioned solutions before using this security mitigation which are discussed above. In future this techniques may be modified with the advancement of security technologies

References:

1. Alok Tripathi, Abhinav Mishra, *Signal Processing, Communications and Computing (ICSPCC) Proceeding International Conference IEEE(Xi'an, China ,14-16 Sept.2011).*
2. Mohamed Al Morsy, John Grundy and Ingo Muller *An Analysis of The Cloud Computing Security Problem at 17th Asia-Pacific Software Engineering Conference (APSEC 2010) Cloud Workshop, (Sydney, Australia, 30 November-03 December 2010).*
3. Farzad Sabahi *Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference* .
4. "*A Security Analysis of Cloud Computing*" http://cloudcomputing.syscon.
5. "*Cloud Computing and Security –A Natural Match, Trusted computing Group (TCG)* http://www.trustedcomputinggroup.org.

