MAT JOURNALS

Journal of Web Development and Web Designing

Volume 2 Issue 2

Cloud Computing Models: Background, Data security, & Security Issues

Ms. Shashi
Reseach Scholar
Noida International Univeristy, Noida
Email: teotia.shashi@gmail.com

Dr. Anuranjan Mishra
Professor & Head CSE
Noida International Univeristy, Noida
Email:amc290@gmail.com

Abstract

Cloud computing is getting popular ,cost effective ,powerful resources over internet and rapidly growing area in last few years. Cloud Computing is more growing and features mentioned above encourage the organizations to shift their applications and service to cloud and grid. For the sharing resources that contains software, applications, infrastructures, cloud computing is the main key. Cloud computing has brought remarkable potential changes and good opportunities to information technology industry. A major concern in cloud computing is towards its security and privacy. Security issue is organized into many categories:- Data portability, Data protection, Reliability and ownership. However, most existing Cloud Computing platforms have not formally adopted the service-oriented architecture (SOA) that would make them more flexible, extensible, and reusable. By bridging the power of SOA and virtualization in the context of Cloud Computing ecosystem, this paper presents the existing issues in cloud computing. Proposition of solution for these issues has been provided also.

Keywords: *Cloud Computing, SAAS, Security*

INTRODUCTION

Cloud computing is a computing paradigm where a large pool of system are connected in private or public network to provide infrastructure for application, data and file storage.

Cloud provides virtual space to the user using various technologies. For eg. web server, virtual environment etc. It is a computing that provides on demand services to the organizations or individuals. The cloud service provider provides the services only to the registered users on payment base. It is the main task of service provider to provide the security and trust into environment. The cloud computing promotes availability and reliability. Cloud computing is divided into three categories (model) and it has four deployment model .

The Background of Cloud Computing

Cloud Computing is emerged as the modern technology which developed in last few years, and considered as the next big thing, in the years to come. Since it is new, so it require new security issues and face new challenges as well [3]. In last few years it is grown up from just being a concept to a major part of IT industry. Cloud computing accepted as the adoption of virtualization, Service Oriented Architecture. The security issue might be vulnerable in cloud computing. The security of data provided by service provider will be under infrastructure area. Data security over the cloud computing is major issue for service provider. There are many methods are proposed to preserve the data and keep secure the data in cloud computing. .

Cloud computing works in layers as applying policies on these layers provide better security approach and to manage the security concerns [8]. The most important thing of cloud computing is that it enables customers a new way to increase capacity and add capabilities to their machines on the go.

Cloud Computing Evolution

Before we start with cloud computing, three concepts of computing must be clearly understood those are:-

A. Cluster Computing
B. Grid Computing
C. Utility Computing

Cluster Computing

This is clustering of the coupled computers, to work in a group to accomplish a single computing task by working closely equivalent of forming a single computer. The cluster components are not mendatory, connected to each other through local area networks. This grouping of computers improves the performance, speed and availability as well as reduces the overall cost, instead of working over a single computer.

Grid Computing

Grid computing (group of networked computers) that work together as a virtual server to perform large task. The system in grid can be in multiple locations. And Grid computing is composed of many network loosely coupled system to perform a large task. The main differences between the grids computing from cluster computing are

a) More loosely coupled
b) Heterogeneous
c) Geographically distributed.

The separate grids can be dedicated to single application; but a single grid can also be accessed for a variety of different applications.

Utility Computing

Utility computing is a service model in which service provider make resource and infrastructure to user as needed and it works on pay per use basis . User pays for that what we used or accessed from pool e.g. storage, software and servers. Utility computing is wrapping up of computing resources as a payed service. This computing service become on demand computing, software as a service IBM, and HP were early leaders in the field of utility computing. Lots of organization works on architecture and payment and what will be the new challenges in this computing model. Google, Amazon and others started to take the lead in 2008, as they established their own utility services for computing, storage and applications.

Models of Cloud Computing

The major cloud providers in the current market segment are Amazon, Google, IBM, Microsoft etc. Some major challenges that are being faced by cloud computing are to be secured, protect and process the data which is the property of the user.

The users are able to use application as services on the clouds using the internet. User can typically connect to clouds via web browser or web services. It has several security issues. Cloud computing providers services based on three fundamental service delivery models.

An Infrastructure-as-a-Service (IaaS) model provides the capability to provision the computing and storage resources on demand by the users. The users are able to deploy and run the software which includes operating system and other applications and some selected network component, but they don't control the cloud infrastructure. Data

security consideration for IaaS includes the management of virtual resources allocation and addressing the virtualization and vulnerabilities and risks that affect the IaaS delivery model.[2]

A Platform-as-a-Service (PaaS) model provides the computing platform and solution stack as a service to the users. The users are able to develop their application without purchasing and managing the hardware and software necessary for their application development. The complete life cycle support the delivering application and services are provided by the PaaS model. The user has controlled over the applications. and hosting environment configuration. They do not control the overall cloud infrastructure, network, servers, operating systems. In PaaS, the service provider give control to the user to build the application on platform.

Software-as-a-Service (SaaS) model allow the cloud users to access the applications from cloud providers.
The user od SaaS will not have to worried about the cloud infrastructure and platform The applications are mostly accessed by users using thin clients via the web browser. The users have control over only their application configuration. The cloud resources should be managed and controlled by the cloud providers.These applications are hosted in the cloud SaaS are used as common delivery model for most of the business applications like Enterprise Resources planning , Customer Relationship Management , and human Resource Management (HRM) and so on. In effect, there should be more focus provided for access control and identities for accessing the enterprise applications in cloud. SaaS users are billed based on the usage in the monthly or yearly basis.

All these cloud services are accessed via the cloud clients such as desktop, laptop, smart phones, tablets and wireless sensor nodes which are connected to the network

Types of clouds
There are four basic types of clouds

Public cloud
Public Cloud is very popular type of cloud system. In public cloud system ,the infrastructure in own by the service provider. The user pay the service provider to services and resources they use. Public cloud can be deployed much faster. Public cloud user pay as they demand for cloud services they utilized. Amazon is the most popular public cloud computing service provider.

Private cloud
Private cloud is that cloud that is run and managed by only for single organization The infrastructure can be manged by the organization or managed bt the third party. Private cloud is expensive and considered more secure than public clouds. Resource in private cloud are not utilized by any other user..

Hybrid Cloud
The cloud infrastructure is a composition of two or more clouds (private, public, community). Organizations host some critical, secure applications in private clouds. Cloud bursting (data and application portability) is the term used to define a system where the organization uses its own infrastructure for normal usage, but cloud is used for peak loads.

Community cloud
It is a collaborative effort in which infrastructure is shared between several organizations from specific community

which is managed by internally or by third party.

Characteristics of Cloud Computing

In general, Cloud Computing has the following characteristics

Accessibility: Cloud services can be accessed from anywhere at any time via browsers or APIs by different client platforms such as laptops, desktops, mobile phones and tablets. Cloud services are network dependent, so the network (Internet, LAN, or WAN) has to work in order to access cloud services.

On demand self-service: Customers access cloud services when they need them without going through a lengthy process.

Elasticity: Elasticity refers the asbility of a service to adjust (increase or decrease capacity) in order to meet the user's needs.

Pay-as-you-go: Depending on the pricing model, customers only pay for the services they consume (computing power, bandwidth, storage, number of users, etc.). Sometimes, the services have flat rate, or they are free of charge.

Versatility: Cloud Computing supports different types of services: IaaS, PaaS, and SaaS, and each service can provide various applications running at the same time.

Shared Resources: Cloud resources such as infrastructure, platform and software are shared among multiple customers (multi-tenant), which enable unused resources to serve different needs for different customers.

Security: Cloud resources are centrally managed, so in theory security should be improved in this type of environments. However, security in complex environments is hard to undertake due to the fact data is stored and processed in unknown places, resources are shared by unrelated users, and other concerns.

Reliability: Cloud computing supports reliability by adding redundant sites in case an error or attack happens.

Performance: The performance of applications can be better in clouds because computing resources can be assigned to them when workloads surge. Clouds can be suitable for intense-data applications since they require several computing resources.

Data Security & Security Issues of Cloud Computing

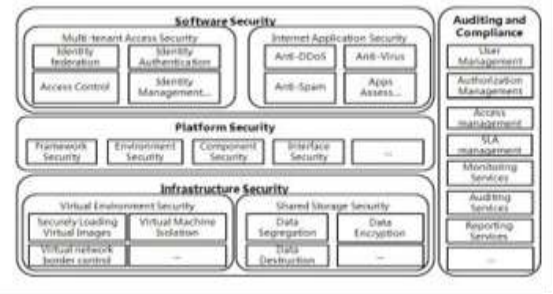
A. Cloud Computing Security

The issue of security in cloud computing is great challenge .Confidentiality and integrity are widely used terms in security in computing . Security threats in cloud would affect multiple users.

Cloud computing security (simply as "cloud security") is an evolving sub-domain of computer security, network security, and, broadly, information security.."

B. Security Issues Associated with the Cloud

The security issues in cloud is differ from risk of infrastructure in nature. In cloud , any user can access data from any location.. cloud computing do not difference between common data and secure data. It is mandatory to service provider to check the integrity by their own system. and restricted the unauthorized users. The main issue that affect the performance of cloud envirionment is unethical transaction and data access applications and user at very long distance from provider , may experience delay. this is due to avalaible bandwidth of network. Session hijacking is also a security issue over cloud computing. DoS is also a attack in SaaS model DoS make the resource and service assigned to unauthorized users. and acts as an interrupt of service to assigned user. The CSA has identified thirteen domains of concerns on cloud computing security [16].



The cloud applications and APIs on the SaaS and PaaS layers require special security attention to have secure development and execution life cycle. The cloud security alliance [21] recommends that the security to the cloud applications and APIs must be provided without any assumption about the external environment. The following are the focal recommendations by the CSA with respect to cloud applications and APIs. _ Security and privacy requirements (both functional and regulatory) should be defined in accordance to the needs of the cloud development and deployment. The defined requirements should also be in the order based on the impact and possibility. _ The risks and attack vectors specific to the cloud computing must be explored and assimilated into the security requirements. The risk models and attack models should be continuously built and maintained. _ The secure software development life cycle and software architecture should be developed and maintained.

CONCLUSION

Computing clouds is changing the whole IT industry, businesses and global economy. Clearly, cloud computing demands effectiveness, security, and trustworthiness. Cloud computing has now become a common in business [10], government, education, and entertainment which is maintained by the 50 millions of servers globally installed at thousands of data centres today. Private clouds will also become usual in addition to using a few public clouds that are under heavy competition among Google, MS, Amazon, Intel, EMC, IBM, SGI, VMware, and Saleforce.com

REFERENCES

1. P. Mell and T. Grance, "The NIST Definition of Cloud Computing," NIST, Special Publication 800-145, Sep. 2011.
2. Rajkumar Buyya et al, Cloud computing and emerging IT platforms: Vision, hype, and reality fordelivering computing as the 5th utility, www.scincedirect.com, 2008.
3. B. Hay, K. Nance, and M. Bishop, "Storm Clouds Rising: Security Challenges for IaaS Cloud Computing,"Proceedings of the 44th Hawaii International Conference on System Sciences pp. 1–7 (Jan. 2011).
4. On technical security issues in cloud computing, Meiko Jensen etal, 2009
5. Security & Architectural Issues for the national Security cloud computing, Anya Kim etal, 2010 [5] Ensuring Data Storage security in cloud computing, Cong Wang, etal, 2010
6. Privacy reserving, Cong Wang etal, 2010
7. Data Security in the world of cloud computing, John Harauz, etal, 2010
8. A layered security approach for cloud computing infrastructure, Mehnet Yeldiz etal, 2010
9. Deloitte. (2010, 31 August 2010). *Executive Forum – Cloud Computing: risks, mitigation strategies, and the role of Internal Audit*. Available: http://www.deloitte.com
10. C. Pettey and B. Tudor. (2010, 5 August 2010). *Gartner says worldwide cloud services market to surpass $68 billion in 2010* Available: http://www.gartner.com/it/page.jsp?id=1389313
11. Press Office. (2010, 31 August 2010). *Cloud Computing Services - New Market Report Published.*

12. Cloud computing security, http://en.wikipedia.org/wiki/Cloudcomputing_security.
13. Gartner: Seven cloud-computing security risks. InfoWorld. 2008-07-02.
14. http://www.infoworld.com/d/security-central/gartner-seven-cloudcomputing-security-risks-853.ffh
15. Cloud Security Front and Center. Forrester Research.2009-11-18. http://blogs.forrester.com/srm/2009/11/cloud-security-front-andcenter. html
16. Cloud Security Alliance. http://www.cloudsecurityalliance.org.
17. Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing, V2.1, http://www.cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf.
18. P. Mell and T. Grance, "The NIST Definition of Cloud Computing," NIST, Special Publication 800-145, Sep. 2011. Available: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf
19. H. Leigang and X. Mingqing, "The future of automatic test system (ATS) brought by Cloud Computing," in 2009 IEEE AUTOTESTCON, 2009, pp. 412 –414.
20. S. Zhang, S. Zhang, X. Chen, and X. Huo, "Cloud Computing Research and Development Trend," in Second International Conference on Future Networks (ICFN '10), Sanya, Hainan, China, 2010, pp. 93 –97.
21. C. Gong, J. Liu, Q. Zhang, H. Chen, and Z. Gong, "The Characteristics of Cloud Computing," in 2010 39th International Conference on Parallel Processing Workshops (ICPPW), 2010, pp. 275 –279.
22. M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, and M. Zaharia, "Above the Clouds: A Berkeley View of Cloud Computing," 2009.