INTERNATIONAL JOURNAL OF ADVANCE RESEARCH AND DEVELOPMENT

(Volume3, Issue7)

Available online at: www.ijarnd.com

Cloud computing security issues and challenges

Gowthami K.[1], Dr. Jagadhesan B.[2]

[1]*Student, Dhanraj Baid Jain College, Chennai, Tamil Nadu*

[2]*Associate Professor, Dhanraj Baid Jain College, Chennai, Tamil Nadu*

ABSTRACT

Cloud computing has raised IT to newer limits by contribution the market environment data storage and volume with springy scalable computing processing power to match elastic demand supply, with reducing capital expenditure. Usually cloud computing services are delivered by a third party provider who owns the infrastructure. Cloud computing offers an innovative business model for organizations to adopt IT services without upfront investment. Security is one of the major issues which hamper the growth of cloud. Today, leading players, such as Amazon, Google, IBM, Microsoft and salesforce.com offer their cloud infrastructure for services.

Keywords: *Cloud computing, Cloud security issues, IAAS, PAAS, SAAS*

1. INTRODUCTION

Cloud computing is one of today's most exiting technologies due to its ability to reduce costs associated with computing while increasing flexibility and scalability for computer process. Cloud computing is model that enables convenient, on-demand network access to a shard pool of configurable computing resources such as networks, servers, storage, applications that can be rapidly provisioned and released with minimal management effort or service provider's interaction. There are various reasons for organizations to move towards IT solutions that include cloud computing as they are just required to pay for the resources on consumption basis. Cloud supports large scale user accesses at distributed locations over the internet, offers on-demand application services anytime, and provides both virtual and/or physical applications for customers.

1.1 Characteristics

- Broad- Network Access
- On-demand self service
- Rapid elasticity
- Resource pooling
- Pay-per-use measured service

2. CLOUD COMPUTING SERVICES

2.1 Infrastructure as a Service (Iaas)

Infrastructure as a service is a single tenant cloud layer where the cloud computing vendor's enthusiastic resources are only shard with contracted clients at a pay-per-use fee. In this model, the vendor provides physical computer hardware, including data storage, CPU processing and network connectivity also provides virtual machines and other abstracted hardware and operating systems which may be control though a service API.

IaaS Service providers: Amazon EC2 and S3, Terremark Enterprise Cloud, Windows Live SkyDrive.

2.2 Software as a Service (Saas)

Software as a Service also operates on the virtualised and pay-per-use costing model where by software applications are leased out to contracted organizations by focussed SaaS vendors. This is traditionally accessed remotely using a web browser via the internet. In this model, the vendor provides customers with software applications using their cloud infrastructure and cloud platforms. Saas is software offered by a third party provider.

SaaS Service Providers: Online word processing and spreadsheet tools, CRM services and web content delivery services (Salesforce CRM, Google Docs).

2.3 Platform as a Service (PaaS)

Platform as a service cloud layer works like IaaS but it provides an additional level of "rented" functionality. PaaS lets customers use the vendor's cloud infrastructure to deploy user made web applications/software also allows customers to develop new applications using APIs deployed and configurable remotely. The platforms offered include development tools, configuration management, and deployment platforms.

PaaS Service Providers: Microsoft Azure, Force and Google App engine.

3. CLOUD DEPLOYMENT MODEL

3.1 Private Cloud

Private cloud is a new term that some vendors have recently used to describe offerings that emulate cloud computing on private networks. It can be owned by or leased and managed by the organization or a third party and exist at on-premises or off-premises. It is more expensive and secure when compared to public cloud. Utilization on the private cloud can be much more secure than that of the public cloud because of its specified internal exposure. Only the organization and designated stakeholders may have access to operate on a

specific private cloud. A private cloud is usually managed via internal resources. The terms private cloud and virtual cloud (VPC) are often used interchangeably. Private clouds are often deployed when public clouds are deemed inappropriate or inadequate for the needs of a business.

3.2 Public Cloud

A cloud infrastructure is provided to many customers and managed by exist beyond the company firewall. Public cloud describes cloud computing in the traditional mainstream sense, whereby resources are dynamically provisioned on a fine-grained, third-party provider who shares resources and bills on a fine-grained utility computing basis. In this model, no access restrictions can be applied and no authorization and authentication techniques can be used. Public cloud users share these resources, a model known as a multi-tenant environment. Public cloud users simply make an agreement, use the resources, and pay for what's used at within a certain amount of time.

3.3 Hybrid Cloud

A hybrid cloud is a private cloud linked to one or more external cloud services, centrally managed, provisioned as a single unit, and circumscribed by a secure network. Itprovides virtual IT solutions through a mix of both public and private clouds. The majordrawback to the hybrid cloud is the difficulty in effectively creating and governing such a solution.

4. SECURITY ISSUES OF CLOUD COMPUTING

Security problems faced by the cloud system about in the following aspects:

a) **Security attacks**: Due to vast amounts of user data stored in the cloud systems, for attackers there has greater allure. If the attacker in some way successfully attack cloud systems.

b) **Cloud platform services and high availability of user data and business:** The software itself may have loopholes and a large number of malicious attacks happen, all these above greatly increase the possibility of service interruption. How to product the high availability of software services and user application and how to provide convenience security management to the thin-client user have become one of the biggest challenges of cloud security.

c) **Perfect the cloud standards**: Many manufactures have defined their own application standards and data formats, forcing the user deploying IT system and their own business in accordance with the framework set by different service provider. To a certain extent, the establishment of cloud standards, decides the future evolution of cloud computing.

d) **Virtualization technology**: It only brings cloud computing platform flexibly resources configured, but also brings new security challenges. Once be hacked, all the virtual machines running on the virtualization platform platform will be under control of attackers on that time, the cloud providers and users will suffer huge loss.

e) **The safety and privacy of user data**: User data stored in the cloud system, for malicious attacks, the primary purpose is to get user privacy, and then to obtain economic benefits. Only security system and regulations gradually be perfected and security technology continues to progress, the future of public cloud services will get a sustainable evolution.

f) The above analysis is mostly based on the public cloud. In security issues, private cloud are motley inherited the advantages of cloud computing. The public cloud is still very beneficial to the vast number of small and medium enterprises and individual users.

5. SECURITY CHALLENGES

a) High level security management standards such as honesty, payment, and space to yourself of sensitive information.

b) One of the most serious threats to cloud computing itself comes from HTTP Denial of Service or XML-Based Denial of service attacks. These types of attacks are simple and easy execute by the attacker, but to security experts they are twice as difficult to stop.

c) Security vulnerabilities existing in the cloud environment.

d) **Data production:** Data needs to be encrypted at all times, with clearly defined roles when it comes to who will be managing the encryption keys.

e) **User authentication:** Data resting in the cloud needs to be accessible only by those authorized to do so, making critical to both restrict and monitor who will be accessing the company's data through the cloud. As with all cloud computing security challenges, it's the responsibility of the customer to ensure that the cloud provider has taken all necessary security measures to protect the customer's data and the access to that data.

f) **Disaster and Data breach:** Contingency Planning, the cloud serving as a single centralized repository for a company's mission-critical data, the risks of having that data compromised due to a data breach or temporarily made unavailable due to a natural disaster are real concerns.

g) **Insecure access points:** One of the great benefits of the cloud is it can be accessed from anywhere and from any device.

h) Localize virtual machines and physical servers use the same operating systems as well as venture and web applications in a cloud server environment, increasing the threat of an attacker or malware exploiting vulnerabilities in the systems and applications remotely.

i) In the do too quickly to take advantage of the benefits of cloud computing, not least of which is significant cost savings, many corporations are likely rushing into cloud computing without a serious consideration of the security implications.

.

6. CONCLUSION

The cloud computing model is one of the promising computing models for service providers, cloud providers and cloud clients. Although cloud computing can be seen as a new phenomenon which is set to revolutionise the way we use the internet, there is much to be cautious about. There are many new technologies emerging at a rapid rate, each with technological advancements and with the potential of making human's lives easier.

From this paper, detailed explanation of cloud computing and what is entails. Building on that understanding we proceeded to outline and examine the various security issues that emerge as a result of the structures used in the development of various cloud computing solutions.

7. REFERENCES

[1] [Perry08] Geva Perry, "How Cloud & Utility Computing Are Different", 2008. http://gigaom.com/2008/02/28/how-cloud-utility-computing-are-different.

[2] [Gartner08] Gartner, "Seven cloud-computing security risks, "InfoWorld, July 2, 2008, http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853.

[3] [Rittinghouse09] John Rittinghouse, "Cloud Computing: Implementation, Management, and Security", 2009.

[4] Latif, R., Abbas, H., Assar, S.,Ali, Q., "Cloud computing risk assessment: a systematic literature review", Future Information Technology, pp.285 295, Springer, Berlin, Germany, 2014.,

[5] John Rhoton, "Cloud Computing Protected: Security Assessment Handbook", 2013.

[6] Tinankoria Diaby, Babak Bashari Rad, Cloud Computing: A review of the Concepts and Deployment Models, I.J. Information Technology and Computer Science, 2017, 6, 50-58, DOI:10.5815/ijitcs.2017.06.07.

