International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 05 | May -2017 www.irjet.net p-ISSN: 2395-0072

Security Risks in Cloud Delivery Models

Afshan Sultana[1], Dr K Raghuveer[2]

[1]Afshan Sultana *PG Student (M.Tech), Department of ISE, National Institute of Engineering, Mysore, Karnataka, India*

[2]*Dr K Raghuveer Professor, Dept. of Information Science Engineering, The National Institute Of Engineering, Mysore, Karnataka, India*

Abstract - *Cloud computing, mainly known as "Pay as you go model" is a shared environment for accessing the computer resources and data in the form of various cloud delivery models and charges based on the usage. The cloud system is considered as the hosted service in which a particular user can access the cloud system remotely by using mobile applications or by using the browsers. Although its growing very largely and increasing rapidly, amongst the issues in cloud computing top priority is given to security. As there might be increasing chances of security risks in the cloud delivery models in different ways, such as privacy, authenticity, multitenancy, integrity and confidentiality. This paper addressed about the security risks in cloud delivery models and counter measures for the risks*.

***Key Words*: Cloud computing; Security risks, Delivery models, Virtualization.**

1. INTRODUCTION

The cloud computing technology is growing rapidly because it offers reduction in cost for cloud resources, improved performance monitoring and easy maintenance of cloud application. Cloud computing provides many benefits like less hardware cost, fast deployment, software rental service, lesser cost, elasticity, scalability, low cost recovery and data storage solutions, on-demand security controls, real time detection of system tampering and rapid re-constitution of services [3]. Because of the security issues Cloud service providers must be certain that they get the security flanks right, as they are the one who take the responsibility if the things go wrong in the cloud system [1].The security issues will directly impact on the service models.

The cloud provides different service models based on resource focus[8], they are Software-as-a-Service(SaaS), Platform-as-a Service(PaaS) and Infrastructure-as-a-Service (laaS)[2]. SaaS stands for Software as a service that grants end users to use cloud applications. Gmail is one of the example for SaaS service provided by Google. The next delivery model PaaS stands for Platform as a Service in which developer can develop applications using the programming languages and tools supplied by the cloud provider. Windows azure is one of the example for PaaS service provided by Microsoft. The last service model is IaaS which stands for Infrastructure as a Service, allowing a user to quickly regulate the physical resources for the applications and run any software ranging from the operating systems to applications. Amazon Ec2 is an example for IaaS service provided by Amazon[1]. Security is the main part of the any system. Though the cloud offers the spectacular advantages but there are also some security issues yet to be solved. Many security issues resides in the cloud system that may be access based, network based or delivery based. In this paper we will discuss about the security risks in the Cloud delivery model.

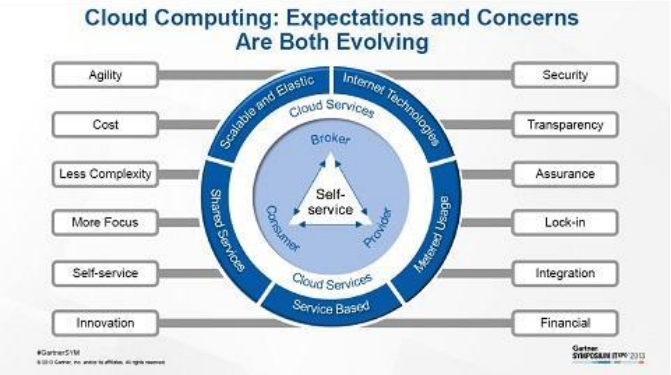

Fig 1- Cloud Computing Expectations and Concerns

The main parameters for security issues of Cloud delivery models are :

1.1 Authentication and Authorization:

Authentication is related to the identity of the user E.g When you log on to your machine and then try to access a resource, say a file server or database, something needs to assure that your username and password are valid. Similarly the authentication in cloud is performed by system of cloud user. This authentication is done by verification of password [3]. Authorization it is right to be given to the particular individual to access the resources and the information. This process is based on the Digital certificate's [3]

1.2 Multitenancy:

Multi-tenancy is an architecture in which a single instance of a software application serves multiple customers. Each customer is called a tenant. Multi-tenancy can be economical because software development and maintenance costs are shared. These shared resources of an organization gives birth to confidentiality issues. These systems and applications must be isolated to some extent in order to keep confidentiality alive. Otherwise it is very difficult to supervise the data flow and the insecurity issues arise [3]

1.3 Integrity:

Data that is stored in the cloud could suffer from the damage on transmitting to/from cloud data storage. Since the data and computation are outsourced to a remote server, the data integrity should be maintained and checked constantly in order to prove that data and computation are intact. The data cannot be modified by any unauthorized user or the process. The data can modified and altered only by the user who is authorized to do so.

1.4 Trust:

Trust is assured alliance on the strength, ability, character of someone or something in the contrast of cloud computing. The customer's has to trust that the organization is capable of providing the required services accurately and infallibly [5].

2. SOFTWARE AS A SERVICE (SAAS)

A Saas is the application service provided by the service provider. Such services are Workflow management, Customer relationship management (CRM) and Desktop software. The user does not have the control over the underlying the cloud infrastructure [4].

Security risks and measures in SaaS are

1.1 Securing the data:

Software as a Service [SaaS] is rapidly emerging as the dominant delivery model for meeting the needs of enterprise IT services. However, most enterprises are still uncomfortable with the SaaS model due to lack of visibility about the way their data is stored and secured. The sensitive data of the enterprise is should be secured against the attacks so the additional security must be provided by SaaS service provider against the following attacks [1].

1.2 Port Scanning:

Port scanning is a technique to identify the open ports in the network by using some network tool such as Nmap. This open port can be used to theft the data. Leads the stealing of the data in the cloud so the service provider must implement the strong encryption techniques on the open ports[1].

1.3 SSL Attack:

Secure Socket layer protocol is used to provide the communication security over the computer network at the transport layer level [5]. Data theft can also happen if the SSL is not properly configured it can be avoided by configure the SSL before the communication of data [1].

1.4 Malware injection:

Malware injection is one category of attack, in which hackers exploit vulnerabilities of application and embed malware into it that changes the course of its normal execution. Malware is malicious code or software it can be remotely injected to the cloud by using the various methods. Results in inserting of the malicious data into to the original data it can countered by using the hashing techniques [1].

1.5 Network sniffing:

Network sniffing is the common term can be used to address the both sniffing of the data and the passwords. It is common and crucial attack in the cloud network so the SaaS is must implemented the good encryption techniques to avoid the data and passwords sniffing over the network [1].

3. PLATFORM AS A SERVICE (PAAS)

The cloud service provider allow the user to deploy the consumer created application and the user having a control over the deployed application configuration but he does not have a control over the underlying cloud infrastructure [4].

Security risks and measures in PaaS are

1.1 Lack of secure software development process:

The PaaS offer the software development lifecycle(SDLC) but the secure software development lifecycle (SSDLC) is not widely used. The lack of SSDLC could lead the insecure code after development [6]. So the PaaS service provider must adopt the SSDLC to avoid the security risks in software development process.

1.2 SLA related risk:

Service level agreement in contrast of cloud computing is a negotiated contract between the customer and the cloud service provider[4] . lack of adequate provisions in SLA is the main risk in PaaS. The Cloud Computing Bill of Rights provides a useful checklist of protection with which to benchmark a supplier's offering [6].

1.3 Disaster Recovery:

Dynamic scalability is a feature that PaaS makes especially easy. Sometimes availability is restricted due not to outages or disasters, but simply due to traffic volumes and responsiveness. Nothing is worse for a public-facing application than slow speeds or unresponsive links. Whenever any catastrophic failure or disaster is happen the it is responsibility to fix or correction only by the PaaS vendor not your IT team's [6].

1.4 Vendor Lock in:

Vendor lock-in also known as customer lock-in it makes a customer dependent on a vendor for products and services. Platform as a Service (PaaS) vendors tend to dictate the database, storage and application framework used. Enterprises will still require the skills and infrastructure to be able to run them [6].

1.5Disaster Recovery:

Whenever any catastrophic failure or disaster is happen the it is responsibility to fix or correction only by the PaaS vendor not your IT team's [6].

4. INFRASTUCTURE AS A SERVICE (IAAS)

In IaaS the cloud user can deploy and run the arbitrary software it may include the operating systems and application [5]. The user does not have full control over the underlying cloud infrastructure but he may have a ability to tweak the some networking elements such as firewall[4].

Security risks and measures of IaaS are

1.1 Virtualization:

The user or the developer has the better control over the security as long as there is no security holes in the virtualization manager. Virtual machines are vulnerable to side channel effects and the buffer overflow attacks [6]. The deployment of insecure or rogue VM's in the VM repository leads into lack of access control. So the IaaS service provider should be taken care of the insecure or rogue VM's

1.2 Physical security:

The Physical security of the IaaS environment such as the physical servers, computer resources and the whole environment of IaaS must be secured by unauthorized entries and the intruders [7].

1.3 Time critical:

Down time due to man mad or nature disaster could introduce significant business risks if the hosted application is critical so the IaaS service provider should take safety measures to avoid the down time [7].

3. CONCLUSIONS

Cloud computing is a nascent and rapidly evolving model, with new aspects and capabilities being announced regularly. Although we have done our best in this paper to provide the security risks that may evolve during your involvement and working with cloud.
Although, cloud computing model is one of the promising computing models for service providers, cloud providers and cloud consumers. But to best utilize the model we need to block the existing security holes. Based on the details explained above this paper

REFERENCES

[1]Navdeep Singh, Abhinav Hans, Ashish Sharma, KapilKumar" unfolding security brawls and concerns of cloud computing "International Conference on Innovative Applications of Computational Intelligence on Power, Energy and Controls with their Impact on Humanity (CIPECH14) 28 & 29 November 2014.

[2]Tina Francis, S. Vadivel "Cloud Computing Security: Concerns, Strategies and Best Practices" Proceedings of 2012 International of Cloud Computing, Technologies, Applications & Management.

[3] Patil Madhubala R. "Survey on Security Concerns in Cloud Computing" 2015 International Conference on Green Computing and Internet of Things (ICGCIoT).

[4] Irfan Hussain and Imran Ashraf "Security Issues in Cloud Computing - A Review" ,Int. J. Advanced Networking and Applications Volume: 6 Issue: 2 Pages: 2240-2243 (2014) ISSN : 0975-0290.

[5] Dan C. Marinescu Cloud Computing: Theory and Practice.

[6]http://en.wikipedia.org/wiki/Transport_Layer_Security.

[7]https://www.owasp.org/index.php/Cloud Top_5_Risks_with_PAAS.

[8] Michael Miller, "Cloud Computing-Web Based Applications that Change the Way You Work and Collaborate Online", Que Publishing, (August 21, 2008) ISBN-10: 0789738031.