IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 2, Ver. V (Mar – Apr. 2015), PP 93-96
www.iosrjournals.org

Internal & External Attacks in cloud computing Environment from confidentiality, integrity and availability points of view

[1]Tayseer TagElsir Ahmed Osman, [2]Dr. Amin babiker A/Nabi Mustafa
Alneelian University

Abstract: *Cloud computing is set of resources and services offered through the Internet. Cloud services are delivered from data centers located throughout the world. Cloud computing facilitates its consumers by providing virtual resources via internet. General example of cloud services is Google apps, provided by Google and Microsoft SharePoint. The rapid growth in field of "cloud computing" also increases severe security concerns. This paper aims to identify security threats in cloud computing, which will enable both end users and vendors to know about the key security threats associated with cloud computing.*

I. Introduction:

Security is one of the major issues which hamper the growth of cloud. The idea of handing over important data to another company is worrisome; such that the consumers need to be vigilant in understanding the risks of data breaches in this new environment. Security has remained a constant issue for Open Systems and internet, when we are talking about security cloud really suffers. Lack of security is the only hurdle in wide adoption of cloud computing. Cloud computing is surrounded by many security issues like securing data. This paper will presented type of threats that effect the cloud computer environment and what's the techniques use to prevent the security .

Technical Components of Cloud Computing:
key functions of a cloud management system is divided into four layers, respectively the Resources & Network Layer, Services Layer, Access Layer, and User Layer. Each layer includes a set of functions:

- The Resources & Network Layer manages the physical and virtual resources.
- The Services Layer includes the main categories of cloud services, namely, NaaS, IaaS, PaaS, SaaS/CaaS, the service orchestration function and the cloud operational function.
- The Access Layer includes API termination function, and Inter-Cloud peering and federation function.
- The User Layer includes End-user function, Partner function and Administration function.

Security as a Service

Security as a Service is more than an outsourcing model for security management; it is an essential component in secure business resiliency and continuity. A security focused provider offers greater security expertise than is typically available within an organization.

Governance and Enterprise Risk Management

A major element of governance will be the agreement between provider and customer (SLA).Risk management is the primary means of decision support for IT resources dedicated to delivering the confidentiality, integrity, and availability of information**.**

Security Threats Originating Between the Customer and the Datacenter

Virtual machines live their lives as disk images that are hosted on a hypervisor platform and are easily copied or transferred to other locations. This mobility is advantageous because it allows VMs to be transported to other physical machines via an image file that defines the virtual disk for that IDENTIFYING CLOUD COMPUTING SECURITY RISKS 69 . Unfortunately, the ability to move and copy VMs poses a security risk because the entire system, applications, and data can be stolen without physically stealing the machine "From a theft standpoint, VMs are easy to copy to a remote machine, or walk off with on a storage device"

Threats for Cloud Service Users

1. Loss of Governance
2. Loss of Trust
3. Unsecure Cloud Service User Access
4. Lack of Information/Asset Management
5. Data loss and leakage

Threats for Cloud Service Providers

1. Evolutional Risks
2. Business Discontinuity
3. License Risks Software
4. Bad Integration
5. Unsecure Administration API
6. Shared Environment
7. Service Unavailability
8. Data Unreliability

Cloud Threats

The threats to information assets residing in the cloud can vary according to the cloud delivery models used by cloud user organizations. Cloud threats were categorized according to the Confidentiality, Integrity and Availability (CIA).Next table below cloud computing threats

Table (1): Cloud Threats

	Threats	Description
Confidentiality		
	Insider user threats: - Malicious cloud provider user - Malicious cloud customer user - Malicious third party user (supporting either the cloud provider or customer organizations)	The threat of insiders accessing customer data held within the cloud is greater as each of the delivery models can introduce the need for multiple internal users
	Threats	Description
	External attacker threats: - Remote software attack of cloud infrastructure - Remote software attack of cloud applications - Remote hardware attack against the cloud - Remote software and hardware attack against cloud user organizations' endpoint software and hardware	All types of cloud delivery model are affected by external attackers. Cloud providers with large data stores holding credit card details, personal information and sensitive government or intellectual property, will be subjected to attacks from groups.
	Data Leakage: - Failure of security access rights across multiple domains - Failure of electronic and physical transport systems for cloud data and backups	A threat from widespread data leakage amongst many, potentially competitor organizations, using the same cloud provider could be caused by human error or faulty hardware that will lead to information compromise.
Integrity		
	Data segregation: - Incorrectly defined security perimeters - Incorrect configuration of virtual machines and hypervisors	The integrity of data within complex cloud hosting environments such as SaaS configured to share computing resource amongst customers could provide a threat against data integrity if system resources are not effectively segregated.
	User access: - Poor identity and access management procedures Data quality: - Introduction of faulty application or infrastructure components	Implementation of poor access control procedures creates many threat opportunities
	Threats	Description
Availability		
	Change management: - Customer penetration testing impacting	The threat of denial of service against available cloud computing resource is

	other cloud customers - Infrastructure changes upon cloud provider, customer and third party systems impacting cloud customers	generally an external threat against public cloud services. The threat can impact all cloud service models as external and internal threat agents could introduce application or hardware components that cause a denial of service. Physical
	Denial of Service threat: - Network bandwidth distributed denial of service - Network DNS denial of service - Application and data denial of service	the threat can impact all cloud service models as external and internal threat agents could introduce application or hardware components that cause a denial of service.
	Physical disruption: - Disruption of cloud provider IT services through physical access - Disruption of cloud customer IT services through physical access - Disruption to third party WAN providers services	The threat of disruption to cloud services caused by physical access is different between large cloud service providers and their customers. These providers should be experienced in securing large data centre facilities and have considered resilience among other availability strategies. There is a threat that cloud user infrastructure can be physically disrupted more easily whether by insiders or externally where less secure office environments or remote working is standard practice

Types of attackers

Many of the security threats and challenges in cloud computing will be familiar to organizations managing in house infrastructure and those involved in traditional outsourcing models. Each of the cloud computing service delivery models' threats result from the attackers that can be divided into two groups:

Table (2): Type of Attackers

Internal Attacks	External Attacks
Is employed by the cloud service provider, customer or other third party provider organization supporting the operation of a cloud service	Is not employed by the cloud service provider, customer or other third party provider organization supporting the operation of a cloud service
May have existing authorized access to cloud services, customer data or supporting infrastructure and applications, depending on their organizational role	Has no authorized access to cloud services, customer data or supporting infrastructure and applications
Uses existing privileges to gain further access or support third parties in executing attacks against the confidentiality, integrity and availability of information within the cloud service.	Exploits technical, operational, process and social engineering vulnerabilities to attack a cloud service provider, customer or third party supporting organization to gain further access to propagate attacks against the confidentiality, integrity and availability of information within the cloud service

II. Conclusion

In any cloud service (infrastructure, software or platform) the end service provider or enterprise will control the access to the services. If these services are being hosted on the cloud, then the cloud provider also needs to protect their network from unauthorized accesses. However, since the cloud provider and the service provider or enterprise is legally different entities, they may in certain cases need to isolate their respective user information. Security efforts to assure confidentiality, integrity and availability can be divided into those oriented to prevention and those focused on detection.

Reference

[1]. Cloud Security Whitepaper , A Briefing on Cloud Security Challenges and Opportunities October 2013.

[2]. International Journal of Security and Its Applications Vol. 6, No. 4, October, 2012.

[3]. Security of Cloud Computing Providers Study. April 2011.

[4]. Identifying Cloud Computing Security Risks February 2011 .

[5]. Security Threats in Cloud Computing Environments1 October 2012.

[6]. Cloud Security Alliance, “Top threats to cloud computing”, Cloud Security Alliance, March 2010.

[7]. Information Security Briefing 01/2010 Cloud computing .

[8]. [8] Secure Cloud Architecture ,Advanced Computing: An International Journal (ACIJ), Vol.4, No.1, January 2013

[9]. [9] Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 8958, Volume-1, Issue-5, June 2012

[10]. [10] External Insider Threat: a Real Security Challenge in Enterprise Value Webs