**Available Online at www.ijcsmc.com**

**International Journal of Computer Science and Mobile Computing**

**A Monthly Journal of Computer Science and Information Technology**

**ISSN 2320–088X**

*IJCSMC, Vol. 4, Issue. 6, June 2015, pg.126 – 130*

**RESEARCH ARTICLE**

# VULNERABILITY, THREATS AND ITS COUNTERMEASURE IN CLOUD COMPUTING

**SK Prashanth, N. Sambasiva Rao**

[1]Associate Professor, IT Dept., Vardhaman College of Engineering, Hyderabad

[2]Professor, CSE Department, SR IT Womens College, Warangal

[1] Sk_p21@yahoo.co.in, [2] snandam@gmail.com

***Abstract - cloud computing is a resource sharing, low cost and offering services to users over Internet on rented base. Such services attract the organization to increase or decrease the resources as per requirement. However, the cloud computing services are provided by third-party which is difficult to maintain data security and adds risk to it. Cloud computing has pros and cons such as flexibility, availability, scalability and security issues respectively. We discuss here, to find vulnerabilities in system and related threats found in the literature in cloud computing as well identifying possible solutions for vulnerability and threats.***

## I. INTRODUCTION

The need of cloud computing is increased and substantial growth in the scientific and business organizations. According to a study by Garner [1] recognized cloud computing as top most in utilizing technology and has seven major risks to be considered before implementing or transforming into cloud model[3]. Even though many reasons are existing for adopted cloud computing , there are also some restrictions in adopting, The major roles for not adopting is security , privacy and legal matters[s],Since for cloud computing new design and models are represented, there exists how far security can be provided in each levels (i.e. network devices , application host and data level).

High security should provide to external data storage dependency on public internet, multi-tenancy and privacy in internal security. Traditional security systems are not enough for cloud to huddle like distributed, heterogeneous and virtualization [2]. Its difficulty for an organization to move its application and sensitivity data into cloud, as it maintained by third-part, which overall customer require the same security and control over their application and sensitivity data and they can meet their service - level agreement.[4]

## II. BENEFITS OF CLOUD COMPUTING

Many businesses, small medium enterprises (SME) moving today either directly (e.g. Google or Amazon) or indirectly (e.g. Twitter) into cloud computing, reasons like

- Low costs –deploying applications in the cloud can be less due to lower hardware costs from more effective use of physical resources.
- Universal access - remotely located employees to access applications or data via the internet.

 

- Up to date software - resent software releases or kept.
- Flexibility users can switch applications fast and easily, using the one that suits their application.

We analyses and cluster or domain the security issues for cloud computing referred as SPI model (SaaS, PaaS, IaaS), identifying the most vulnerability and finding threat in literature refereed in cloud computing. "Vulnerability" refers flaws in software or hardware that may provide an attacker the open door to get into a computer or network and have unauthorized access to resources and term threat refers to any potential attack for misusing information or system. The threat or threat agent is someone like intruder, a process, or employees which identify a particular vulnerability and use it against the organization and exposes confidential information or destroy file integrity. Here we present a list of vulnerability and threat and also distinguish between to cauterize it, to identify what cloud effect the cloud service model by them .

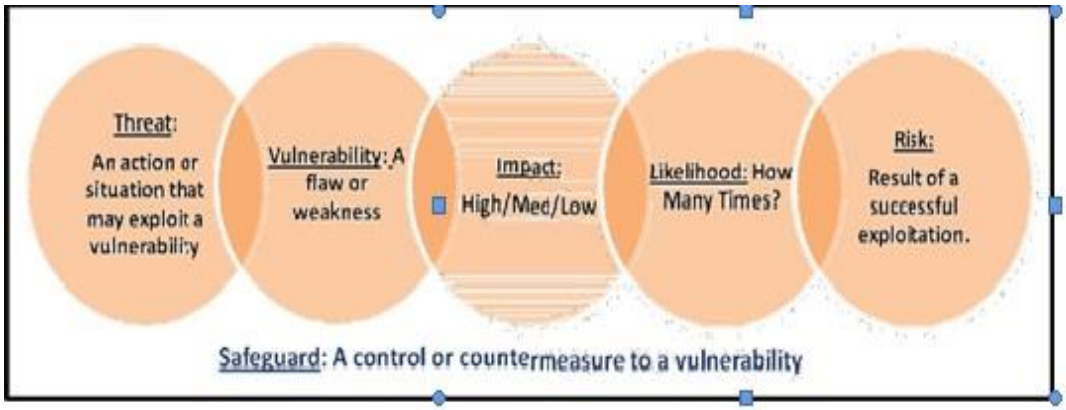


**Figure 1. Risk = Vulnerability x Threat x Impact x Likelihood.**

## III. CLOUD COMPUTING SECURITY IN THE SPI MODEL

There are three major types of service model

- Software as a service (SaaS). Its software distribution model where applications are hosted by a service provider's and made available to customers through network, typically the Internet, accessible from different client devices through a thin client interface such as Web Browsers.

- Platform as a Service (PaaS) .It's a paradigm for delivering operating systems and to deploy onto the cloud Infrastructure without installing any tools and platform or operating system on local machines.

- Infrastructure as a Service (IaaS) .It's capability to involves outsourcing the equipment used to support operations, including storage, hardware, servers networking components and other fundamental computing resources where the client is able to deploy and run different software which have operating system and applications.

 

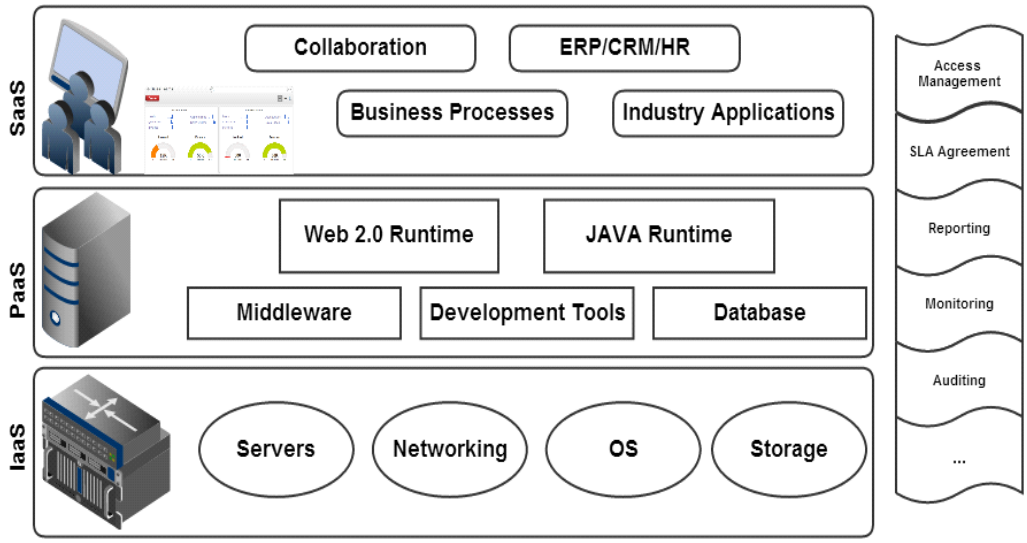


Figure 2. Cloud computing delivery models ( referred from [4,5,6] )

## IV. CLOUD COMPUTING THREATS AND VULNERABILITIES WITH ITS COUNTERMEASURES

The details are taken from resources.infosecinstitute.com and cloud security Alliance (CSA).

### A. Data Breaches

When a virtual machine is able to access the data from another virtual machine or organization's sensitive internal data falls into the hands of their competitors, a data breach occurs. The side-channel attacks are valid attack vectors they attack timing information to extract private cryptographic keys being used in other virtual machines on the same physical server. In multitenant cloud service database is not properly designed, a flaw in one client's application could allow an attacker access not only to that client's data, but every other client's data as well.

*Countermeasure*: while data loss and data leakage are both serious threats to cloud computing, the measures you put in place to mitigate one of these threats can exacerbate the other. You may be able to encrypt your data to reduce the impact of a data breach, but if you lose your encryption key, you'll lose your data as well.

### B. Data Loss

Data loss can be happened in the cloud when data gets into wrong hands while transferring or be lost due to the hard drive failure. A CSP could accidentally delete the data; an attacker might modify the data. Any accidental such as a fire or earthquake, could lead to the permanent loss of customer's data.

*Countermeasure:* Many new compliance policies require organizations to retain audit records, FRC techniques [10], digital signatures [11], encryption [12], and homographic encryption [13] .The provider must takes adequate measures to backup data.

### C. Account Hijacking

Credentials and passwords are often reused to access our account in the cloud by which an attacker gaining access to our account can manipulate and change the data. An attacker having access to the cloud virtual machine hosting our business website can induce a malicious code into the web page to attack users visiting our web page – this is known as the watering hole attack. An attacker can also disrupt the service by turning down the web server serving our website, rendering it inaccessible.

 

*Countermeasures:* Organizations should look to prohibit the sharing of account credentials between users and services, and leverage strong two-factor authentication techniques where possible.

**D. Insecure APIs**

Various cloud services on the Internet are exposed to a set of software interfaces or APIs that customers use to manage and interact with cloud services .Organizations and third parties often build upon these interfaces to offer value-added services to their customers. An attacker gaining a token used by a customer to access the service through service API can use the same token to manipulate the customer's data. Therefore it's imperative that cloud services provide a secure API, rendering such attacks worthless.

*Countermeasure:* Analyze the security models of cloud provider interface and understanding strong authentication and access controls are implemented in concrete transmission with encryption.

**E. Denial of Service**

Denial-of-service attacks are attacks meant to prevent users of a cloud service from being able to access their data or their applications. By forcing the victim cloud service to consume inordinate amounts of finite system resources such as processor power, memory, disk space or network bandwidth, the attacker (or attackers, as is the case in distributed denial-of service (DDoS) attacks) causes an intolerable system slowdown and leaves all of the legitimate service users confused and angry as to why the service isn't responding.

*Counter measure*: cloud providers can force policies to offer limited computational resources.

**F. Malicious Insiders**

malicious insider threat to an organization is a current or former employee, contractor, or other business partner working at cloud service provider , who has or had authorized access to an organization's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems. Since cloud service provides often don't follow the best security guidelines and don't implement a security policy, employees can gather confidential information from arbitrary customers without being detected. An attacker can create a valid account can create a virtual image containing malicious code such as Trojan horse.

*Countermeasure*: Access control framework, image filtering [15].

## V. CONCLUSION

Cloud computing is utilizing the most current technology .The utilization of cloud service by organization seems to be gaining more importance. Cloud computing presents some benefits for user which are discussed in this paper; however it faces incredible security problems which leads to declain in usage of services. The various vulnerabilities and threats explored were examined and some countermeasures were proposed. As technology increases, services of cloud increases which intern leads to some vulnerability and threats which adds risk in cloud computing models. At each model or surrounding each level with specific regard to cloud computing will have to be resolved in future.

## REFERENCES

[1] Gartner Inc Gartner identifies the Top 10 strategic technologies for 2011. Online. Available: http://www.gartner.com/it/page.jsp?id=1454221. Accessed: 15-Jul-2011

[2] Li W, Ping L (2009) Trust model to enhance Security and interoperability of Cloud environment. In: Proceedings of the 1st International conference on Cloud Computing. Springer Berlin Heidelberg, Beijing, China, pp 69–79

 

[3] J. Brodkin, "Gartner: Seven Cloud-Computing Security Risks," InfoWorld, 2008. http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853

[4] Rittinghouse JW, Ransome JF (2009) Security in the Cloud. In: Cloud Computing. Implementation, Management, and Security, CRC Press

[5] D. Chen and H. Zhao, "Data Security and Privacy Protec- tion Issues in Cloud Computing," *International Confe- rence on Computer Science and Electronics Engineering*, Vol. 1, Hangzhou, 23-25 March 2012, pp. 647-651

[6] A. Lenk, M. Klems, J. Nimis, S. Tai and T. Sandholm, "What's Inside the Cloud? An Architectural Map of the Cloud Landscape," *Proceedings of the* 2009 *ICSE Work- shop on Software Engineering Challenges of Cloud Com- puting*, Washington DC, 23 May 2009, pp. 23-31. http://dx.doi.org/10.1109/CLOUD.2009.5071529

[7] Zhang F, Huang Y, Wang H, Chen H, Zang B (2008) PALM: Security Preserving VM Live Migration for Systems with VMM-enforced Protection. In: Trusted Infrastructure Technologies Conference, 2008. APTC'08, Third Asia- Pacific. IEEE Computer Society, Washington, DC, USA, pp 9–18

[8] Cloud Security Alliance (2012) SecaaS implementation guidance, category 1: identity and Access managament. Available: https://downloads.cloudsecurityalliance.org/ initiatives/secaas/SecaaS_Cat_1_IAM_Implementation_Guidance.pdf

[9] Xiao S, Gong W (2010) Mobility Can help: protect user identity with dynamic credential. In: Eleventh International conference on Mobile data Management (MDM). IEEE Computer Society, Washington, DC, USA, pp 378–380

[10] Wylie J, Bakkaloglu M, Pandurangan V, Bigrigg M, Oguz S, Tew K, Williams C, Ganger G, Khosla P (2001) Selecting the right data distribution scheme for a survivable Storage system. CMU-CS-01-120, Pittsburgh, PA

[11] Somani U, Lakhani K, Mundra M (2010) Implementing digital signature with RSA encryption algorithm to enhance the data Security of Cloud in Cloud Computing. In: 1st International conference on parallel distributed and grid Computing (PDGC). IEEE Computer Society Washington, DC, USA, pp 211–216

[12] Harnik D, Pinkas B, Shulman-Peleg A (2010) Side channels in Cloud services: deduplication in Cloud Storage. IEEE Security Privacy 8(6):40–47

[13] Tebaa M, El Hajji S, El Ghazi A (2012) Homomorphic encryption method applied to Cloud Computing. In: *National Days of Network Security and Systems (JNS2)*. IEEE Computer Society, Washington, DC, USA, pp 86–89

[14] Wei J, Zhang X, Ammons G, Bala V, Ning P (2009) Managing Security of virtual machine images in a Cloud environment. In: Proceedings of the 2009 ACM workshop on Cloud Computing Security. ACM New York, NY, USA, pp 91–96

 