ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 2, Issue 1, January 2014

A Survey on Cloud Computing Security Threats and Vulnerabilities

S. Venkata Krishna Kumar[1], S.Padmapriya[2]

Associate Professor, Department of Computer Science, P.S.G College of Arts and Science, Coimbatore, India[1]

Research Scholar, Department of Computer Science, P.S.G College of Arts and Science, Coimbatore, India[2]

Abstract: Cloud computing is using internet the connected computers share the resources, software information and other devices on-demand, from the resource pool of the cloud providers. The main thing that grabs the organizations to adapt the cloud technology is cost reduction through optimized and efficient computing. Though the cloud computing has its advantages many IT companies have expresses concern about critical security issues which threatens them such as data security, unauthorized access of network and use of infected application . The aim of this paper is to make a survey of the major security threats and vulnerabilities affecting Cloud Systems and the possible solutions available to such threats.

Keywords: Cloud Models, Security Threats, Solutions, Vulnerability

I. INTRODUCTION

Cloud Computing is a computing model that enables sharing of resources on-demand with cost effectiveness and location independent. In Cloud systems the customers need not to buy any resources in their own instead they can use the resources from the cloud and they can pay for the resource as per the usage. Cloud computing is a technology that offers many advantages, in that the main drivers of cloud computing is the following

- Cost Saving
- Improved Flexibility
- Better Scalability

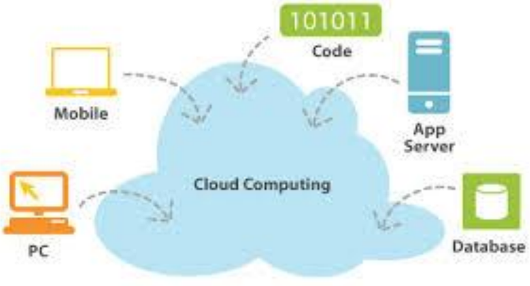

Figure 1: Cloud Computing System

II. CLOUD COMPUTING SERVICE MODELS

A. Infrastructure as a Service (IaaS)
IaaS is the foundation of cloud services. This type of service provides storage space, processing power and managing the organizations Database On-Demand of the particular company.

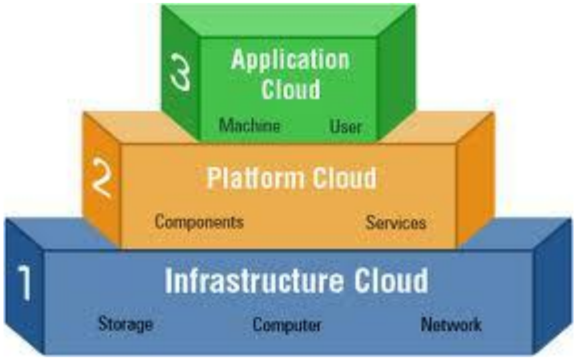

Figure 2: Cloud Models

B. Platform as a Service (PaaS)
Here the platforms or environment needed to develop the applications are provided as a service. The organizations that need a particular environment can buy it from the cloud infrastructure for developing their applications which will run on the provider's infrastructure and release the environment when the work completed.

C. Software as a Service (SaaS)
In SaaS the software applications such as CRM, ERP and some other online applications to manage the organizations are offered as a service. The additional hardware and software's that are required to support the pre made application can be offered by the cloud provider itself. It clears the idea that on customer side there is no need of investment for the extra things either the service we occupy.

III. TYPES OF CLOUDS

A.Public
A public cloud can be accessed by any subscriber with an internet connection which own and operated by a service

provider who hosts the cloud infrastructure with an access control mechanism. All customers share the same resource pool of the cloud provider with limited security and availability of the resources on demand.

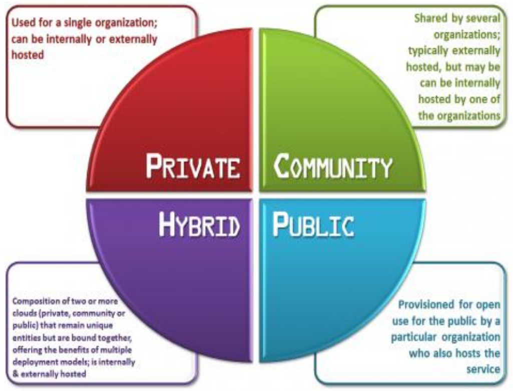
Used for a single organization; can be internally or externally hosted
Shared by several organizations; typically externally hosted, but may be can be internally hosted by one of the organizations
PRIVATE
COMMUNITY
HYBRID
PUBLIC
Composition of two or more clouds (private, community or public) that remain unique entities but are bound together, offering the benefits of multiple deployment models; is internally & externally hosted
Provisioned for open use for the public by a particular organization who also hosts the service

Figure 3: Cloud Types

B .Private

Private cloud is cloud infrastructure delivered to a single organization. The main advantage of private cloud is the protection of the data of user's because they are restricted into the organization data center. It is not shared with other organizations, whether managed by own or by a third-party cloud providers, and it can be hosted internally or externally.

C .Hybrid

Hybrid Clouds are a combination of two or more cloud methods of resource pooling. The Hybrid cloud environment is independent in it but commonly connected through a standard interface.

D .Community

A community cloud is shared among several organizations and that is operated, managed and secured commonly by the group of organizations or a third party service provider.

IV. SECURITY THREATS

A Secure cloud is always a trustworthy source of resources or information's so securing the cloud is a main aspect of the cloud providers who are in charge for the cloud area. Cloud computing security means that securing data from the malicious persons, providing high performance to users, using high quality encryption standards which protect data from the hackers etc. The main problems cloud computing faces are securing confidentiality and integrity of data in terms data security. The CSA (Cloud Security Alliance) has identified the top nine cloud computing threats for 2013 [1].

A. Data Breaches

One of the security threat which is identified as a top threat in a survey conducted by the CSA is data breaches. The concept of data breach is that any malicious person or un authorized person enters into a corporate network and stolen the sensitive or confidential data. The CSA illustrate the amount of risk of this threat by pointing a research paper from last November which describes how a malicious virtual machine can extract the private cryptographic keys of the other virtual machines on the same server.

B. Data Loss

Another serious threat that threatens the CSP is the potential incapacity to prevent data loss because many of the companies treat their data as a valuable asset. In our networked world, most people know that loss of data is unavoidable at one point or another. There is increasing amount of sensitive data which is relayed to cloud computing providers and this data could get lost in any number of ways, including through accidental deletion or corruption of stored data.

C. Account Hijacking

In Account Hijacking a malicious intruder can use the stolen credentials to hijack cloud computing services and they can enter on other's transactions, insert false information, and divert users to abusive web sites which resulted in legal issues for cloud service providers.

D. Insecure application programming interfaces (APIs)

If the Application Programming Interfaces which are used by the users to communicate with the cloud services are weak or not sufficiently secured, accidental or malicious attempt to violate them may expose the cloud data to many security threats related to inflexible access control, scalability and limited monitoring and many other issues.

E. Denial of Service

DoS have become very serious threat when the organizations are dependent on the services for 24/7. It temporarily denies the access of data stored in the cloud to the authorized users by make an attack on the server by sending thousands of requests to it become unable to respond to the regular clients.

F. Malicious insiders

A person who enters into the cloud network to harm the organizations confidential data and assets, damage valuable brands, penalize financial damage, stop productivity is known as a malicious insider.

G. Abuse and Nefarious Use

Network hackers are always developing new technologies to extend their reach by propagating malwares or share the pirated software, escape from being detected, and improve the effectiveness of their activities. Some cloud computing providers who are weak in their security measures such as detecting the intruders are the target of the attackers.

H. Insufficient Due Diligence

CSA's basic advice is for organizations to make sure that they have sufficient resources and to perform extensive due diligence before jumping into the cloud. Due diligence refers to the care a reasonable person should take before entering into an agreement or a transaction with another party.

I. Shared Technology Issues

Cloud computing is known for its sharing technology so it is very difficult to obtain a strong isolation property for multi-tenant architecture. It is the responsibility of the CSP to provide a scalable service to the user without interfering with the other client system.

V. SOLUTIONS

A. Data Breaches

The remedy for the data breach taken by Amazon Web Services is that they isolate all the virtual machines and the data which is resides on AWS and they offer the data to the next customer by wiped off the previous session data completely to prevent any leak of information to the competitors.

B. Data Loss

Data Loss can be prevented by using the Data Loss Prevention (DLP) tool which is used to track the data in motion in the cloud, detect sensitive data stored in our cloud and also data at any end point like personal computer. Enterprise Rights Management (ERM) is a technology which applies Digital Rights Management (DRM) to the corporate documents to control the access rights to sensitive information whether it is inside or outside of the company.

C. Account Hijacking

Prohibit the sharing of account credentials between employees by setting up a protocol which act as a firewall. By implementing a two-factor authentication technique the unauthorized users can be detected. A strong SLA can also be used for protect the Account Hijacking.

D. Insecure application programming interfaces (APIs)

Evaluate the API before using it for the organization cloud risk and ensure that the CSP provide strong access control, authentication and use of encrypted transmission.

E. Denial of Service

The Intrusion Detection System can be used to protect against the DoS attack. The approach the IDS takes place is that each cloud is assigned with a separate ID's and when a specific cloud is under attack then the corresponding ID alert the whole system to prevent others from the attack.

F. Malicious insiders

This type of attack can be prevented by providing different user access level control. All the login credentials are unique and limited to their own space in which they work in their data to prevent the data leakage to the malicious person.

G. Abuse and Nefarious Use

The nefarious use of cloud services can be prevented by introducing an initial registration and validation process before entering into the cloud environment.

Many value added services can be employed to monitor the customers to use their own service without affecting the overall process.

H. Insufficient Due Diligence

Data security measures combined with risk transfer in the form of insurance coverage and the acceptance of taking risk from the cloud service providers is the major solution to this problem.

I. Shared Technology Issues

A strong compartmentalization should be taken to assure that individual customers do not disturb other customers on the shared network. The SLA should ensure remedy for patching and vulnerabilities. The strong authentication methods also reduce the risk.

VI. CLOUD COMPUTING VULNERABILITIES

According to the Open Group's risk taxonomy [11], Vulnerability is the probability that an asset will be unable to resist the actions of a threat agent. Vulnerability exists when there is a difference between the force being applied by the threat agent, and an object's ability to resist that force. In this section, we list out major Cloud specific vulnerabilities, which provide serious problems to Cloud computing.

According to the research conducted in [12] there are several criteria, which can be met by a vulnerability to make it cloud specific.

○ Virtualization, service-oriented architecture and cryptography are examples of core technologies of cloud computing. A Vulnerability is cloud specific if it is frequent and fundamental to these core technologies.

○ Elasticity, resource pooling and pay-as-you go mode are example on the other hand of cloud characteristics [13]. A Vulnerability is cloud specific if its root cause is in one of those characteristics.

○ Another criteria that makes a vulnerability cloud specific is if it hard to implement existing security controls to cloud innovations.

○ The last criteria they mention is that it has to be frequent in established state-of-the-art cloud services

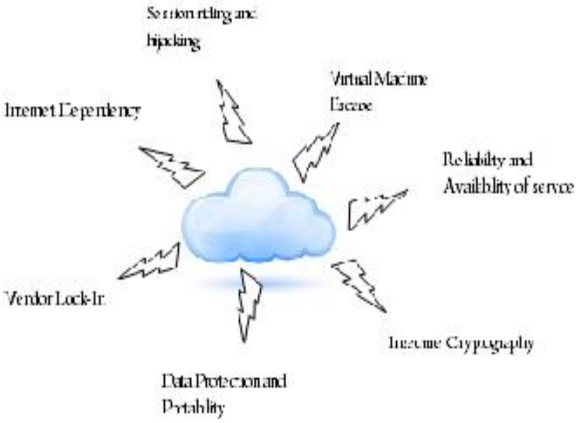
Session riding and hijacking
Virtual Machine Escape
Internet Dependency
Reliability and Availability of service
Vendor Lock-In
Insecure Cryptography
Data Protection and Portability

Figure 4: Seven Vulnerabilities to cloud

Knowing what makes a vulnerability cloud specific one can then identify vulnerabilities in the cloud. The paper [14] has identified in total 7 major vulnerabilities of cloud computing:

A. Session Riding and Hijacking

This vulnerability is related to web applications weaknesses which allow the hackers to perform malicious activities such as session hijacking by using a valid session key gain the unauthorized access into the computer system of the authorized users. On the other hand the session riding refers the act of tricking the user open an email or to visit a harmful website which deletes the user information by sending commands to a web application.

B. Reliability and Availability of Service

When considering this issue cloud computing is not perfect because when building more and more services on top of the cloud infrastructure many internets based services and applications may stop working. The paper [14] gives the example of an event in 2008 when Amazon's Web Service cloud storage infrastructure went down for several hours. This caused data loss and access issues.

C. Insecure Cryptography

For all cryptographic algorithms there is a novel method identified by the attackers to break the cryptography which results in insecurity. It is very common to identify flaws in the cryptographic algorithms which turn a very strong encryption into a weak encryption. The Virtual machines used on the cloud do not have enough sources of entropy and are therefore susceptible to attacks.

D. Data Protection and Portability

This vulnerability is based on the protection of data such that if the client doesn't want to continue the service or if the agreement between the CSP and the client was terminated then what happens to the sensitive data of the client. On the other hand in terms of portability if the provider get out of the business then what will happen to the data of the client and the services which provided by the provider.

E. Virtual Machine Escape

In this type of vulnerability the attacker directly interact with the host operating system by breaking the isolation layer which separate the VM's from the host OS. Through this there is an increase in the attack surface for the attacker.

F Vendor Lock-in

The Lock-in will make the client dependent on the vendor for services. Though the providers not capable of providing good standards of services the client will not switch to another provider because of the principles and policies established before the agreement.

G. Internet Dependency

Cloud Computing is mostly dependent on the internet because all the application interfaces used to connect to the cloud will work only when the internet connection is available. All the services accessed through the web browsers by the users. The question on the dependency is that whether the internet is reliable for the users who have use the cloud for 24 hours such as the Health care industry.

VII. CONCLUSION

Cloud computing provides many benefits like storage capacity, cost reduction and processing power etc. However it has its own security related issues that threaten the organizations to adopt the cloud technology. Many researches are going at present to identify the security threats and the possible solutions to those threats. This paper describes the survey of the available solutions for the threats which are noted as notorious threats by CSA. The main solution obtained to these security threats based on many research papers is that the SLA(Service Level Agreement) between the vendor and the customer, good degree of encryption standards provided by the vendor which protects the data security.

REFERENCES

[1] http://www.cloudsecurityalliance.org/ Top Threats Working Group the Notorious Nine Cloud Computing Top Threats in 2013.
[2] "Introduction to Cloud Computing and Virtualization", Mayank Mishra, Sujesha Sudevalayam PhD Students CSE, IIT Bombay.
[3] "Cloud Computing Security Issues", Florin OGIGAU-NEAMTIU, IT Specialist, The Regional Department of Defense Resources Management Studies, Brasov, Romania.
[4]http://www.cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf.
[5] "Security Issues for Cloud Computing", Kevin Hamlen, Murat Kantarcioglu, Latifur Khan and Bhavani Thuraisingham.
[6] "Cloud Computing Basics", J.SRINIVAS, K.VENKATA SUBBA REDDY, Dr.A.MOIZ QYSER, International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 5, July 2012.
[7] "Security in Cloud Computing", Amar Gondaliya, Information Technology, Hasmukh Goswami College of Engineering, Ahmedabad.
[8] "Survey of Security Issues in Cloud Computing", Uttam Thakore, College of Engineering, University of Florida.
[9] "Cloud Computing Basics", Association of Information Technology Professionals Research and Strategy Advisory Group.
[10] "Facing Security Challenges Head-on", Mr. Daryl Choo, Chief Information Offi cer, FingerTec HQ
[11] http://pubs.opengroup.org/onlinepubs/9699919899/toc.pdf
[12] "Understanding cloud computing vulnerabilities." Security & Privacy, Grobauer, Bernd, Tobias Walloschek, and Elmar Stocker IEEE 9, no. 2 (2011): 50-57.
[13] "A survey of risks, threats and vulnerabilities in cloud computing." Dahbur, Kamal, Bassil Mohammad, and Ahmad Bisher Tarakji. In Proceedings of the 2011 International Conference on Intelligent Semantic Web-Services and Applications, p. 12. ACM, 2011.
[14] T. Schreiber, "Session Riding a Widespread Vulnerability in Today'sWebApplications"[Online],Available:http://www.securenet.de/papers/Session_Riding.pdf, white paper, 2004.
[15] "Secure Cloud Architecture", Kashif Munir1 and Prof Dr. Sellapan Palaniappan , Advanced Computing: An International Journal (ACIJ), Vol.4, No.1, January 2013
[16]http://www.scribd.com/doc/177989110/Seven-Deadly-Threats-and-Vulnerabilities-in-Cloud
[17]http://www.infoq.com/articles/ieee-cloud-computing-vulnerabilities