Research Article Impact Factor: 0.621 ISSN: 2319-507X
Sonali Chavan, IJPRET, 2014; Volume 2 (9): 761-768 IJPRET

INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

NETWORK SECURITY ISSUES IN CLOUD COMPUTING

MS. SONALI R. CHAVAN

Bhartiya, Mahavidhyalaya, Amravati. Ms India

Accepted Date: 27/02/2014 ; Published Date: 01/05/2014

Abstract: Cloud Computing is the technology of distributed data processing in which some scalable information resources and capacities are provided as a service to multiple external customers through Internet technology. A cloud refers to a distinct IT environment that is designed for the purpose of remotely provisioning scalable. and measured IT resources. The term originated as a metaphor for the Internet which is, in essence, networks of network. Providing remote access to a set of decentralized IT resources. The cloud refers to the datacenter hardware and software that supports a client's needs, often in the form of data stores and remotely hosted applications. These infrastructures enable companies to cut costs by eliminating the need for physical hardware, allowing companies to outsource data and computations on demand. This paper focus on the security issues which arise in the cloud: the confidentiality of data, the retrievability and availability of data, and issues surrounding the correctness and confidentiality of computation executing on third party hardware.

Keywords: Cloud Computing, Security, Issues, Challenges, Threat And Countermeasures.

PAPER-QR CODE

Corresponding Author: MS. SONALI R. CHAVAN

Access Online On:

www.ijpret.com

How to Cite This Article:

Sonali Chavan, IJPRET, 2014; Volume 2 (9): 761-768

INTRODUCTION

From initial concept building to current actual deployment, cloud computing is growing more and more mature. Nowadays many organizations, especially Small and Medium Business (SMB) enterprises, are increasingly realizing the benefits by putting their applications and data into the cloud. The adoption of cloud computing may lead to gains in efficiency and effectiveness in developing and deployment and save the cost in purchasing and maintaining the infrastructure.[8] Cloud computing is a new variation of traditional distributed computing and grid computing. The development of cloud computing is still facing enormous challenges. A major concern is about data security, that is, how to protect data from unauthorized users and leakage [5]

II. SECURITY ISSUES IN CLOUD COMPUTING

A. Security Stack in cloud computing Iaas, Paas , Saas:-

Lower down the stack the cloud vendor provides, the more security issues the Consumer has to address or provide.

B. Security Issues in SaaS:-

Following key security element should be carefully considered as an Integral part of the SaaS deployment process:

- *Data Security*
- *Network Security*
- *Data locality*
- *Data integrity*
- *Data access*
- *Data Segregation*
- *Authorization and Authentication*
- *Data Confidentiality.*
- *Data Breaches*
- *Virtualization vulnerability*
- *Availability*
- *Backup*

C. Security Issues in PaaS:-

- In PaaS, the provider might give some control to the people to build applications on top of the platform. But any security below the application level such as host and network intrusion prevention will still be in the scope of the provider.
- Applications sufficiently complex to leverage an Enterprise Service Bus (ESB)
- need to secure the ESB directly, leveraging a protocol such as Web Service (WS) Security (Oracle, 2009).The ability to segment ESBs is not available in PaaS environments. Metrics should be in place to assess the effectiveness of the
- Application security programs.
- Hackers are likely to attack visible code, including but not limited to code running in user context. They are likely to attack the infrastructure and perform extensive black box testing. The vulnerabilities of cloud are not only associated with the web applications but also vulnerabilities associated with the machine-to-machine Service Oriented Architecture (SOA) applications[10].

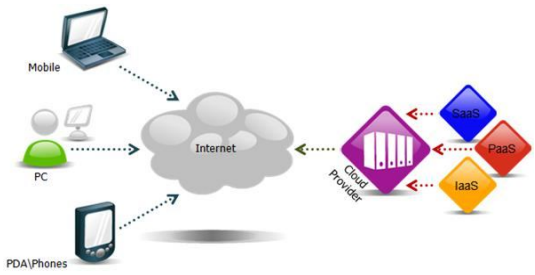

Fig. IaaS , PaaS, SaaS

D. Security Issues in IaaS:-

Taking virtual machines, which contain critical applications and sensitive data, off premise to public and shared cloud environments creates security challenges for organizations that have relied on network perimeter defense as the main method to protect their datacenter. It may also revoke compliance and breach security policies. OS Security issues also alive in IaaS. Following are the points which are considered in IaaS[10].

E. Security Attacks in Cloud:-

- Denial of Service (DoS) attacks: Some security professionals have argued that
- the cloud is more vulnerable to DoS attacks, because it is shared by many users,

- which makes DoS attacks much more damaging. Twitter suffered a devastating
- DoS attack during 2009.
- placing a malicious virtual machine in close proximity to a target cloud server and
- then launching a side channel attack.
- Authentication attacks: Authentication is a weak point in hosted and virtual
- services and is frequently targeted. There are many different ways to authenticate users; for example, based on what a person knows, has, or is. The mechanisms used to secure the authentication process and the methods used are a frequent target of attackers.
- Man-in-the-middle cryptographic attacks: This attack is carried out when an
- attacker places himself between two users. Anytime attackers can place themselves in the communication's path, there is the possibility that they can intercept and modify communications.
- *Network Security*:

1. Network penetration and packet analysis
2. Session management weaknesses
3. Insecure SSL trust configuration.

- Web Application Security:-

1. Injection flaws like SQL, OS and LDAP injection
2. Cross-site scripting
3. Broken authentication and session management
4. Insecure direct object references
5. Cross-site request forgery
6. Insecure cryptographic storage
7. Failure to restrict URL access
8. Insufficient transport layer protection
9. Un-validated redirects and forwards Cloud 20/20 Version 3.

III. CLOUD SECURITY CHALLENGES:

A. Administrative Access To Servers And Applications:-

One of the most important characteristics of cloud computing is that it offer "selfservice" access to computing power, most likely via internet. In traditional Datacenters, administrative access to servers is controlled and restricted to direct or on-premise connections. In cloud computing, this administrative access must now be conducted via internet, increasing exposure and risk. It is extremely important to restrict administrative access and monitor this access to maintain visibility of changes in the system control.

B. Dynamic Virtual Machines:[VM State and Sprawl]:-

Virtual machines are dynamic. They can quickly be reverted to previous instances, paused and restarted, relatively easily. They can also readily clone and seamlessly moved between physical servers. This dynamic nature and potential for VM sprawl makes it difficult to achieve and maintain consistent security. Vulnerabilities or configuration errors may be unknowingly propagated. Also, it is difficult to maintain an auditable record of the security state of a virtual machine at any given point in time. In the cloud computing environments, it will be necessary to be able to prove the security state of a system, regardless of its location or proximity to other, potentially insecure virtual machines.

C. Vulnerability Exploits and VM-to-VM attacks:-

Cloud computing servers use the same operating systems. Enterprise and webapplications as localized virtual machines and physical servers. The ability for anattacker or malware to remotely exploit vulnerabilities in these systems and applications is a significant threat to virtualized cloud computing environments. InAddition co-location of multiple virtual machines increases the attack surface andRisk of VM-to-VM compromise. Intrusion detection and prevention system need to be able to detect malicious activity at the VM level regardless of the location of the VM within the virtualized cloud environment.

IV. SECURITY THREATS OF CLOUD COMPUTING

Cloud computing is an emerging technology with shared resources and lower cost that relies on pay per use according to the user demand. Due to its characteristics, it may face lots of threats and problems in the scopes of security. In this section, these issues are explained below

A. *Threats to cloud computing discovered by "Cloud Security Alliance" (CSA) [6]:-*

Cloud Security Alliance is a renowned community in the scope of cloud security. It has proposed the biggest security threats of cloud systems.

B. Security Problems Concerning Location of the Cloud Systems:-

Some problems are inherited from the specific features of cloud computing. In cloud computing system, data storages are spread around the world.

C. Cloud Challenges Inherited From Network Concept:-

There are some dangerous types of threats which are not specific to cloud environment, but lunched vastly in cloud Systems due to the characteristics of cloud systems and their generality at present.

D. Inevitable Cases of Information Disclosure:-

There are some activities done in cloud environment that fail to protect the information to be disclosed to government.

E. Other Common Security Threats:-

- *Investigation*

Investigating an illegitimate activity may be impossible in cloud environments. Cloud services are especially hard to Investigate , because data for multiple customers may be co-located and may also be spread across multiple datacenters.

- *Data Segregation*

Data in the cloud is typically in a shared environment together with data from other customers. Encryption cannot be Assumed as the single solution for data segregation problems. In some situations, customers may not want to encrypt Data because there may be a case when encryption accident can destroy the data.

- Long-term Viability

Service providers must ensure the data safety in changing business situations such as mergers and acquisitions. Customers must ensure data availability in these situations. Service provider must also make sure data security in Negative business conditions like prolonged outage etc.[7]

V. SECURITY COUNTER MEASURES:-

There numerous ways in which cloud computing can expand on the issue of security. For example, Qualys Guard is a Compilation of products that are used to discover network weaknesses. It is used by over 200 companies in Forbes Global 2000, so it acquired significant acceptance in the marketplace. So beside all these threats, there are lots of Techniques to leverage the security to an acceptable level. This paper basically focuses on these techniques.

A. GENERAL SECURITY COUNTERMEASURES:-

This section provides the research for general security issues in the cloud computing environment.

- *Architecture security*

Cloud computing security challenges can be handled practically by performing security assessment [24]. An Architecture ontology approach for secure cloud computing is defined by Kelvin Jackson [25]. The architecture of cloud includes various security components like Access Management, Security API, Network Security and Storage Security. These components embedded in the cloud architecture to provide secure cloud computing.

- *Data Security*

Privacy in terms of legal compliance and user trust, data leakage for sensitive data are provided. Ji Hu Klein gave a Benchmark to secure data-in-transit in the cloud. Large scale search system for the purpose of Information exchange Between internets communities leads to formation of covert Channels. An agent based security model to control Data from covert channel is presented. It may solve the problem of data leakage in the cloud environment.

- *CAPTCHA Breaking*

Integration of multiple authentication techniques along with CAPTCHA identification (as adopted by companies like Face book, Google etc.) may be a suitable option against CAPTCHA breaking. Various techniques such as: Implementing letter overlap, variable fonts of the letters used to design a CAPTCHA, increasing the string length and using a perturbative background can be used to avoid CAPTCHA breaking. Single frame zero knowledge CAPTCHA design principles have been proposed, which will be able to resist any attack method of static optical Character recognition (OCR).[7]

VI. CONCLUSION:-

Paper is based on the Security Issues, Challenges, Security Treats and its Countermeasures. Security concerns are an active area of research and experimentation. Lots of research is going on to address the issues like network security, data protection, virtualization and isolation of resources. Addressing these issues requires getting confidence from user for cloud applications and services. Obtaining user confidence can be achieved by creating trust for cloud resource and applications, which is a crucial issue in cloud computing. A number of new challenges that is inherently connected to the new cloud paradigm has also been deliberated in the paper.

VII. REFERENCES:-

1. Kwang Mong Sim Senior Member, IEEE "Agent-Based Cloud Computing."

2. Amar Gondaliya Information Technology Hasmukh Goswami College of Engineering, Ahmedabad." Security in Cloud Computing."

3. Kangchan Lee" Security Threats In Cloud Computing Environments" International Journal of Security and Its Applications Vol. 6, No. 4, October, 2012

4. Anthony Bisong1 And Syed (Shawon) M. Rahman2" An Overview Of The Security Concerns In Enterprise Cloud Computing", International Journal Of Network Security & Its Applications (IJNSA), Vol.3, No.1, January 2011.

5. Rashmi, Dr. G.Sahoo, Dr. S.Mehfuz." Securing Software As A Service Model Of Cloud Computing: Issues And Solutions", International Journal On Cloud Computing: Services And Architecture (IJCCSA), Vol.3, No.4, August 2013

6. Kevin Hamlen, Murat Kantarcioglu, LatifurKhan3, Bhavani Thuraisingham4," Security Issues for Cloud Computing", International Journal Of Information Security And Privacy, 4(2), 39-51, April-June 2010.

7. Vahid Ashktorab, Seyed Reza Taghizadeh," Security Threats And Countermeasures InCloud Computing", International Journal Of Application Or Innovation In Engineering & Management (IJAIEM), Issue 2, October 2012 ISSN 2319 – 4847

8. Deyan Chen, Hong Zhao," Data Security and Privacy Protection Issues In Cloud Computingdata Security and Privacy Protection Issues In Cloud Computing", 2012 International Conference On Computer Science And Electronics Engineering

9. Mladen A. Vouk, Department Of Computer Science, North Carolina State University, Raleigh, North Carolina, USA," Cloud Computing Issues, Research And Implementations", Journal Of Computing And Information Technology CIT 16, 2008, 4, 235–246 Doi:10.2498/Cit.1001391.

10. Ramgovind S, Eloff MM, Smith E," The Management Of Security In Cloud Computing".

11. Pankaj Arora, Rubal Chaudhry Wadhawan, Er. Satinder Pal Ahuja3," Cloud Computing Security Issues In Infrastructure As A Service", International Journal Of Advanced Research In Computer Science And Software Engineering ,Volume 2, Issue 1, January 2012 ISSN: 2277 128X

12. Anthony Bisong and Syed (Shawon) M. Rahman, "An Overview Of The Security Concerns In Enterprise Cloud Computing", International Journal Of Network Security & Its Applications (IJNSA), Vol.3, No.1, January 2011.