International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163
Issue 9, Volume 2 (September 2015) www.ijirae.com

# Security challenges and issues in Cloud Computing – The way ahead

Prof.Rajesh Kumar Kashyap
*M.C.A. Department*
*Z.E.S's ZIBACAR, Pune-41*

Dr.Sarika Sharma
*Director-MCA*
*JSPM's EICA, Wagholi, Pune*

***Abstract:- Cloud computing as a technology facilitates large scale, on-demand and flexible infrastructure to cope up with the needs of the scaling requirements of the IT organizations. Organizations which are using cloud infrastructure have understood the need of security measures to be embedded in the innovative technology of cloud without which the potential of cloud cannot be exploited to the fullest manner. The large scale of adoption of cloud computing has introduced new kind of risks to the existing risks which are already pertinent in the systems. Since cloud is, a combined space where everything is put in a single box like structure it will indeed provide an opportunity for the hackers and intruders to make their attempts in an easier way. This researcher paper focuses on the overview and study of cloud computing with special reference to security challenges in the emerging area of cloud computing and the measures being employed to thwart the challenges and the future trends of cloud computing.***

***Keywords: Cloud Computing, Security, Infrastructure, Vulnerabilities,***

## 1. INTRODUCTION

Cloud computing which is one the most discussed IT innovations in the recent past in the IT sector as well as other sectors also. The cloud-computing bug has bitten most IT companies who either plan or have products, which are relating to the cloud-computing paradigm. The technology of cloud computing is still not mature enough to the extent that security issues in cloud computing is in itself is a critical flaw in this technology [1][2]. As when the technology is growing the concern for security exploitation is also growing due to the increasing vulnerabilities which are being compromised by intruders which are going to increase the research in this domain to a large extent. The idiosyncratic requirements and capabilities regarding privacy and security issues that this new paradigm rises has given researchers a new scope and way ahead in the cloud computing security discipline which has been evolving on a constant basis and there is a growing concern in developing new models.

At a technical level, the growing attacks by intruders and the hacking attempts in cloud computing has given a new set of challenge to cloud computing security. The existing set of security criteria is not enough to cope up to the specific security threats and vulnerabilities of services and service-oriented architectures because of which the attacks have been increasing for so ever. This work –in- progress is aimed at giving preliminary solutions to many of the classes of security issues which are on the rise and focus of providing solutions based on the notion as when as the attack surfaces.

## II. CLOUD COMPUTING SECURITY

Cloud Security Alliance (CSA), an organization dealing with security issues in cloud computing during its RSA Conference held in San Francisco, 2013 has identified 9 top threats to cloud computing and discussed in detail about how to tackle them. The conference report names these threats as the 'Notorious Nine' and the notorious nine are as follows:

1. Data breaches
2. Data loss
3. Traffic hijacking
4. Insecure interfaces and API's
5. Denial of Service
6. Malicious insiders
7. Cloud abuse
8. Insufficient due diligence
9. Technology vulnerabilities

## III. ISSUES IN CLOUD

**Cloud Security Issues and Challenges:**

Due to the ever-increasing malicious attacks by external users, the availability of cloud services and resources take a hit. Some of the activities, which are done, are Port scanning, IP spoofing, DNS poisoning and Phishing are done to gain access of cloud resources. Packet Sniffing is an activity done by malicious users to analyze the data packets sent over a cloud.

 

When a malicious user impersonates a legitimate users IP address to access information through the use of that IP address an IP Spoofing occurs. In case of the exhaustion of host servers which is caused by malicious users resulting in legitimate users not gaining access to resources, it results in a loss of cost to the company as well time. When external users can cause so much damage it is easy for internal users who are authorized to gain access to resources without being detected. An Insider has higher privileges and higher access with respect to network, security , mechanism and resources for them to attack and cause more damage than caused by an external users.

**Vulnerabilities in the cloud:**

Vulnerabilities in a cloud are defined as the loop holes in the security architecture of the cloud, which can be exploited by malicious users to gain access to the cloud network and the resource infrastructure.
The major cloud specific vulnerabilities are:

- Insecure Interfaces and Application Programming Interfaces
- Malicious Insiders
- Virtualized Technology
- Data Loss or Leakage
- Account or Service Hijacking
- Unknown Risk Profile
- Session Riding and Hijacking
- Virtual Machine Escape
- Reliability and Availability of Service
- Insecure Cryptography
- Data Protection and Portability
- Vendor Lock In

## IV. SECURITY CONCERN

Some of the major security concerns with the cloud are given below:
1) Legal issues arising to non-adherence to the law of the land in case of foreign countries.
2) Incompatible with one storage vendor's services with another vendor's services if user decides to move from one to the other [9].
3) The encryption/decryption keys are controlled by whom? Is it the customer or the Service Provider?
4) The transfer, storage, and retrieval which is called as the integrity of data has to be ensured.
5) What kind of data can be stored about the citizens of the country and for how long has regulations of the government which have to be adhered to? Also in the case of Bank regulators who require that customer's financial data remain in their home country.
6) In case of violations of privacy rights, customers have the option of taking legal action against service providers which may cause a dent in their reputation.
7) Since in a cloud sharing of resources happen, and there is no control of where the resources run, the physical control of cloud security is compromised.
8) The consistency of security as well as ensuring the audit ability of records is difficult to maintain because of the dynamic and fluidic nature of virtual machines.
9) In case of Payment Card Industry Data Security Standard (PCI DSS) data logs must be provided to security managers and regulators. [10][11[12]
10) It is imperative for users to keep them up to date with application improvements to be sure they are protected.

## V. APPROACHES FOR SECURITY ISSUES IN CLOUD COMPUTING

Following approaches can be helpful to secure cloud computing-

- **Investigation Support:** The storage, protection, usage and policy enforcement can be ensured by audit tools which are provided to the users, but the actual investigation of illegal activity is quite difficult owing to the reason that data for multiple users may not be easily collated and geographically spread across a set of hosts and data centers and the best way to avoid this is to make the audit tools contractually committed along with the substantiating evidence.
- **Network Security**: IP spoofing is being used by users to deny any internet based service and it may result in security vulnerability prone to harm [6]. This can be avoided by using a digital signature. The best method to encounter the problem of repsurce hacking is to use a SSL protocol.

 

- **Encryption Algorithm:** An encryption algorithm is an effective way to encrypt the user's information by service providers to add to security but in case of an accident to the encryption it may result in making the data totally unusable and leads to the complication of the availability of the data [6]. The best way to solve this problem is to ensure that encryption scheme were designed and tested by experienced specialists.
- **Backup:** Data backup is most critical because the advent of any natural disaster may lead to damage of physical devices leading to a data loss.
- **Customer satisfaction:** Since a provider has facility spans across multiple levels and spread across the globe it is impossible for the end user to actually verify the currently implemented security measures adopted by the service provider as well as the initiatives as implemented [8]. A certification from a n institute which is authenticated for standardization of this measure would solve the purpose.

## VI. SECURITY MANAGEMENT MODEL (CMM)

The recommended security management models and their requirements for cloud computing that cloud service providers should definitely consider as they develop or refine their compliance programs are discussed below:

**1)** ***Security management (People):***

- Developing a formal charter for the security organization and program.
- Clearly defined roles will ensure in clear understanding of what is expected of all team members.

**2)** ***Security governance:***

- A security steering committee should be developed whose objective is to focus on providing guidance about security initiatives and alignment with business and IT strategies.

**3)** ***Risk management:*** Risk management entails identification of technology assets [15]; identification of data and its links to business processes, applications, and data stores; and assignment of ownership and custodial responsibilities. Actions should also include maintaining a repository of information assets. Owners have authority and accountability for information assets including protection requirements, and custodians implement confidentiality, integrity, availability, and privacy controls.

**4)** ***Risk assessment:*** Security risk assessment is critical to helping the information security organization make informed decisions when balancing the dueling priorities of business utility and protection of assets [16][17]. A formal information security risk management process should proactively assess information security risks as well as plan and manage them on a periodic or as -needed basis. More detailed and technical security risk assessments in the form of threat modeling should also be applied to applications and infrastructure.

**5)** ***Data governance:*** This framework should describe who can take what actions with what information, and when, under what circumstances, and using what methods.

**6)** ***Virtual machine security:*** In the cloud environment, physical servers are consolidated to multiple virtual machine instances on virtualized servers. Not only can data center security teams replicate typical security controls for the data center at large to secure the virtual machines, they can also advise their customers on how to prepare these machines for migration to a cloud environment when appropriate.

**7)** ***Disaster recovery:*** In the SaaS environment, customers rely heavily on 24/7/365 access to their services and any interruption in access can be catastrophic. Using the virtualization software virtual server can be copied, backed up, and moved just like a file (live migration).

**8)** ***Third party risk management:*** Lack of a third-party risk management program may result in damage to the provider's reputation, revenue losses, and legal actions should the provider be found not to have performed due diligence on its third-party vendors.

**9)** ***Vulnerability assessment:*** Classifies network assets to more efficiently prioritize vulnerability-mitigation programs, such as patching and system upgrading.

**10)** ***Security image testing:*** Virtualization-based cloud computing provides the ability to create "Test image" VM secure builds and to clone multiple copies. Gold image VMs also provide the ability to keep security up to date and reduce exposure by patching offline. Offline VMs can be patched off-network, providing an easier, more cost-effective, and less production-threatening way to test the impact of security changes.

## VII. CONCLUSION AND FUTURE WORK

This paper is an attempt to discuss about cloud computing security issues and Challenges. An effort is made to analyze cloud computing vulnerabilities, security threats cloud computing faces and presented the security objective that need to be achieved. It is seen that security-sensitive applications of a Cloud computing require high degree of security but it is seen that, cloud computing are inherently vulnerable to security attacks. Therefore, it is imperative to make them more secure and robust to adapt to the demanding requirements of these networks. As we can see the present situation, which shows that there is a general trend in cloud, computing is toward mesh architecture and large scale.

 

There is a demand for improvement in bandwidth and capacity is required, which implies the need for a higher frequency and better spatial spectral reuse. The growing paradigm of Cloud based technologies is another challenging issue in the near future, which can be already foreseen.

## REFERENCES

[1]. Ricardo vilaca, Rui oliveira 2009. Clouder: A Flexible Large Scale Decentralized Object Store. Architecture Overview. Proceeding of WDDDM '09
[2]. Michael Miller. 2009. Cloud Computing-Web Based Application that change the way you collaborate online. Publishing of QUE, 2nd print.
[3]. National Institute Of Standard and technology. csrc.nist.gov/groups/ SNS/cloud-computing/cloud-def-v15.doc, 2009
[4]. Open Security Architecture http://www.opensecurityarchitecture.org/
[5]. Tim Mather, Subra Kumaraswamy, Shahed Latif, "Cloud Security and Privacy : An Enterprise perspective of Risks"
[6]. GregBoss, Padma Malladi, Dennis Quan, Linda Legregni and Harold hall 2007. "Cloud- Computing". Available from www.ibm.com/developerworks/websphere/zones/hipods/.
[7]. Anthony T.Velte, Toby J.Velte and Robert Elsenpeter 2010. Cloud Computing- A Practical Approach". Publishing of Tata McGRAW Hil.
[8]. Nils Gruschka and Meiko Jensen, "Attack Surfaces: A Taxonomy for Attacks on Cloud Services". IEEE rd International Confrence on Cloud Computing,2010.
[9]. M. Casassa-Mont, S. Pearson and P. Bramhall, "Towards Accountable Management of Identity and Privacy: Sticky olicies and Enforceable Tracing Services", Proc. DEXA 2003, IEEE Computer Society, 2003, pp. 377- 382 https://www.pcisecuritystandards.org/index.shtml
[10]. http://en.wikipedia.org/wiki/Payment_Card_Industry_Data_ Security_Standard ", 24 January 2010
[11]. J. Salmon, "Clouded in uncertainty – the legal pitfalls of cloud computing",24 Sept 2008,
[12]. http://www.computing.co.uk/computing/features/2226701/clouded- uncertainty- 4229153
[13]. Krešimir Popović, Željko Hocenski," Cloud computing security issues and challenges", MIPRO 2010, May 24-28, 2010, Opatija, Croatia
[14]. Gartner: Seven cloud-computing security risks, 02 July 2008 http://www.infoworld.com/d/security-central/gartnerseven-cloud-computing-security-risks-853?page=0,0
[15]. Wikipedia, 6 February 2010, http://en.wikipedia.org/wiki/Risk_management
[16]. Wikipedia, 27 January 2010, http://en.wikipedia.org/wiki/Risk_assessment
[17]. D.Catteddu, Giles Hogben : European Network and Information Security Agency, November 2009, http://www.enisa.europa.eu/act/rm/files/deliverables/cloudcomputing-risk-assessment

 