International Journal of Technical Research and Applications e-ISSN: 2320-8163,
www.ijtra.com Volume 3, Issue 6 (November-December, 2015), PP. 23-25

SECURITY CHALLENGES AND ISSUES FACED IN CLOUD COMPUTING

Sudhanshu Garg
Department of Computer Science, Srm University
Chennai, Tamilnadu, India
Sudgarg94@gmail.com

Abstract— **Cloud computing as a technology facilitates massive scale, on-demand and adjustable infrastructure to cope up with the need of the scaling requirements of the IT organizations. The large scale of adoption of cloud computing has introduced new kind of risks to the present risks that are already pertinent within the systems. Since cloud is, a combined area where everything is placed in an exceedingly single box like structure it'll so offer a chance for the hackers and intruders to create their attempts in an easier manner. This research paper focuses on the analysis and study of cloud computing with special regard to security challenges within the rising area of cloud computing and the measures being employed to thwart the challenges and also the future trends of cloud computing.**

Index Terms: **Cloud Computing, Security Challenges, Issue in Cloud Computing.**

I. INTRODUCTION

Cloud computing is one of the most discussed IT innovations in the recent past in the IT sector and in other sectors also. The cloud-computing bug has bitten most IT companies who either plan or have products, which are about the cloud-computing paradigm. The technology of cloud computing is yet not complete 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 expanding due to the increasing vulnerabilities, which are being compromised by intruders, which are going to escalate the research in this domain to a huge extent. The distinctive 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 that has been expanding on a regular basis and there is a increasing concern in developing new models. At a technical level, the increasing attacks by intruders and the hacking attempts in cloud computing has provided a new set of challenge to cloud computing security. The current set of security criteria is not enough to cope up to the explicit 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 prior solutions to many of the classes of security issues which are on the rise and target of providing solutions based on the notion as when as the attack surfaces.

II. CLOUD COMPUTING SECURITY

Cloud Security Alliance (CSA), a corporation dealing with security problems in cloud computing during its RSA Conference held in San Francisco, 2013 has identified 9 top threats to cloud computing and discussed in detail regarding a way to tackle them. The conference report names these threats as the 'Notorious Nine', which 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. Cloudabuse
8. Insufficient due diligence
9. Technology vulnerabilities

III. ISSUE IN CLOUD

A. Cloud Security Issues and Challenges:

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

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

B. Vulnerabilities in the cloud:

Vulnerabilities in a cloud are defined as the loopholes 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 main 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 choose to move from one to the other.

3) Who controls the encryption/decryption keys? Is it the customer or the Service Provider?

4) The transfer, storage, and retrieval, which is said, as the integrity of data has to be ensured.

5) What kind of data can be saved about the residents 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 needs that customer's financial data remain in their home country?

6) In any case of violations of privacy rights, customers have the right of taking legal action against service providers, which may cause a dent in their fame.

7) Since in a cloud sharing of resources happens, and there is no control of where the resources run, the physical control of cloud security is compromised.

8) The firmness of security as well as assuring the audit ability of records is burdensome 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 given to security administrator and governor.

10) It is crucial for users to stay them up to date with application enhancements to make sure they're protected.

V. APPOACHES FOR SECURITY ISSUE IN CLOUD COMPUTING

Following approaches can be useful to secure cloud computing -

- Investigation Support: The storage, protection, usage and policy imposition can be ensured by audit tools that are given to the users, however the particular investigation of illegal activity is sort of difficult owing to the reason that information for multiple users might not be simply collated and geographically spread across a group of hosts and data centers and this can be avoided by making the audit tools contractually committed beside the substantiating evidence.

- Network Security: Users to deny any web-based service are using IP spoofing and it might result in security vulnerability prone to damage [5]. Using a digital signature can avert this. The simplest technique to solve the problem of resource hacking is to use a SSL protocol.

- Encryption Algorithm: An encryption algorithm is an efficient method to cipher the user's information by service providers to add to security however in case of an accident to the encryption it might result in making the data entirely unusable and leads to the complication of the provision of the data [6]. The best technique to handle such a problem is to make sure that encryption scheme were designed and tested by experienced specialists.

- Backup: Data backup is most crucial because in the case of any natural disaster might cause damage to physical devices resulting in data loss.
- Customer fulfillment: As a supplier has facility spans across multiple levels and spread across the world, it is not possible for the end user to actually verify the currently enforced security measures adopted by the service provider as well as the initiatives as enforced. A certification from an institute, which is genuine for standardization of this measure, would solve the aim.

VI. SECURITY MANAGEMENT MODEL

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

1) Security management (People):

- Establishing a formal charter for the security organization and program.
- Clearly outlined roles will guarantee in better understanding of what is expected of all team members.

2) Security governance:

- A security steering committee must be developed whose objective is to focus on giving guidance regarding security initiatives and alignment with business and IT strategies.

3) Risk management: Risk management require identification of technology assets [15]; recognition of data and its links to business processes, applications, and data stores; and assignment of possession and custodial responsibilities.

Actions should also consist of managing a repository of information assets. Owners have authorization and accountability for information assets, which includes protection requirements, and custodians implement confidentiality, integrity, availability, and privacy controls.

4) Risk assessment: Security risk assessment is essential to helping the information security organization build informed decisions when equalization the dueling preferences of business utility and protection of assets. A formal information security risk management method should proactively assess information security risks as well as arrange and maintain them on a periodic or as -needed basis. More elaborated and technical security risk computation in the form of threat modeling should also be enforced to applications and infrastructure.

5) Data governance: This framework should describe who can decide what actions and with what information, and when, in what circumstances, and by using what methods.

6) Virtual machine security: Within the cloud environment, physical servers are consolidated to multiple virtual machine instances on virtualized servers. Not alone can data center security teams duplicate conventional security controls for the data center at large to protect the virtual machines, they can also advise their customers on how to develop these machines for migration to a cloud environment when appropriate.

7) Disaster recovery: In the SaaS environment, customers depend heavily on 24/7/365 access to their services and any interference in access can be destructive. Using the virtualization software virtual server can be reproduced, backed up, and moved just like a file.

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

9) Vulnerability assessment: Classifies network assets to greater efficiently prioritize vulnerability-mitigation programs, like patching and system enhancement.

10) Security image testing: Virtualization-based cloud computing gives the ability to develop "Test image" VM secure builds and to clone multiple copies. Gold image VMs also gives the capability to maintain security up to date and decrease exposure by patching offline. Offline VMs can be patched off-network, giving an easier, greater cost-effective, and reduce production threatening way to test the impact of security changes.

VII. CONCLUSION AND FUTURE WORK

This paper is an effort to discuss regarding cloud computing security issues and Challenges. An attempt is made to investigate cloud-computing susceptibility, security issue cloud computing faces and presented the safety objective that needs to be accomplished. It is observed that security-sensitive applications of a Cloud computing needs high degree of security however, cloud computing are innately sensitive to security attacks. Hence, it is essential to create them more safe and robust to adapt to the rigorous needs of these networks. As we can see the current situation, which shows that there's common bent in cloud computing is toward mesh architecture and huge scale.

There is a requirement for advancement in bandwidth and capacity is needed, which suggests the requirement for a higher frequency and better spatial spectral reuse. The expanding paradigm of Cloud based technologies is one more difficult issue in the near future, which can be already predicted.

VIII. ACKNOWLEDGMENT

I wish to thank my parents for providing me with the needed funding and my university for providing the required resources for this research.

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 changes 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-defv15.doc, 2009

[4].OpenSecurityArchitecturehttp://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/.