International Journal of Innovative Research in Science and Engineering
Vol. No.2, Issue 04, April 2016
www.ijirse.com
ISSN: 2454-9665

SECURITY PERSPECTIVE OF CLOUD COMPUTING

Himani Trivedi[1], Deepali Tripathi[2], Dr. N. K. Joshi[3]

[1]Student,MIMT, Kota, Raj,India

[2]Research Scholar,MIMT, Kota, Raj,India

[3]MIMT, Kota, Raj,India

ABSTRACT

Cloud computing has become a new trend in IT firms for its scalability, reduced cost, flexibility and availability.But this technology currently is going through its infant stage. Still now cloud computing technology suffers from privacy and security issues. Also there are a lot of distributed system issues and legal, compliance issues in large scale. For an ordinary user it is very difficult to choose a particular service provider because different service providers use different taxonomy for a particular service, hence need proper guidance and manuals. Here we discuss various security issues in cloud.

I. INTRODUCTION

Cloud computing, often referred to as simply "the cloud," is the delivery of on-demand computing resources—everything from applications to data centers—over the internet on a pay-for-use basis. It is not an innovation, but a means to constructing it services that use advanced computational power and improved storage capabilities by using set of resources and services offered through the internet. cloud services are delivered from data centers located throughout the world. In cloud computing, resources are made virtual and unlimited, the resources can be provisioned from anywhere i.e. always available at any location. so, cloud computing is a new paradigm where we can provision resources dynamically, deploy applications, and can access platform independent services.

II. BASIC PRINCIPLES

Following are the basic principles of cloud computing.

1.Elastic unlimited capacity

2.Pay as you go

3.Simple ,reliable and fast

III. FUNCTIONALITY

a) Infrastructure as a Service (IaaS):-

also referred to as Resource Clouds, provide (managed and scalable) resources as services to the user – in other words, they basically provide enhanced virtualisation capabilities. Accordingly, different resources may be provided via a service interface. IaaS provides raw computing power, storage and interchangeable services over the web . An example of IaaS is cloud storage, which provides users access to scalable online storage.

ISSN: 2454-9665

b) (Cloud) Platform as a Service (PaaS):-

it provide computational resources via a platform upon which applications and services can be developed and hosted. PaaS typically makes use of dedicated APIs to control the behaviour of a server hosting engine which executes and replicates the execution according to user requests (e.g. access rate). As each provider exposes his / her own API according the respective key capabilities, applications developed for one specific cloud provider cannot be moved to another cloud host – there are however attempts to extend generic programming models with cloud capabilities (such as MS Azure).

c)(Clouds) Software as a Service (SaaS):-

It also sometimes referred to as Service or Application Clouds are offering implementations of specific business functions and business processes that are provided with specific cloud capabilities, i.e. they provide applications / services using a cloud infrastructure or platform, rather than providing cloud features themselves. Often, kind of standard application software functionality is offered within a cloud. Examples: Google Docs, Salesforce CRM, SAP Business by Design. (SaaS): A complete application is offered to the client as a table service on their requirement, applications both world-wide, such as word processing, email and spreadsheet, specify such as customer relationship management (CRM) and enterprise resource management (ERP).

IV. SECURITY ISSUES

1) Data Issues:-

a) Data integrity :- Whenever a data is on a cloud, anyone from anywhere anytime can access data from the cloud since data may be common, private and sensitive data in a cloud. So at the same time, many cloud computing service consume and provider accesses and modify data. Thus there is a need of some data integrity method in cloud computing.

b) Data stealing:- Data stealing is a one of serious issue in a cloud computing environment. Many cloud service provider do not provide their own server instead they acquire server from other service providers due to it is cost affective and flexible for operation and cloud provider. So there is a much probability of data can be stolen from the external server.

c) Data loss:- Data loss is a common problem in cloud computing. If the cloud computing service provider shut down his services due some financial or legal problem then there will be a loss of data for the user. Moreover, data can be lost or damage or corrupted due to miss happening, natural disaster, and fire. Due to above condition, data may not be accesessable to users.

d) Data location:-In general, cloud users are not aware of the exact location of the datacenter and also they do not have any control over the physical access mechanisms to that data. Most well-known cloud service providers have datacenter around the globe. In many a cases, this can be an issue.[3][4]

2. Insecure Interfaces and APIs:- Cloud Computing providers expose a set of software interfaces or APIs that customers use to manage and interact with cloud services.Provisioning, management, orchestration, and monitoring are all performed using these interfaces. The security and availability of general cloud services is dependent upon the security of these basic APIs. From authentication and access control to encryption and activity monitoring, these interfaces must be designed to protect against both accidental and malicious attempts to circumvent policy. Furthermore, organizations and third parties often build upon these interfaces to offer

value-added services to their customers. This introduces the complexity of the new layered API; it also increases risk, as organizations may be required to relinquish their credentials to thirdparties in order to enable their agency.[5]

3. **Governance**: Issues related to (losing) administrative and security controls in cloud computing solutions

.**(a) Data control**: Moving data to the cloud means losing control over redundancy, location, file systems and other relevant configurations.

(b) Security control: Loss of governance over security mechanisms and policies, as terms of use prohibit customer-side vulnerability assessment and penetration tests while insufficient Service Level Agreements (SLA) lead to security gaps.

(c) Lock-in: User potential dependency on a particular service provider due to lack of well-established standards (protocols and data formats), consequently becoming particularly vulnerable to migrations and service termination.[6][7]

4. Malicious Insiders:-

The threat of a malicious insider is well-known to most organizations.This threat is amplified for consumers of cloud services by the convergence of IT services and customers under a single management domain, combined with a general lack of transparency into provider process and procedure. For example, a provider may not reveal how it grants employees access to physical and virtual assets, how it monitors these employees, or how it analyzes and reports on policy compliance.

To complicate matters, there is often little or no visibility into the hiring standards and practices for cloud employees. This kind of situation clearly creates an attractive opportunity for an adversary — ranging from the hobbyist hacker, to organized crime, to corporate espionage, or even nation-state sponsored intrusion. The level of access granted could enable such an adversary to harvest confidential data or gain complete control over the cloud services with little or no risk of detection.[8][9]

5. Legal and Regulatory Issues:-

Aspects related to judicial requirements and law, such as multiple data locations and privilege management.

(a) Data location: Customer data held in multiple jurisdictions depending on geographic location are affected, directly or indirectly, by subpoena law-enforcement measures.

(b) E-discovery: As a result of a law-enforcement measures, hardware might be confiscated for investigations related to a particular customer, affecting all customers whose data were stored in the same hardware.Data disclosure is critical in this case.

(c) Provider privilege: Malicious activities of provider insiders are potential threats to confidentiality, availability and integrity of customers' data and processes' information

(d) legislation: Juridical concerns related to new concepts introduced by cloud computing[10][11][12]

6. Abuse of Cloud Services:-

The term abuse of cloud services refers to the misuse of cloud services by the consumers. It is mostly used to describe the actions of cloud users that are illegal, unethical, or violate their contract with the service provider. Abusing of cloud services was considered to be the most critical cloud threat in 2010 , and different measures were taken to prevent it. However, 84 percent of cloud users still consider it as a relevant threat . Research has

ISSN: 2454-9665

shown that some cloud providers are unable to detect attacks launched from their networks, due to which they are unable to generate alerts or block any attacks. The abuse of cloud services is a more serious threat to the service provider than service users. For instance, the use of cloud network addresses for spam by malicious users has resulted in blacklisting of all network addresses, thus the service provider must ensure all possible measures for preventing these threats.

7. Account or Service Hijacking:-

Account or service hijacking is not new. Attack methods such as phishing, fraud, and exploitation of software vulnerabilities still achieve results. Credentials and passwords are often reused, which amplifies the impact of such attacks. Cloud solutions add a new threat to the landscape. If an attacker gains access to your credentials, they can eavesdrop on your activities and transactions, manipulate data, return falsified information, and redirect your clients to illegitimate sites. Your account or service instances may become a new base for the attacker. From here, they may leverage the power of your reputation to launch subsequent attacks.[13][14]

8. Denial of Service Attacks:-

A DoS attack is an attempt to make the services assigned to the authorized users unavailable. In such an attack, the server providing the service is flooded by a large number of requests and hence the service becomes unavailable to the authorized user. Sometimes, when we try to access a site we see that due to overloading of the server with the requests to access the site, we are unable to access the site and observe an error

9). Shared Technology Issues:- IaaS vendors deliver their services in a scalable way by sharing infrastructure. Often, the underlying components that make up this infrastructure (e.g., CPU caches, GPUs, etc.) were not designed to offer strong isolation properties for a multi-tenant architecture. To addressthis gap, a virtualization hypervisor mediates access between guest operating systems and the physical compute resources. Still, even hypervisors have exhibited flaws that have enabled guest operating systems to gain inappropriate levels of control or influence on the underlying platform. A defense in depth strategy is recommended, and should include compute, storage, and network security enforcement and monitoring. Strong compartmentalization should be employed to ensure that individual customers do not impact the operations of other tenants running on the same cloud provider. Customers should not have access to any other tenant's actual or residual data, network traffic, etc.[15]

V. SOLUTION OF SECURITY ISSUES

1. Use of Data Encryption for security purpose :-

Developers should develop the application which provides encrypted data for the security. So additional security from enterprise is not required and all security burdens are placed on cloud vendor

2. Protection from Malicious Insiders:-The protection from these threats can be achieved by limiting the hardware and infrastructure access only to the authorized personnel. The service provider must implement strong access control, and segregation of duties in the management layer to restrict administrator access to only his authorized data and software. Auditing on the employees should also be implemented to check for their suspicious behaviour. Moreover, the employee behaviour requirements should be made part of legal contract,

and action should be taken against anyone involved in malicious activities. To prevent data from malicious insiders encryption can also be implemented in storage, and public networks.[16]

3. Protection from Abuse of Cloud Services:- The implementation of strict initial registration and validation processes can help in identifying malicious consumers. The policies for the protection of important assets of organization must also user and service provider. This will familiarize user about the possible legal actions that can be conducted against him in case he violates the agreement. The Service Level Agreement definition language (SLAng) enables to provide features for SLA monitoring, enforcement and validation. Moreover, the network monitoring should be comprehensive for detecting malicious packets and all the updated security devices in network should be installed.[17]

4. Protection from Account or Service Hijacking: - Account or service hijacking can be avoided by adopting different security features on cloud network. These include employing intrusion detection systems (IDS) in cloud to monitor network traffic and nodes for detecting malicious activities. Intrusion detection and other network security systems must be designed by considering the cloud efficiency, compatibility and virtualization based context . An IDS system for cloud was designed by combining system level virtualization and virtual machine monitor (responsible for managing VMs) techniques . In this architecture, the IDSs are based on VMs and the sensor connectors on Snort which is a well-known IDS. VM status and their workload are monitored by IDS and they can be started, stopped and recovered at any time by management system of IDS.[18]

5. Protection from Denial of Service:- To avoid DOS attacks it is important to identify and implement all the basic security requirements of cloud network, applications,databases, and other services. Applications should be tested after designing to verify that they have no loop holes that can be exploited by the attackers.The DDOS attacks can be prevented by having extra network bandwidth, using IDS that verify network requests before reaching cloud server, and maintaining a backup of IP pools for urgent cases.[19]

6. Protection from Shared Technology Vulnerabilities:- In cloud architecture hypervisor is responsible for mediating interactions of virtual machines and the physical hardware. Therefore, hypervisor must be secured to ensure proper functioning of other virtualization components, and implementing isolation between VMs. Moreover, to avoid shared technology threats in cloud a strategy must be developed and implemented for all the service models that includes infrastructure, platform, software, and user security. The baseline requirements for all cloud components must be created, and employed in design of cloud architecture. The service provider should also monitor the vulnerabilities in the cloud environment, and release patches to fix those vulnerabilities regularly

7. Protection from Insecure Interfaces and APIs: To protect the cloud from insecure API threats it is important for the developers to design these APIs by following the principles of trusted computing. Cloud providers must also ensure that all the all the APIs implemented in cloud are designed securely,and check them before deployment for possible flaws. Strong authentication mechanisms and access controls must also be implemented to secure data and services from insecure interfaces and APIs. The Open Web Application Security Project (OWASP) [20] provides standards and guidelines to develop secure applications that can help in avoiding such application threats. Moreover, it is the responsibility of customers to analyze the interfaces and APIs of cloud provider before moving their data to cloud.[20]

ISSN: 2454-9665

VI. CONCLUSION

Cloud computing is getting widely adopted in businesses around the world. However, there are different security issues associated with it. In order to maintain the trust of customers, security should be considered as an integral part of cloud.In this paper we have focused on most severe threats on cloud computing that are considered relevant by most users and businesses. We have divided these threats into categoriesof data threats, networks threats, and cloud environment specific threats. The impact of these threats on cloud users and providers has been illustrated in the paper. Moreover, we also discuss the security techniques that can be adopted to avoid these threats.

REFERENCE

1). Mahbub Ahmed, "Above the Trust and Security in Cloud Computing: A Notion towards Innovation", IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, 2010, Australia.

2) ss Bowman, S. Roschke, et aI., "Intrusion Detection in the Cloud," presented at the Eighth IEEE International Conference on Dependable, AutonomIc and Secure Computing, Chengdu, China, 2009.

3) 51, University of Texas, USA, April-June 2010. Problems Faced by Cloud Computing, Lord CrusAd3r, dl.packetstormsecurity.net/.../ProblemsFacedbyCloudComputing.pdf.

4). [8] Kevin Hamlen, Murat Kantarcioglu, Latifur Khan, Bhavani Thuraisingham, Security Issues for Cloud Computing, International Journal of Information Security and Privacy, 4(2),39

5). http://securitylabs.websense.com/content/Blogs/3402.aspx

6) Chow R, Golle P, Jakobsson M, Shi E, Staddon J, Masuoka R, Molina J(2009) Controlling data in the cloud: outsourcing computation without outsourcing control. In: Proceedings of the 2009 ACM workshop on, Cloud computing security, CCSW '09. New York, NY, USA, ACM, pp 85–90 http://doi.acm.org/10.1145/1655008.1655020

7). Sadeghi AR, Schneider T, Winandy M (2010) Token-Based Cloud Computing - Secure Outsourcing of Data and Arbitrary Computations with Lower Latency. In: Proceedings of the 3rd international conference on Trust and trustworthy computing, TRUST '10

8) http://blogs.bankinfosecurity.com/posts.php?postID=140

9) http://technicalinfodotnet.blogspot.com/2010/01/tetheredespionage.Html

10). Zierick J (2011) The special case of privileged users in the sloud. http://blog.beyondtrust.com/bid/63894/The-Special-Case-of-Privileged-Usersin-the-Cloud

11). Dinoor S (2010) Got Privilege? Ten Steps to Securing a Cloud-BasedEnterprise. http://cloudcomputing.sys-con.com/node/1571649

12). Pavolotsky J (2010) Top five legal issues for the cloud. http://www.forbes.com/2010/04/12/cloud-computing-enterprise-technology-cio-networklegal.Html

13) http://www.infoworld.com/d/cloud-computing/hackers-findhome-in-amazons-ec2-cloud742

14) http://vmetc.com/2009/03/12/virtual-machine-sniffer-on-esxhosts/

15) http://www.microsoft.com/technet/security/Bulletin/MS10-010.mspx

16) "Cloud controls matrix (ccm), cloud security alliance," https://cloudsecurityalliance.org/research/ccm/, last Accessed: 2014-12-02

17). A. Al Falasi and M. A. Serhani, "A framework for sla-based cloud services verification and composition," in Innovations in Information Technology (IIT), 2011 International Conference on. IEEE, 2011, pp. 287–292. (IJACSA) International Journal of Advanced Computer Science and Applications,Vol. 6, No. 3, 2015 113

18). C. Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel, and M. Rajarajan "A survey of intrusion detection techniques in cloud," Journal of Network and Computer Applications, vol. 36, no. 1, pp. 42–57, 2013. 19).C. Jin, H. Wang, and K. G. Shin, "Hop-count filtering: an effective defense against spoofed ddos traffic," in Proceedings of the 10th ACM conference on Computer and communications security. ACM, 2003,pp. 30–41. 20).D. Fox, "Open web application security project," Datenschutz und Datensicherheit-DuD, vol. 30, no. 10, pp. 636–636, 2006.