International Journal of Scientific Research in Science, Engineering and Technology (www.ijsrset.com)
© 2014 IJSRSET | Volume 1 | Issue 1 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
DOI : https://doi.org/10.32628/IJSRSET207250

Identifying Cloud Computing Vulnerabilities

Baldev Singh
Lyallpur Khalsa College, Jalandhar, India

ABSTRACT

Cloud computing is passing through development stage and with the passage process of development, cloud is also posing with security threats, challenges and risks. Lots of security threats, risks and challenges are directly or indirectly due to vulnerabilities in cloud environment. Virtualization is the process used in cloud computing through which software hardware is provided to the cloud users and also load balancing is possible in cloud resources and this process is also prone to various security threats and risks. Vulnerabilities and threats to the cloud services leads not only to the malpractices, misuse and exploitation of resources but also to the privacy violations and breaches in data. If these vulnerabilities are not properly identified and specific security measures are not adopted then cloud services will be adversely affected and hence there is dire need to address these vulnerabilities and threats at the cloud customer satisfaction level. In this paper various vulnerabilities and threats to the cloud computing are highlighted which are definitely instrumental to act as the basis of cloud computing security solutions.

Keywords : Cloud computing, vulnerability, Virtualization, Cloud Security.

I. INTRODUCTION

Many of the Internet based technologies have been developed in the past and Cloud computing is one of them. A tremendous growth is noticed in cloud based business endeavors and with the development of Big Data, Internet of Things (IoT), the scale of cloud computing will expand many fold. Cloud computing is basically a service model that provides services like Infrastructure as a Service, Platform as a Service, Software as a Service. The NIST definition of cloud which is used widely defines cloud as [5] "a pay-per-use model for enabling available, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

Cloud computing services are provided by the cloud service provides (CSPs) to the cloud users on Pay-as-Usage basis at anytime and anywhere. Features of cloud computing [2,3] includes on-demand service, broad Internet based access, resource pooling, scalability, pay-as-usage basis service. Cloud service delivery model works as pay-as-you-go model. Cloud has various features due to which its usage has been increased many fold. Some of the unique characteristics of cloud [3,4] are its on-demand availability, shared pool of resources, wide accessibility, customized services, measurement of services used, elasticity, rapid provisioning, low-cost disaster recovery etc. These unique characteristics leads to implementation of cloud computing by various main companies including Amazon, Microsoft and Google. Furthermore, the data store is being used as Google Drive, iCloud, Dropbox by huge number of users. Still the users are hesitating using cloud services

due to various vulnerabilities and security issues of cloud computing environment.

II. VIRTUALIZATION

Virtualization is treated as a technology or a process that creates a virtual environment by way of creating virtual servers, virtual infrastructures [2], virtual storage devices and/or computing resources and applications. Through virtualization, we can run desired program without interfering or changing any existing services provided by the server or platform. Multiple users can use a single physical instance of an application of a computer resource on shared basis, it is possible by creating logical resources of a physical resource through virtualization software. Virtualization is classified into four types:

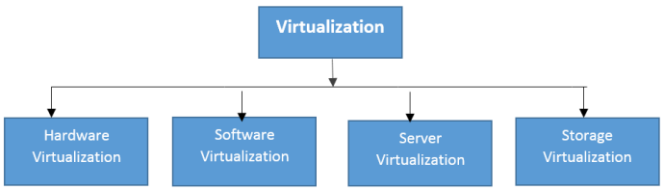

Figure-1: Virtualization

Hardware virtualization is taken place by installing virtual machine software on hardware (physical machine). Virtual machine manager (VMM) or hypervisor which is installed on the server machine is treated as server virtualization. Multiple servers are created on a single physical server and are used on demand basis as well as for purpose of load balancing. Virtualization software (VMM) also acts as a controller and monitor to control and monitor the various resources of the machine like processor, memory and other resources related to hardware. Software virtualization further classified as Operating System Virtualization, Application Virtualization and Service Virtualization. Software Virtualization is used to create a virtual environments on the host machine to run multiple operating systems virtually, hosting multiple applications on the single instance of hardware as well as hosting particular services or processes for individual applications. For example (Operating System Virtualization) user can run Linux on the host machine and you are also able to run other operating system like Linux as native operating system on the same hardware.

Storage virtualization technique is used to create a virtual pool of storage (simulated) by using various physical storages that are interconnected and is managed by using a single command console. Example of storage virtualization is VMware's vStorage. Other types of virtualizations are data, network and desktop virtualization. Some of the examples of hypervisor are Oracle Virtual Box, VMware Fusion, Oracle OVM for SPARC, Hyper-V. Virtualization is the process used in cloud computing through which software hardware is provided to the cloud users and also load balancing is possible in cloud resources.

III. VULNERABILITIES IN CLOUD COMPUTING

Cloud environment is prone to various types of threats and attacks due to its various vulnerabilities. Data is important for every organization and to place the data on cloud which is owned and handled by third party is naturally be secured enough otherwise no one will go for cloud space for data storage. Cloud may be of the type Public, Community or Hybrid or even Private but there is ample potential of threats, attacks [6] and vulnerabilities. Vulnerability is basically a conspicuous and apparent factor of risk. Vulnerability defined in [1] refers to "the probability that threat capability exceeds the ability to resist the threat". 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 [1].

Vulnerability is further determined by considering two factors which are Threat Capability (TA) and Control Strength (CS) [2,7]. If in a scenario, Threat capability is greater than (suppose around 85% to 95%)

the Control Strength (suppose around 75% e.g. password strength), then the difference between these TA and CS represents to Vulnerability. Similarly Threat defined in [1] refers to "anything that is capable of acting in a manner resulting in harm to an asset and/or organization; for example, acts of God (weather, geological events, etc.); malicious actors; errors; failures". If threats are not controlled, that can lead to unauthorized access, misuse by way of unauthorized access, discloses sensitive information illegitimately, unauthorized modification or alternations, destruction or denial of service attacks [8]. When vulnerability is exploited, it causes various types of losses.

IV. RELATED WORK

Vulnerabilities in cloud determines the risks to the cloud users. Vulnerability factor is also determined by the access level, efforts, risks and motivation of attackers in a cloud environment [14]. To know about Cloud-Specific Vulnerabilities [2,9], we must first know about abstract view of cloud computing and various core cloud computing technologies. In simple words, a vulnerability in cloud can be because of:

- Its Core cloud computing technology vulnerabilities [2,10]:-
  - vulnerability as inherent to virtualization
  - session riding/hijacking vulnerabilities are inherent to web application technologies
  - critical flaws and faults in implementations of cryptographic algorithms
  - weak encryption or no encryption
- vulnerabilities due to its root causes (as per NIST defined cloud features) in one or more cloud characteristics [6]:-
  - vulnerability due to unauthorized access to organization interface
  - Internet protocol vulnerabilities that may lead to man-in-the-middle attacks.
  - Resources reallocation based data recovery vulnerability
  - Vulnerabilities due to metering and billing data manipulation/ evasion.
- non implementation of security controls properly [2,13]
  - Control challenges vulnerabilities of the form insufficient network-
  - based controls in virtualization.
  - Network based threats and vulnerabilities due to control challenges in cloud virtual environment.
  - Inadequate key management procedures in cloud infrastructures
  - Very difficult to apply and implement hardware security module that are of the type standard controls in virtual cloud infrastructure
  - Lack of sufficient standardized cloud-specific security metrics
  - Lack of applying controls for audit and security assessment as well as accountability
- cloud-specific vulnerabilities [2,11]
  - Injection vulnerabilities like SQL injection, command injection, cross-site scripting
  - Weak authentication mechanisms like weak passwords, insecure user behavior, reuse of passwords, one-factor authentication aspect, weak authentication implementation
  - service denial because of account lockout
  - weak password-recovery mechanisms
  - faulty or lack of sufficiency in authorization checks
  - due to uneven or coarse authorization control
  - Uneven logging and monitoring facilities
- architectural components specific challenges and vulnerabilities [2,12]
  - cloud-specific threats and vulnerabilities
  - applying weak IT-support infrastructure in cloud architecture
  - cloud access through untrusted network
  - vulnerabilities in layers of cloud software environment
  - vulnerabilities in configuration and patch levels
  - vulnerabilities in virtual images with respect to IaaS

- vulnerabilities due to Data leakage because of replication of VM

V. CONCLUSION

Cloud computing is emerged Internet based distributed computing that provides services to the cloud users and is vulnerable to various attacks, risks and challenges. Different type of vulnerabilities discussed in this paper are needed to be addressed to the level of the satisfaction of the cloud users. As there is immense concentrations of data and resources, therefore cloud computing is very much attractive target to the attackers, and the attackers find the soft points of attacks by identifying vulnerabilities in the cloud environment. A robust, cost effective and scalable defense line is the only solution for cloud computing security in which in-depth knowledge of the cloud vulnerabilities is must which is highlighted in this paper. This paper has generally contributed to acquaint with the cloud vulnerabilities to the cloud security planners and implementers as well as cloud services consumers and cloud service providers. The evaluation, perspectives and findings of the paper can be used as a reference for further apposite and pertinent implementation of worthwhile cloud security solution.

VI. REFERENCES

[1]. Technical Standard Risk Taxonomy ISBN- 1-931624-77-1 Document Number-C081 Published by The Open Group January 2009

[2]. B. Grobauer, T. Walloschek, and E. Stocker, “Understanding Cloud Computing Vulnerabilities,” Security & Privacy, IEEE, vol. 9, no.2, pp. 50-57, 2011

[3]. European Network and Information Security Agency (ENISA), Cloud Computing: Benefits, Risks and Recommendations for Information Security, Nov. 2009; www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport.

[4]. Kevin Hemalen, Murat Kantarcioglu, Latifur Khan, and Bhavani Thuraisingham, The University of Texas at Dallas, USA, “Security Issues for cloud computing”, April-June 2010,international Journal of Information Security and Privacy.

[5]. Jinpeng Wei, Xiaolan Zhang, Glenn Ammons,Vasanth Bala,peng Ning.”Managing Security of virtual machine images in a cloud environment “.CCSW’09:Proceedings of the 2009 ACM workshop on Cloud computing security, November 2009, pp 91-96.

[6]. Miranda Mowbray, Siani Pearson “A Client – based privacy Manager for Cloud Computing”. OMSWARE '09: Proceedings of the Fourth International ICST Conference on communication system software and middle ware, June 2009.

[7]. Mervat Adib Bamiah, sarfraz Nawaz Brohi, “ Seven Deadly Threats and Vulnerabilities in Cloud Computing” International Journal of Advanced Engineering Sciences And Technologies, Vol No. 9, Issue No. 1. 2011.

[8]. Song.D.,Shi.E,Fischer.I,Shankar.U,” Cloud Data protection for the masses”, IEEE computer Society,Vol: 45,issue:1,2012; pg: 39-45,ISSN:0018-9162

[9]. A. J. Choudhury, P. Kumar, M. Sain, H. Lim and H. Jae-Lee, "A Strong User Authentication Framework for Cloud Computing," 2011 IEEE Asia-Pacific Services Computing Conference, Jeju Island, 2011, pp. 110-115.

[10]. S .Kuyoro, F. Ibikunle, O. Awodele, “Cloud Computing Security Issues and Challenges,” in Proc. International Journal of Computer Networks (IJCN), volume 3, issue 5, 2011.

[11]. W. Jansen and T.Grance, “Guidelines on Security and Privacy in Public Cloud Computing,” Nist Special Publication, NIST SP-800-144,Dec 2011.

[12]. Meiko Jensen, Jörg Schwenk, Nils Gruschka and Luigi Lo Iacono, "On Technical Security Issues in Cloud Computing," in IEEE ICCC, Bangalore 2009, pp. 109-116.

[13]. Kresimir Popovic , Zeljko Hocenski, "Cloud computing security issues and challenges," in The Third International Conference on Advances in Human oriented and Personalized Mechanisms, Technologies, and Services, 2010, pp.344-349.

[14]. Balachandra Reddy Kandukuri, Ramakrishna Paturi and Atanu Rakshit, "Cloud Security Issues," in Proceedings of the 2009 IEEE International Conference on Services Computing, 2009, pp. 517-520.

Cite this article as :

Baldev Singh, "Identifying Cloud Computing Vulnerabilities", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 1_ Issue 1, pp. 198-202, 2014. Available at doi : https://doi.org/10.32628/IJSRSET207250
Journal URL : http://ijsrset.com/IJSRSET207250