© 2016 | International Journal of Scientific Research in Science and Technology
IJSRST | Volume 2 | Issue 1 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Doi : https://doi.org/10.32628/IJSRST207239

An Analysis of Cloud Computing Security Issues

Baldev Singh
Lyallpur Khalsa College, Jalandhar, India

ABSTRACT

Cloud computing is one of the emerged technologies in the past decade. Tremendous growth is noticed in the usage and implementation of Cloud computing. Although cloud spectrum is widely popular still there are lot of challenges and issues to be addressed for its optimal usage. Vulnerabilities and threats to the cloud services leads to attacks and exploitation of resources as well as data breaches and privacy violations that need to be addressed at the cloud customer satisfaction level. This paper highlights different cloud security issues and their security requirements. The review aspects and findings of the paper can be used as a reference for further appropriate and effective implementation from the suggested practically viable cloud security solution in an independent manner or using as a hybrid technique.

Keywords : Cloud Computing, Privacy, DOS Attacks, Cloud Security Requirements.

I. INTRODUCTION

Various technologies are developed and evolutionized from time to time. Cloud computing is one of the technological paradigm which is evolutionized from the existing technologies. This distributed paradigm is being used for providing variety of services to the cloud users. The basic services of cloud computing are referenced by cloud computing reference model. The cloud reference model encompasses three main services [1] known as Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). The NIST definition of cloud which is used widely defines cloud as [2] "a model for enabling 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 is capable to provide IaaS, PaaS and SaaS services to the cloud users on Pay-as-Usage basis at anytime and anywhere. Features of cloud computing includes on-demand service, broad Internet based access, resource pooling, elasticity, scalability, pay-as-usage basis service.

Cloud services are delivered through the Internet. Cloud has the distributed architecture and provides computational facility as well through which various cloud computing features like availability, scalability, adaptability, agility and collaboration which are helpful for increasing the efficiency and performance of an enterprise or organization. Cloud has a vast pool of resources which are actual and virtual in nature. Virtualization is used for providing the secure services to the cloud users. As various issues, threats and vulnerabilities [3,6] exist in traditional information technology (IT) tools, there exists more or less similarities in cloud computing environment. Vulnerabilities and threats to the cloud services lead to attacks and exploitation of resources as well as data breaches and privacy violations [4, 5].

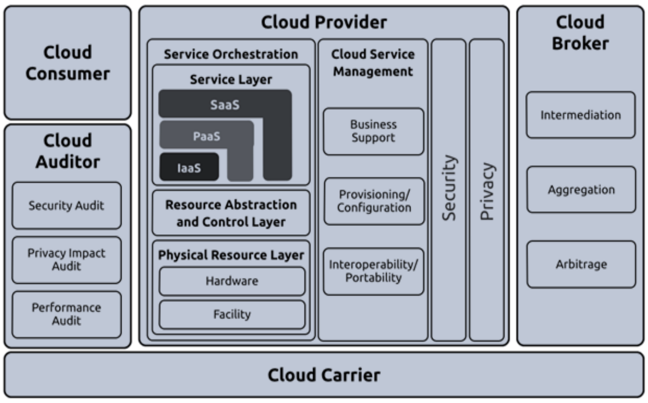

Figure 1: Cloud Computing Reference Architecture

Cloud computing reference architecture [2] is shown in figure-1. This generic reference model depicts high-level conceptual design which encompasses the requirement specification, structures, as well as various operations and activities of cloud computing. The cloud reference model discussed here is not specific to any implementation, vendor products or services.

1. Actors in Cloud Computing

Various actors [2] along with their role, activities and functions that are part of cloud computing taxonomy are presented. Various views and descriptions, uses, as well as standards of cloud computing are depicts in this reference model.

Table-1: Actors in Cloud Computing

Actor	Role
Cloud Provider	Cloud provider provides various services like IaaS, SaaS and PaaS to the cloud end users.
Cloud Consumer	Cloud consumer refers to the person or an organization who uses the cloud based services which are provided by the cloud service provider.
Cloud Broker	Cloud broker refers to an entity that provides three categories of services. These three categories are Intermediation, Aggregation and Arbitrage.
Cloud Auditor	A cloud auditor provides the role of auditing of cloud services like assessment of services provided by the cloud providers, security, privacy and performance aspects that are included in service level agreements.
Cloud Carrier	A cloud carrier provides the role of intermediary between the cloud consumers and cloud service providers. Cloud carrier acts as a bridge to provide connectivity and transport of cloud services. It provides the access of cloud computing devices like tablets, laptops, notebooks, navigation, computers, storage services etc.

2. Threats in Cloud Computing

Security threats and attacks are the main concern to the cloud stakeholders. Confidentiality and integrity of data is very much significant in cloud computing. Vulnerabilities in cloud computing enables the attackers for malicious activities and security threats. Various security issues are directly related with the cloud computing service delivery Models (IaaS, PaaS, and SaaS). Some of the security issues related to IaaS are virtual machine (VM) operating system security, Virtual network security, Securing VM boundaries, VM images repository security and Hypervisor security. Similarly PaaS Security Issues consists of Service-oriented Architecture (SOA) security issues and API Security [9]. Categorically SOA attacks are of the nature of DOS attacks [7,11], Injection attacks, Man-in-the-middle attacks, input validation related attacks, XML-related attacks, Dictionary attacks and Replay attacks. Figure-2 shows various security threats [8,18] in cloud computing environment.

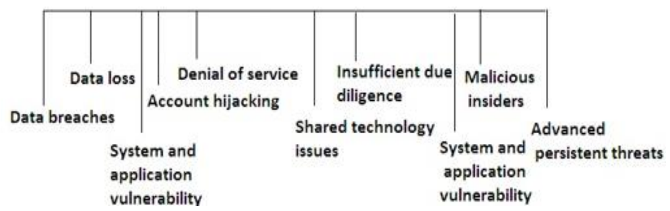
Data loss
Denial of service
Insufficient due diligence
Malicious insiders
Data breaches
Account hijacking
Shared technology issues
Advanced persistent threats
System and application vulnerability
System and application vulnerability

Figure-2 : Cloud Security Threats

Cloud computing exposes services and resources over the internet 10,12]. The access to these resources is made through HTTP and HTTPS for web application. Various protocols namely SOAP, REST and RPC Protocols are required for web services and APIs in PaaS. To access IaaS, remote connections, VPN and FTP are in use for virtual machines and storage services. The potential attackers use the vulnerabilities related to these grey areas and attack-prone protocols for attack purpose and top priority protection of data and data transfer is must between the cloud platform and the consumers. VM hoping threat is related to IaaS delivery model of cloud. In this threat, VM is compromised by another VM by way of gaining its access. This is caused if access restrictions are not made properly and the used of unrestricted access leads to falsely allocate and deallocate of resources of targeted machine.

3. Cloud Computing Security Countermeasures

Threats and vulnerabilities in cloud computing [13] causes serious loss to individual and business losses if these are not dealt with utmost care. These can lead to abundant adverse effects to the cloud users. Proper strategy and implementation of various security measures [14]is required. Various threat aspects and their impacts as well as Cloud Security Requirements are discussed as shown in Table-2 below.

Table-2 : Various Threat Aspects, their Impacts and Cloud Security Requirements

Threat Aspects	Impact of Threat Aspects	Cloud Security Requirements
Breach of Data	Confidential, important, as well as sensitive or personal information is stolen and that may be used for unethical or economic gains by the intruders or attackers [12].	Confidentiality and Privacy
Misconfiguration	Misconfiguration leads to vulnerabilities [15] in the system at different levels that are susceptible to attacks.	Confidentiality, Privacy, Authentication, Integrity,
Non-implementing Proper Security	Proper security checks and firewalls saves from potential for attacks [16] . Different user interfaces as well as APIs may have inherent vulnerabilities which are further susceptible to attacks on the system.	Authorization, Accountability, Confidentiality, Privacy, Integrity
Inadequate Protection of Credentials	Inadequate protection of the credentials results in unauthorized access [2,18] to the attackers and breach of data that may cause damage to the image of the target users or economic losses.	Confidentiality and Privacy, Authorization

Account Hijacking	In this traditional mechanism of account hijacking, illegitimate users get access of the account and are able to perform falsified and harmful activities.	Authorization, Accountability, Confidentiality, Privacy, Integrity, Availability, Authentication
Insider Threats	Insider users are basically employees or partners in an organization and can act as malicious users to steal confidential information [17] and harm personnel or economic way.	Authorization, Accountability, Confidentiality, Privacy, Integrity, Authentication
Weak Set of Interfaces and APIs	Weak set of user interfaces or application program interfaces (APIs) are having potential of vulnerabilities [6] that further leads to sniffing of private and secure information to effect the system adversely.	Authorization, Accountability, Confidentiality, Privacy, Integrity
Inadequate Control Plane	Due to new ways of attacks and intrusions, there is huge potential of Advanced Persistent Threats (APTs) which are advanced in nature and difficult to eliminate at earlier stage. Inadequate control plane causes to such types of vulnerabilities and threats.	Authorization, Confidentiality and Privacy
Inadequate Cloud Usage Visibility	Cloud usage is based on shared technology in nature. The sharing aspects of technology if not designed in effective isolation way can lead to shared technology vulnerabilities [12].	Authorization, Confidentiality, Privacy, Integrity, Availability, Authentication
Misuse of Cloud Resources	Poor deployment of cloud controls leads to flaws and vulnerabilities. These further are susceptible to misuse of cloud resources, phishing and denial of service attacks [6,13].	Availability

To address the various security requirements of cloud computing, various countermeasures and security solution approaches are suggested by the researchers and also applied depending upon their practical usage and implications. These countermeasures are associated with cloud security requirements in nature. For example, Strong access control and authorization as well as the use of standard protocols for authentication and authorization are security solution approaches for authentication and authorization related cloud security requirements. Similarly Trust based security and privacy countermeasures are the measures that take into account various cloud security requirements like Authorization, Accountability, Confidentiality, Privacy, Integrity, Availability, Authentication and suggest solution by using PKIs, Hybrid cryptography, Privacy preserving access control, TTP etc. controls. By considering Web Services and Interfaces vulnerabilities again various cloud security requirements like Availability, Authorization, Accountability, Privacy, Integrity, Authentication and privacy are treated as utmost important for secure solutions. Physical security measures, Data storage security measures and Virtual environment security measures are also the area of research for proper security solutions to tackle cloud computing security challenges and issues.

II. CONCLUSION

Cloud computing is an emerged technology providing IaaS, PaaS and SaaS to the cloud-end users and there has been tremendous growth noticed in the past decade in spite of widened cloud threat spectrum. Although there are numerous benefits and advantages of the cloud computing, but there are lot of challenges and issues to be addressed for its optimal usage. Cloud vulnerabilities, potential security threats, security and privacy protection issues are the key problems that need to address at the cloud customer satisfaction level. This paper focuses on various cloud security issues and their security requirements. This review survey is limited to the narrative review work of published research papers from academia and industry. The findings and reviews of the paper can be used as a reference for proper and effective implementation of the suggested practical solution in an independent manner or as hybrid way of mechanism.

III. REFERENCES

[1]. L. Jun-Ho et.al. "Multi-level intrusion detection system and log management in cloud computing," Proceedings of the13th International Conf. pp. 552–555, Feb. 2011

[2]. P. Mell and T. Grance, "The NIST definition of cloud computing," NIST special publication 800-145, September 2011.

[3]. Monowar H. Bhuyan, H. J. Kashyap, D. K. Bhattacharyya and J. K. Kalita. Detecting Distributed Denial of Service Attacks: Methods, Tools and Future Directions . The Computer Journal, 2013.

[4]. Mohd Faizal Abdollah, Mohd Zaki Masud, Shahrin S., Robiah Y. , Siti Rahayu S. "Threshold verification using Statistical Approach for Fast Attack Detection" Intl. Journal of Computer Science and Information Security, Vol.2, No 1, 2009.

[5]. B. B. Gupta, R. C. Joshi and M. Misra, "Defending against Distributed Denial of Service Attacks: Issues and Challenges," Information Security Journal: A Global Perspective, Vol. 18, No. 5, 2009, pp. 224-247.

[6]. Cloud Security Alliance, March 2010 —Top Threats to Cloud Computing at (http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf)

[7]. Ahmed Patel et. al., "An intrusion detection and prevention system in cloud computing: A systematic review", Journal of Network and Computer Applications (2012)

[8]. "CERT Advisory: SYN Flooding and IP Spoofing Attacks," CERT® Coordination Center Software Engineering Institute, Carnegie Mellon, 2010. http://www.cert.org/advisories/CA-1996-21.html

[9]. Vincenzo Gulisano, Zhang Fu, Mar Callau-Zori, Ricardo Jimenes-Peris, Marina Papatraintafilou, Marta Patino-Martinez "STONE: A Stream-based DDoS Defense Framework Technical Report" no. 2012-07, ISSN 1652-926X, Chalmers University of Technology, Sweden, 2012

[10]. Felix Lau Simon , Stuart H. Rubin , H. Smith, Trajkovic , "Distributed Denial of Service Attacks"; http://www2.ensc.sfu.ca/~ljilja/papers/smc00_edited.pdf, 2000.

[11]. Faizal M.A., and Zaki M.M., and Shahrin S., and Robiah Y., and Rahayu S.S., (2010) Statistical Approach for Validating Static Threshold in Fast Attack Detection. Journal of Advanced Manufacturing.

[12]. Subashini, S., & Kavitha, V. (2011). Review: A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications, 34(1), 1-11.

[13]. Kaufman, L. M. (2009). Data security in the world of cloud computing. Security & Privacy, IEEE, 7(4), 61-64.

[14]. Jensen, M., Gruschka, N., Schwenk, J., & Iacono, L. L. (2009). On Technical Security Issues in cloud computing. 2009 IEEE International Conference on Cloud Computing, 0, 109-116.

[15]. Prachi Deshpande, Aditi Aggarwal, S.C. Sharma, P.Sateesh Kumar, Ajith Abraham, "Distributed port-scan attack in cloud environment", Computational Aspects of Social Networks (CASoN) 2013 Fifth International Conference on, pp. 27-31, 2013.

[16]. S Meena, Esther Daniel, N.A. Vasanthi, "Survey on various data integrity attacks in cloud environment and the solutions", Circuits Power and Computing Technologies (ICCPCT) 2013 International Conference on, pp. 1076-1081, 2013.

[17]. Kelly Beardmore, “The Truth about DDoS Attacks: Part1, TheCarbon60Blog. http://www.carbon60.com/the-truth-about-DDOS-attacks-part-1/Nov.21, 2013.

[18]. Zhifeng Xiao, Yang Xiao, "Security and Privacy in Cloud Computing", Communications Surveys & Tutorials IEEE, vol. 15, no. 2, pp. 843-859, 2013.

Cite this article as :

Baldev Singh, "An Analysis of Cloud Computing Security Issues", International Journal of Scientific Research in Science and Technology (IJSRST), Online ISSN : 2395-602X, Print ISSN : 2395-6011, Volume 2 Issue 1, pp. 212-217, January-February 2016. Available at doi : https://doi.org/10.32628/IJSRST207239
Journal URL : http://ijsrst.com/IJSRST207239