DOI: http://dx.doi.org/10.26483/ijarcs.v9i1.5141

ISSN No. 0976-5697

Volume 9, No. 1, January-February 2018

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

VULNERABILITIES IN CLOUD STORAGE AND THEIR COUNTERMEASURES

Varsha Nagele
Department of Computer Science
University Institute of Technology RGPV
Bhopal, India

Deepak Tomar
Department of Computer Science
Maulana Azad National Institute of Technology
Bhopal, India

Abstract: An effective and efficient paradigm that offers an innovative business model for IT organizations to adopt varied services ,direct investment is termed as Cloud Computing. Because it has opened new dimensions towards advancement , simultaneously it's a colossal scope of issues associated with the safety breaches within the cloud model , its design and on its varied dependency layers. Due to this , the adoption of cloud services is questionable owing to the constraints over its advantages that area unit achieved from cloud computing model. In this paper we've done an in depth analysis and located out countermeasures of the cloud security related problems.

Keywords: cloud computing , cloud threats , cloud security , cloud vulnerabilities , countermeasures

I. INTRODUCTION

Cloud computing , a web primarily based computing wherever package , shared resources and data area unit served as associate degree economical delivery model for ensuing generation of internet- primarily based, extremely ascendible and cosmopolitan computing systems within which the procedure resources supply services. The 2 key characteristics of the cloud model embody Multi-tenacy and physical property .Multi-Tenancy is that the development of sharing an equivalent service instance among varied totally different tenants. Physical property options includes scaling ups and downs of resources allotted to a service supported the desired service demands. These characteristics focus chiefly on improvising resource utilization, budgets and repair accessibility. In keeping with a survey [2] on revenues generated by cloud computing, the cloud market was value USD fifty nine.6B in 2014, is predicted to be USD 68B in 2011 and can reach USD 148B by 2017. These revenues imply that cloud computing is an effective platform and also a promising platform. On the contrary, the increasing attacks by the attackers' interests to find the prevailing vulnerabilities within the cloud computing design. The potential advantages and revenues gained from the cloud computing model, still incorporates a heap of essential problems that impact the creditability .Major drawbacks embody merchant lock-in, multi-tenancy , information management, mobility of services, SLA management, and cloud security

II. LITERATURE REVIEW

The Cloud Computing Use Cases cluster [3] discuss the varied use case eventualities and connected needs which will exist within the cloud computing model. ENISA [4] investigated the various security risks associated with adopting cloud computing in conjunction with the affected assets, the risks probability, impacts, and vulnerabilities in cloud computing which will cause such tragic risks.An analysis by CSA [5] states ' Top Threats In Cloud Computing'. Also , Bala et al [6] discusses the various objectives and specification of secure SLA. Various high level security issues such as confidentiality and integrity are discussed by Kresimir [7]printed a group of elaborate reports discussing for a few of those connected domains. We tend to researched within the cloud model to spot the foundation causes and essential collaborating dimensions in such security issues/problems mentioned by the previous work. This can facilitate higher so as to grasp the matter and deliver countermeasures.

III. CLOUD ARCHITECTURE AND ITS CONSEQUENCES

The cloud delivery models include: (1) personal cloud: a cloud platform is devoted for specific organization, (2) Public cloud: a cloud platform offered on the market to public users to register and use the available infrastructure, and (3) Hybrid cloud: a personal cloud that may be extended to use resources publically clouds. Public clouds square measure the foremost vulnerable preparation model thanks to the provision for public users to host their services under agency could be malicious users. The cloud service models namely, Infrastructure as a service provides the basic development and runtime environment . Amazon EC2 is that the most outstanding IaaS supplier. - Platform-as-a-service (PaaS): wherever cloud suppliers deliver the entire platforms, tools and different business services that change customers to develop, deploy, and modify their own applications, while not putting in any of those platforms or support tools on their personal machines.

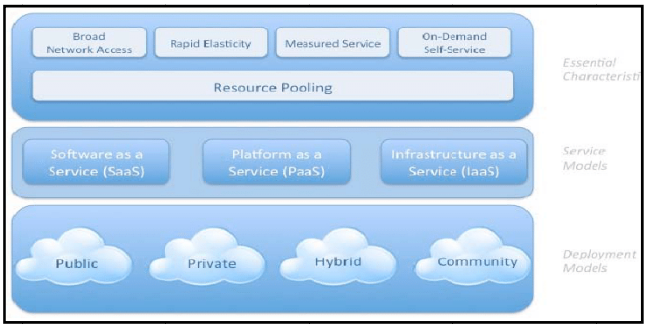

Fig. 1 NIST visual model of cloud computing [1].

© 2015-19, IJARCS All Rights Reserved

III. CLOUD COMPUTING FEATURES AND SECURITY IMPLICATIONS

The cloud computing model meets such desires through a winwin resolution by delivering 2 major characteristics: multitenancy and physical property. There are, many variations, first off every tenant has their own dedicated instance with their own customizations. Moreover, every tenant uses a particular dedicated instance, like previous approach, whereas all instances area unit an equivalent however with totally different configurations. In approach three, all tenants share an equivalent instance with actual timings. within the last approach tenants area unit directed to a balancer that redirects tenants requests to the present instances load. Approaches three and four area unit the foremost vulnerable as tenants area unit synchronous within the same load. This sharing of resources violates the confidentiality feature of tenants' IT assets .To deliver secure multi-tenancy there ought to be correct isolation among tenants' information therefore as to avoid attacks that decide to damage the victim assets [10]. Physical property defines the capability of having the ability to proportion or down resources allotted to services supported the demand and needs. Scaling up and down of tenant's resources provides the access to different tenants to use the tenant recently allotted resources resulting in confidentiality threats. What is more , physical property includes a service placement engine that maintains and modifies list of out there resources from the provider's pool of resources. This list is then accustomed apportion resources and map the individual services. Such engines ought to incorporate essential cloud security and legal needs like to avoid inserting the competitors services on an equivalent server location

IV. CLOUD COMPUTING SERVICE MODELS AND THEIR ISSUES

The key security vulnerabilities in every service delivery model area unit as follows :

i.Infrastructure as a Service - As each Iaas require certain Virtual Machine to function effectively, thus security issues related to common physical servers like viruses and riskwares. Every cloud shopper will use their security controls supported their needs, expected risks, and their self security management method. Securing the VM pictures in an exceedingly repository - in contrast to physical servers VMs area unit still below risk even after they area unit offline. VM pictures are often compromised to attacks by injecting malicious codes within the VM file . Another issue is that the VM templates, that such templates might retain the first owner data which can be employed by a brand new shopper.

ii. PaaS Security Issues- SOA connected security problems – this model relies on the Service-oriented design (SOA) therefore it results in inheritable all security problems that exist within the SOA domain like DOS attacks, Man-in-the-middle attacks, XML-related attacks, Replay attacks,Injection attacks and varied input validation connected attacks [9, 16]. Authentication, authorization and WS- Security standards area unit necessary to secure the services provided by the cloud.

iii. Within the SaaS model incorporating and maintaining security may be a shared responsibility among the each cloud suppliers and repair suppliers. This model inherits the safety problems mentioned within the previous models because it is constructed on prime of each of them together with information security management [11] . internet application vulnerability scanning - internet applications that area unit to be hosted on the cloud infrastructure ought to be valid and scanned therefore on avoid vulnerabilities if any .Scanners ought to be updated with the recently found vulnerabilities and attack ways maintained within the National Vulnerability information and therefore the Common Weaknesses Enumeration (CWE) [14]. The 10 most important internet applications vulnerabilities in 2016 listed by OWASP [15] area unit injection, cross website scripting. Security miss-configuration is additionally terribly essential with multi-tenancy wherever every of the tenant has its own security configurations .

iv. Cloud Management Security problems, within the Cloud Management Layer (CML) additionally called the "microkernel" which might be extended to extrapolate and coordinate totally different parts. The parts of CML embody SLA management, service observation, elasticity, IaaS, PaaS, SaaS services written record, and most significantly security management of the cloud. Such a layer is extremely essential since associate degree style of vulnerability or any breach of this layer can end in an antagonist having management, like associate degree administrator, over the total cloud platform service.

V. THREATS AND THEIR OUNTERMEASURES

- **Insecure Interfaces and API's-**

Cloud computing suppliers exposes set of package interfaces or Apis that customers use to manage , manipulate and act with cloud services. Provisioning, management, orchestration of the read, and observation area unit all performed with these interfaces. The safety and accessibility of basic cloud services depends upon the safety of those general Apis. From authentication and access management to coding and activity observation, these interfaces should be designed to safeguard against varied malicious tries to avoid security policy.

Countermeasures:

Analyze the safety model of cloud supplier interfaces.Also, guarantee sturdy authentication and access controls area unit enforced as one with encrypted transmission.

- **Malicious Insiders**

The malicious business executive attack is outstanding to most organizations. This threat is attenuated for shoppers of cloud services by the convergence of IT services and customers

Countermeasures:

Enforce strict offer chain management and conduct a comprehensive provider assessment annually. Also , Specify human resource needs as a part of legal contracts. It largely

© 2015-19, IJARCS All Rights Reserved

needs transparency into overall data security and management practices, likewise as compliance reportage

- **Shared Technology Issues**

Often, the underlying parts that form up the shared infrastructure weren't designed to supply sturdy isolation properties for a multi-tenant design. To beat this gap, a virtualization hypervisor mediates access between guest in operation systems and therefore the physical reason resources. Still, even hypervisors have exhibited flaws that have enabled guest in operation systems to achieve inappropriate levels of management or influence on the underlying platform. A defense comprehensive strategy is suggested, and should embody reason, storage, and network security social control and observation. sturdy compartmentalization ought to be done to make sure that individual customers don't impact the operations of different tenants on an equivalent cloud supplier

COUNTERMEASURES:

Implementation of the safety with the most effective practices for installation atmosphere for the unauthorized manipulations. Promoting an excellent sturdy authentication and access management for body access and operations. Conduct vulnerability scanning and configuration audits.

- **Account or Service Hijacking**

Account or service hijacking is ancient. Whenever associate degree assailant gains access to your credentials, they'll snoop on your activities,sniffs on network traffic and transactions, manipulate information, come back falsified or tampered data, and harm your shoppers to illegitimate sites.

COUNTERMEASURES:

Prohibiting the sharing of account credentials between users and services provided to them. most significantly, using proactive observation to observe unauthorized activity within the server.

VI. REFERENCES

[1] http://www.wheresmyserver.co.nz/storage/media/faq-files/cloud-def-v15.pdf

[2] IDC, "IDC Ranking of problems with Cloud Computing model," ed, 2016, http://blogs.idc.com/ie/?p=210

[3] Cloud Computing Use Case Discussion cluster, "Cloud Computing Use Cases Version three.0," 2015.

[4]http://www.enisa.europa.eu/act/rm/files/deliverables/cloudcomputing-risk-assessment

[5] Cloud Security Alliance (CSA). (2016),http://www.cloudsecurityalliance.org/

[6] Balachandra Reddy Kandukuri, "Cloud Security problems," in Proceedings of the 2009 IEEE International Conference on Services Computing, 2009, pp. 517-520.

[7] Kresimir Popovic , Zeljko Hocenski, "Cloud computing security problems and challenges," within the Third International Conference on Advances in Human oriented and customized Mechanisms, Technologies, and Services.

[8] S. Subashini, Kavitha, V., "A survey on security issues in commission delivery models of cloud computing," Journal of Network and portable computer Applications

[9] Multi-Tenant data style. Available: http://msdn.microsoft.com/en-us/library/aa479086.aspx

[10] http://aws.amazon.com/ec2-sla/

[11] D. K. Holstein, , Stouffer, K., "Trust however Verify essential Infrastructure Cyber Security Solutions," in HICSS 2010, pp. 1-8.

[12] Z. Wenjun, "Integrated Security Framework for Secure internet Services," in IITSI 2010, pp. 178-183

[13] B. Wang, Huang He, Yuan, Liu Xiao, Xi, Xu Jing, Min, "Open Identity Management Framework for SaaS system," in ICEBE '13. pp. 512-517.

[14] F. Elizabeth, , Vadim, Okun, "Web Application Scanners: Definitions and Functions," in HICSS 2007, pp. 280b-280

[15] OWASP, The 10 most important internet Application Security Vulnerabilities. http://www.owasp.org/index.php/OWASP_Top_Ten_Project

© 2015-19, IJARCS All Rights Reserved