Volume-3, Issue-11, Nov Special Issue -2014 • ISSN No 2277 - 8160

Research Paper | Systems

A Study on Security Analysis in Cloud Computing

L.ARUNA Research Scholar, Ph.D Comp.Science, Periyar University, Salem.Tamilnadu

Dr.M. ARAMUDHAN Assoc.Prof & Head, Department of IT, PKIET, Karaikal.-Tamilnadu

ABSTRACT

Cloud computing has become one amongst the foremost essential in IT trade recently, watching the potential impact on its varied business applications to boot as in our life-style, it will be same that this troubled technology is here to remain. Several of the alternatives that build cloud computing partaking, haven't challenged the prevailing security system simply, however have created serious security problems. This paper provides association with nursing perspective, collaborate degree analysis of the prevailing cloud computing security problems supported by a full survey. Together, it makes a straight up clarification to the protection that challenges in coding system package as a Service (SaaS) model of cloud computing and along doesn't fail to produce future security analysis directions.

KEYWORDS : Cloud computing, Iaas, SaaS, PaaS, Virtual Machine and Security.

I. INTRODUCTION

Cloud Computing technology is in fact a well spoken subject by IT consultants, traders, entrepreneurs and freelance consultants although some believe it's a glitchy trend representing succeeding stages inside the evolution of the web, others believe it is a hardwire, as a results of it uses in earlier computing technologies[2]. From a user's perspective, cloud computing provides some way for getting computing services while not the necessity of everybody to understand each nook and cranny of it. From associate degree's perspective, cloud computing delivers services for shopper aboard with sure business needs. Tips for cloud computing, it's four altogether fully completely different preparation models notably personal, community, public and hybrid to boot as [3] altogether fully completely different deliver models that unit of measuring used inside a specific preparation model. These delivery models unit of measuring the SaaS (Software as a Service), PaaS (Platform as a Service) and IaaS (Infrastructure as a Service). These models kind the core of the cloud that they exhibit sure key characteristics like on demand self-service, broad network access, resource pooling, measured service and fast snap. Our main house of concern throughout this paper is that the pc code package as a service (SaaS) [7] model. This wonderful branch of cloud computing , may even be a delivery model within that applications unit of measuring hosted associate degreed managed in AN passing service provider's data center, obtained on a subscription basis and accessed via a browser over a web association.

It primarily deals with licensing of Associate in Nursing application to the purchasers to be used as a service on demand. This paper focuses on the problems associated with the security analysis in cloud computing services and delivery model of cloud computing. The paper describes the varied security problems with cloud computing with connectedness its service delivery model SaaS.

The organization of the paper is as follows: Section two describes the security challenges with protection problems that unit of measuring show by the pc code package as a Service (SaaS) delivery model. Section three lists kind of this solutions that target the protection challenges show by the SaaS. Section four provides exploits, section five provides integrity of cloud. Section six provides the current security solutions and conclusions derived out of the survey undertaken.

2. SECURITY CHALLENGES AND THREATS

Although the protection problems in ancient communication systems along apply to the cloud, the use of cloud computing introduces new attack vectors which can build attacks either getable or just easier to hold out. sort of the [5]standard security problems that along have an impact on the SaaS model unit represented below

2.1. Authentication and authorization

The authentication and authorization applications for enterprise environments might have to be modified, to figure with secure cloud surroundings. Forensics tasks might become way more powerful since the investigators will not be able to access system hardware physically.[15]They need planned an answer with de-facto standards of open authorization that there's a trust party auditor which maintains all the credentials and cloud supplier will unambiguously distinguish one user from totally different. Verification that is predicated on countersign, open account credit and out of band authentication. to boot, the theme along provides mutual authentication, identity management, session key institution, user privacy and security against several trendy attacks; but the formal security proofing hasn't however been formalized.

2.2. Security Threats

Cloud computing and net services run on a network structure in order that they area unit receptive network sort attacks. One in all these attacks is that the distributed denial of service attacks. If a user might hijack a server then the hacker might stop on-line the net services from functioning and demand a reason to place the services back online.[8] To prevent these attacks the utilization of syn cookies and limiting users connected to a server all facilitate stop a DDOS attack. Another such attack is that the man within the middle attack. If the Secure Sockets Layer (SSL) is incorrectly designed then consumer and server authentication might not behave needless to say so resulting in man within the middle attacks.

Another form of attack is network sniffing.[18]With packet human wrongdoer will capture sensitive knowledge if unencrypted like passwords and alternative net service connected security[10] configuration like the UDDI (Universal Description Discovery and Integrity), SOAP (Simple Object Access Protocol) and WSDL (Web Service Description Language) files. Port scanning is addition all, another threat which might be utilized by a wrongdoer. Port eighty is often opening attributable to it being the port that the net server sits on. But this will simply be encrypted and as long because the server computer code is designed properly then there ought to be no intrusion. Alternative attacks embrace SQL injection wherever a hacker will use special characters or terms to come back causeless knowledge as an example,[10] strings that will find yourself wherever clause of an SQL statement is also tricked into together with a lot of data. As an example a parameter price of X' or 1=1 could cause a full table to be came back as 1=1 is often seen as true. [12]Additionally cross web site scripting wherever inserting code into a field or universal resource locator that gets dead hands over management or sensitive knowledge to the wrongdoer. Eminent cross web site scripting attacks will cause buffer overflows, DOS attacks, inserting spyware and malicious code into visiting browsers and violation of user privacy.

Alternative such risks that area unit marked as high risk in cloud security are:

2.2.1. Loss of Governance

In mistreatment cloud infrastructures, the consumer essentially cedes management to the Cloud supplier (CP) on variety of problems which can have an effect on security. At an equivalent time, SLAs might not provide a [7] commitment to produce such services on the a part of the cloud supplier, so departure a niche in security defenses.

2.2.2. Lock-In

There's presently very little on provide within the means of tools, procedures or customary knowledge formats or services interfaces that would guarantee knowledge, application and repair immovability. [16]This will build it tough for the client to migrate from one supplier to another different or migrate knowledge and services back to an in- house IT surroundings. This introduces a dependency on a selected CP for service provision, particularly if knowledge movability, because the most elementary facet, isn't enabled.

2.2.3. Data Protection

Cloud computing poses many knowledge protection risks for cloud customers and suppliers. In some cases, it's going to be tough for the[18] cloud client (in its role as knowledge controller) to effectively check the information handling practices of the cloud supplier and so to make sure that the information is handled in an exceedingly lawful means. This drawback is exacerbated in cases of multiple transfers of information, e.g., between federate clouds. On the opposite hand, some cloud suppliers do give data on their knowledge handling practices.

2.2.4. Incomplete or Insecure knowledge Deletion

Once a call for participation to delete a cloud resource is created, like most in operation systems, this might not lead to true wiping of the information. Adequate or timely knowledge deletion may additionally be not possible either as result of additional copies of information area unit keep however aren't obtainable, or as a result of the disk to be destroyed additionally stores knowledge [9]from alternative purchasers.[3]Within the case of multiple tenancies and therefore the reprocess of hardware resources, this represents a better risk to the client than with dedicated hardware, terribly the same as that of a regular network. Alternative attacks which cannot be specific to the cloud area unit lack of physical authentication like bioscience and swipe cards. MIS configuration may additionally contribute to the loss of information or enable a hacker to realize entry. Others could embrace un-patched package computer code, use of un-trusted computer code and tools among the cloud

3. CLOUD SPECIFIC SECURITY CHALLENGES

3.1 Body Access to Servers and Applications

One of the foremost necessary characteristics of cloud computing is that it provide "self service" access to computing power, presumably via web.

In ancient [1] knowledge centers, body access to servers is controlled and restricted to direct or on-premise connections. In cloud computing, this body access should currently be conducted via web, increasing exposure and risk. it's very necessary to limit body access and monitor this access to keep up visibility of changes within the system management.

3.2. Dynamic Virtual Machines (DVM)

VM State and Sprawl Virtual machines are dynamic. They will quickly be reverted to previous instances, paused, and restarted simply. They will conjointly pronto clone and seamlessly [7] captive between physical servers. This dynamic nature and potential for VM sprawl makes it troublesome to realize and maintain consistent security. Vulnerabilities or configuration errors could also be inadvertently propagated

Also, it's troublesome to keep up associate degree auditable record of the safety state of a virtual machine at any given purpose in time. With in the cloud computing environments, it'll be necessary to be able to prove the safety state of a system, notwithstanding its location or proximity to alternative, probably insecure virtual machines.

4. VULNERABILITY EXPLOITS AND VM-TO-VM ATTACKS

Cloud computing servers use constant operational systems. Enterprise and internet applications as localized virtual machines and physical servers. The flexibility for associate degree offender or malware to remotely exploit vulnerabilities in these systems and applications may be a important threat to virtualized cloud computing environments. [9]Additionally co-location of multiple virtual machines will increase the attack surface and risk of VM-to-VM compromise. Intrusion find ion and interference system got to be able to detect malicious activity at the VM level notwithstanding the situation of the VM at intervals the virtualized cloud atmosphere.

5. KNOWLEDGE INTEGRITY: CO-LOCATION, COMPROMISE AND LARCENY

According to the 2008 knowledge breach Investigation Report conducted by Version Business Risk Team, fifty nine of knowledge breaches resulted from hacking and intrusions. Dedicated[2] resources are expected to be safer than shared resources. The attack surface in absolutely or partly shared cloud environments would be expected to be larger and cause inflated risk. Enterprises want confidence and auditable proof that cloud resources aren't being tempered with nor compromised, notably once residing on shared physical infrastructure software package and application files and activities got to be monitored.

6. CURRENT SECURITY SOLUTIONS

Every enterprise can have its own identity management system to regulate access to information and computing resources. Cloud suppliers either integrate the customer's identity management system into their own infrastructure, victimization federation or SSO technology, or offer associate degree identity management resolution of their own.The following outlines four distinct security technologies – firewall, intrusion, detection and interference, integrity observation and log inspection- that may be deployed as software package on virtual machines to extend protection and maintain compliance integrity of servers and applications as virtual resources move from on-premise to public cloud atmosphere.[18]

6.1. Firewall

Decreasing the attack surface of virtualized servers in cloud computing environments. A bi-directional firewall, deployed on individual virtual machines will offer centralized management of server firewall policy. [5]It ought to embrace predefined templates for common enterprise server sorts and change the following:

- Virtual Machine isolation.
- Fine-grained filtering (Source and Destination Address, Ports).
- Coverage of all IP-based protocols (TCP, UDP, ICMP, …)
- Coverage of all frame sorts (IP, ARP, …)
- Bar of Denial of Service (DoS) attacks.
- To Style policies per network interface.
- Location awareness to change tightened policy and therefore the flexibility to maneuver the virtual machine from on-premise to cloud resources.

6.2. Intrusion Detection and bar (IDS/IPS)

Shield vulnerabilities in software and enterprise applications till they will be patched, to attain timely protection against famous and zero-day attacks. As antecedently noted, virtual machines and cloud computing servers use an equivalent operational systems, enterprise and net applications as physical servers.[6] Deploying intrusion detection and bar as software package on virtual machines shields recently discovered vulnerabilities these applications and OSs to supply protection against exploits trying to compromise virtual machines.

6.2.1. Integrity Monitoring

Integrity watching of essential software and application files (files,directories, written record keys and values, etc.) is important for police work malicious and sudden changes that might signal compromise of [11]cloud computing resources. Integrity watching software package should be applied at the virtual machine level.

6.2.2. Log Inspection

Log scrutiny collects and analyzes software and application logs for security events. Log scrutiny rules optimize the identification of vital security events buried in multiple log entries. [14]These

events will be sent to a complete security system, however contribute to most visibility once forwarded to a security data and event management (SIEM) system or centralized work server for correlation, reportage and archiving. Like integrity watching, log scrutiny. [18] Capabilities should be applied at the virtual machine level Log scrutiny software package on cloud resources enables, suspicious behavior detection, assortment of security-related body actions and optimized assortment of security events across your datacenter.

7. CONCLUSION

This paper conclude the overall analysis of security in cloud computing consists of discussing the protection problems conclude that we should always take care regarding the protection issues, where as swing our business on Cloud. There are various measures and discussions with open analysis for challenges in cloud computing security that demand intensive analysis the protection model ought to be most likely secure. Security as a Service ought to be provided to the cloud users. Consequently, customers also ought to assure themselves that cloud applications square measure adequately secured for his or her specific functions, as well as their compliance obligations. The Consumer relies on cloud supplier to make sure the subsequent tasks information security and privacy, resources accessible, repairing and monitoring of services and resources. Finally, suppliers and customers should take into account legal problems, like Contracts E-Discovery, and therefore the connected laws, which can vary by country.

REFERENCES

[1]. L.Aruna and Dr.M.Aramudhan, text book for "Fundamentals of Cloud Computing", | ISBN No: 978-93- 5137-266-0. | | [2]. L.Aruna & Dr.M.Aramudhan,"A Novel Survey on SLA based Load leveling in Cloud Computing " International Journal of Research in Computer and Communication Technology, Vol 3, Issue 6, June- 2014-ISSN (Online) 2278- 5841and ISSN (Print) 2320- 5156 | | [3]. Ren K Et Al. 2009. Ensuring Data Storage Security in Cloud Computing. [Online] Available from: www.ece.iit.edu/~ubisec/IWQo S09.pdf [Accessed on 26th January [2011]. [2] Oracle.2009. | | [4]. Architectural Strategies for Cloud Computing. [Online] Available from: http://www.oracle.com/technology/architect/entarch/pdf/architectural_strategies_for cloud _com puting.pdf [Accessed on 26th Febuary2011] | | [5]. Scarfone K, Singhal A, Winograd T. 2007. Guide to Secure Web Services. [Online] Available from: http://csrc.nist.gov/publications/nistpubs/800-95/SP800-95.pdf[Accessed 26th Dec 2010]. | | [6]. Amazon Web Services. 2009. Amazon Virtual private Cloud. [Online] Available from: http://aws.amazon.com/vpc/ [Accessed 26th April 2010] [5] Yang A. 2003. | | [7]. Guide to XML Web Services Security. [Online] Available from: http://www.cgisecurity.com/ws/WestbridgeGuideToWebServicesSecurity.pdf[Accessed 26th April 2010] | | [8]. Catteddu D. 2010. Cloud Computing. [Online] Available from: http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment - [Accessed 26th April 2010] | | [9]. Cloud Computing Use Case Discussion Group. "Cloud Computing UseCases Version 3.0," 2010. | | [10]. ENISA. (2009, Feb) "Cloud computing: benefits, risks and recommendations for information security." available:www.enisa.europa.eu/act/rm/files/deliverables/cloud- | computing-risk-assessment [Jul. 10, 2010]. | | [11]. R. K. Balachandra, P. V. Ramakrishna and A. Rakshit. "Cloud Security Issues." In PROC „09 IEEE International Conference on Services Computing, 2009, pp 517-520. | | [12]. P. Kresimir and H. Zeljko "Cloud computing security issues and challenges." In PROC Third International Conference on Advances in Human-oriented and Personalized Mechanisms, Technologies, and Services, 2010, pp. 344-349. | | [13]. B. Grobauer, T. Walloschek and E. Stöcker, "Understanding Cloud Computing Vulnerabilities," IEEE Security and Privacy, vol. 99, 2010. | [14]. S. Subashini, and V. Kavitha. (2010) "A survey on security issues in service delivery models of cloud computing." J Network Comput Appl doi:10.1016/j.jnca.2010.07.006. Jul., 2010. | | [15]. Vikram Kumar , " Cloud Enables Better Governance," , Cisco India SAARC, on web - http://www.cisco.com /web/IN/about/network/governance.html. | | [16]. M. Armbrust, et al., "Above the Clouds: A Berkeley View of Cloud Computing," UC Berkeley Reliable Adaptive Distributed Systems LaboratoryFebruary 10 2009. | | [17]. .Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing, ver. 2.1," 2009. | | [18]. www.computer.org/cloud computing-- May 2014 issue. |