ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 3, pp: (205-207), Month: July - September 2014, Available at: www.researchpublish.com

SECURITY IN CLOUD COMPUTING

ANJANA.R

STUDENT, SAVEETHA SCHOOL OF ENGINEERING, CHENNAI

Abstract: **Cloud computing has become one of the most essential in IT trade recently. Looking at the potential impact on it's varied business applications additionally as in our life-style, it'll be same that this troubled technology is here to stay. Many of the choices that build cloud computing partaking, haven't challenged the prevailing security system merely, but have created serious security issues. This paper provides association with nursing perspective, collaborate degree analysis of the prevailing cloud computing security issues supported by a full survey. Together, it makes a straightup clarification to the protection that challenges in computer code package as a Service (SaaS) model of cloud computing and together doesn't fail to supply future security analysis instructions.**

Keywords: **Cloud computing, saas, Security.**

I. INTRODUCTION

Cloud Computing technology is of course a well spoken subject by IT consultants, traders, enterprenuers and freelance consultants though some believe it is a glitchy trend representing succeeding stages within the evolution of the internet, others believe it's a hardwire, as a result of it uses in earlier computing technologies. From a user's perspective, cloud computing provides a way for obtaining computing services without the need of everyone to know every nook and cranny of it. From associate degree's perspective, cloud computing delivers services for shopper alongside with certain business desires. Tips for cloud computing, it's four wholly completely different preparation models notably personal, community, public and hybrid additionally as three wholly completely different deliver models that unit of measurement used within a particular preparation model. These delivery models unit of measurement 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 which they exhibit certain key characteristics like on demand self-service, broad network access, resource pooling, measured service and quick snap. Our main house of concern throughout this paper is that the computer code package as a service (SaaS) model. This glorious branch of cloud computing , could also be a delivery model inside that applications unit of measurement hosted associate degreed managed in an passing service provider's knowledge center, obtained on a subscription basis and accessed via a browser over an internet 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 issues related to the service delivery model of cloud computing. The paper describes the various security issues with cloud computing with relevancy its service delivery model SaaS. The organization of the paper is as follows: Section 2 describes the protection issues that unit of measurement show by the computer code package as a Service (SaaS) delivery model. Section 3 lists variety of this solutions that half target the protection challenges show by the SaaS. Section four provides conclusions derived out of the survey undertaken.

II. SECURITY CHALLENGES

Although the protection issues in ancient communication systems together apply to the cloud, the employment of cloud computing introduces new attack vectors which will build attacks either getable or simply easier to carry out. variety of the quality security issues that together have a control on the SaaS model square measure described below:

- ***Authentication and authorization:***

The authentication and authorization applications for enterprise environments may need to be changed, to work with a secure cloud surroundings. Forensics tasks may become far more powerful since the investigators won't be ready to access system hardware physically. they have planned a solution with de-facto standards of open authorization {in that|during that|within which} there is a trust party auditor which maintains all the credentials and cloud provider can unambiguously distinguish one user from different.

Verification, that's predicated on countersign, charge account credit and out of band (i.e. strong two factors) authentication. to boot, the theme together provides mutual authentication, identity management, session key establishment, user privacy and security against many stylish attacks; however the formal security proofing hasn't but been formalized.

III. CLOUD SPECIFIC SECURITY CHALLENGES

- ***Administrative Access to Servers and Applications:***

One of the most important characteristics of cloud computing is that it offer "self service" access to computing power, most likely via internet. In traditional data centers, administrative access to servers is controlled and restricted to direct or on-premise connections. In cloud computing, this administrative access must now be conducted via internet, increasing exposure and risk. It is extremely important to restrict administrative access and monitor this access to maintain visibility of changes in the system control.

- ***Dynamic Virtual Machines:***

VM State and Sprawl Virtual machines are dynamic. They can quickly be reverted to previous instances, paused and restarted, relatively easily. They can also readily clone and seamlessly moved between physical servers. This dynamic nature and potential for VM sprawl makes it difficult to achieve and maintain consistent security. Vulnerabilities or configuration errors may be unknowingly propagated. Also, it is difficult to maintain an auditable record of the security state of a virtual machine at any given point in time. In the cloud computing environments, it will be necessary to be able to prove the security state of a system, regardless of its location or proximity to other, potentially insecure virtual machines.

IV. VULNERABILITY EXPLOITS AND VM-TO-VM ATTACKS

Cloud computing servers use the same operating systems. Enterprise and web applications as localized virtual machines and physical servers. The ability for an attacker or malware to remotely exploit vulnerabilities in these systems and applications is a significant threat to virtualized cloud computing environments. In addition co-location of multiple virtual machines increases the attack surface and risk of VM-to-VM compromise. Intrusion detection and prevention system need to be able to detect malicious activity at the VM level regardless of the location of the VM within the virtualized cloud environment.

V. DATA INTEGRITY: CO-LOCATION, COMPROMISE AND THEFT

According to the 2008 Data breach Investigation Report conducted by Version Business Risk Team, 59% of data breaches resulted from hacking and intrusions. Dedicated resources are expected to be more secure than shared resources. The attack surface in fully or partially shared cloud environments would be expected to be greater and cause increased risk. Enterprises need confidence and auditable proof that cloud resources are not being tempered with nor compromised, particularly when residing on shared physical infrastructure. Operating system and application files and activities need to be monitored

VI. CURRENT SECURITY SOLUTIONS

The following outlines four distinct security technologies –firewall, intrusion detection and prevention, integrity monitoring and log inspection- that can be deployed as software on virtual machines to increase protection and maintain compliance integrity of servers and applications as virtual resources move from on-premise to public cloud environment.

Firewall:

Decreasing the attack surface of virtualized servers in cloud computing environments. A bi-directional firewall, deployed on individual virtual machines can provide centralized management of server firewall policy. It should include predefined templates for common enterprise server types and enable 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 types (IP, ARP, …)
- Prevention of Denial of Service (DoS) attacks
- Ability to design policies per network interface
- Location awareness to enable tightened policy and the flexibility to move the virtual machine from on-premise to cloud resources.

- ***Intrusion Detection and Prevention (IDS/IPS):***

Shield vulnerabilities in operating system and enterprise applications until they can be patched, to achieve timely protection against known and zero-day attacks. As previously noted, virtual machines and cloud computing servers use the same operating systems, enterprise and web applications as physical servers. Deploying intrusion detection and prevention as software on virtual machines shields newly discovered vulnerabilities these applications and OSs to provide protection against exploits attempting to compromise virtual machines.

- ***Integrity Monitoring*:**

Integrity monitoring of critical operating system and application files (files,directories, registry keys and values, etc.) is necessary for detecting malicious and unexpected changes which could signal compromise of cloud computing resources. Integrity monitoring software must be applied at the virtual machine level.

- ***Log Inspection:***

Log inspection collects and analyzes operating system and application logs for security events. Log inspection rules optimize the identification of important security events buried in multiple log entries. These events can be sent to a stand-alone security system, but contribute to maximum visibility when forwarded to a security information and event management (SIEM) system or centralized logging server for correlation, reporting and archiving. Like integrity monitoring, log inspection.

Capabilities must be applied at the virtual machine level. Log inspection software on cloud resources enables:

- Suspicious behavior detection
- Collection of security-related administrative actions
- Optimized collection of security events across your datacenter.

VII. CONCLUSION

After discussing the security issues this paper conclude that we should be careful about the security concerns while putting our business on Cloud. There are open research challenges in cloud computing security which demand intensive research. The security model should be probably secure. Security as a Service should be provided to the cloud users.