Research Paper *IJBARR*
Impact Factor: 3.853 *E- ISSN -2347-856X*
Refereed, Listed & Indexed *ISSN -2348-0653*

PERFORMANCE ANALYSIS OF SECURITY IN CLOUD COMPUTING INFRASTRUCTURES

S.Nagasundaram* Dr.S.K.Srivatsa**
**Research Scholar, SCSVMV University, Kancheepuram, Tamil Nadu, India.*
***Guide,SCSVMV University, Kancheepuram, Tamil Nadu, India.*

Abstract
Cloud computing has been developed and deliver information technologies services in an internet based computing, where shared resources, software and information, are provided to computers and device on-demand. Cloud computing diverse facilitation components like hardware, software and firmware, networking and service integrate to offer different computational facilities while internet provides the backbone to deliver the services. We analysis and architecture for incorporating different security scheme, particularly Infrastructure-as-a-Services(IaaS), Platform-as-a-Service(PaaS) and Software-as-a-service.

Keywords: Cloud Computing, Resources, IaaS, PaaS, SaaS and Security.

Cloud Service Models

IaaS – Infrastructure as a service is referred as Resource cloud. The success rate of data access defines the quality of these cloud servers. As Infrastructure can be dynamically scaled up (or) down based on the need of application resources. It helps to multiple tenants at the same time[i].

PaaS – Platform as a service is supply computational resources via a platform which application and services can be urbanized and hosted. The PaaS supplies all the resources for downloading and uploading or building an application services via the internet[ii].

SaaS – Software as a service is also referred as application or service cloud which hosts the applications as a service to its various cloud users via Internet[iii].

Namely, the categories are: network security, interfaces, data security, virtualization, governance, compliance and legal issues. Each category includes several potential security problems, resulting in a classification with subdivisions that highlights the main issues identified in the base references:[iv]

1. **Network security**: Problems associated with network communications and configurations regarding cloud computing infrastructures. The ideal network security solutionis to have cloud services as an extension of customers' existing internal networks[v], adopting the same protection measures and security precautions that are locally implemented and allowing them to extend local strategies to any remote resource or process[vi].

a. **Transfer security**: Distributed architectures, massive resources haring and virtual machine (VM) instances synchronization imply more data in transit in the cloud, thus requiring VPN mechanisms for protecting the system against sniffing, spoofing, man-in-the-middle and side-channel attacks.
b. **Firewalling**: Firewalls protect the provider's internal cloud infrastructure against insiders and outsiders. They also enable VM isolation, fine-grained filtering for addresses and ports, prevention of Denial-of-Service (DoS) and detection of external security assessment procedures. Efforts for developing consistent firewall and similar security measures specific for cloud environments[vii] reveal the urge for adapting existing solutions for this new computing paradigm.
c. **Security configuration**: Configuration of protocols, systems and technologies to provide the required levels of security and privacy without compromising performance or efficiency.

2.**Interfaces**: Concentrates all issues related to user, administrative and programming interfaces for using and controlling clouds.

a. API: Programming interfaces (essentialto IaaS and PaaS) for accessing virtualized resources and systems must be protected in order to prevent malicious use.
b. **Administrative interface**: Enables remote control of resources in an IaaS (VM management), development for PaaS(coding, deploying, testing) and application tools for SaaS (user access control, configurations).
c. **Userinterface**: End-user interface for exploring provided resources and tools (the service itself), implying the need of adopting measures for securing the environment.

d. Authentication: Mechanisms required to enable access to the cloud. Most services rely on regular accounts[viii] consequently being susceptible to aplethora of attacks whose consequences are boosted by multi-tenancy and resource sharing.

3. **Datasecurity**: Protection of data interms of confidentiality, availability and integrity (which can be applied not only to cloud environments, but any solution requiring basic security levels).

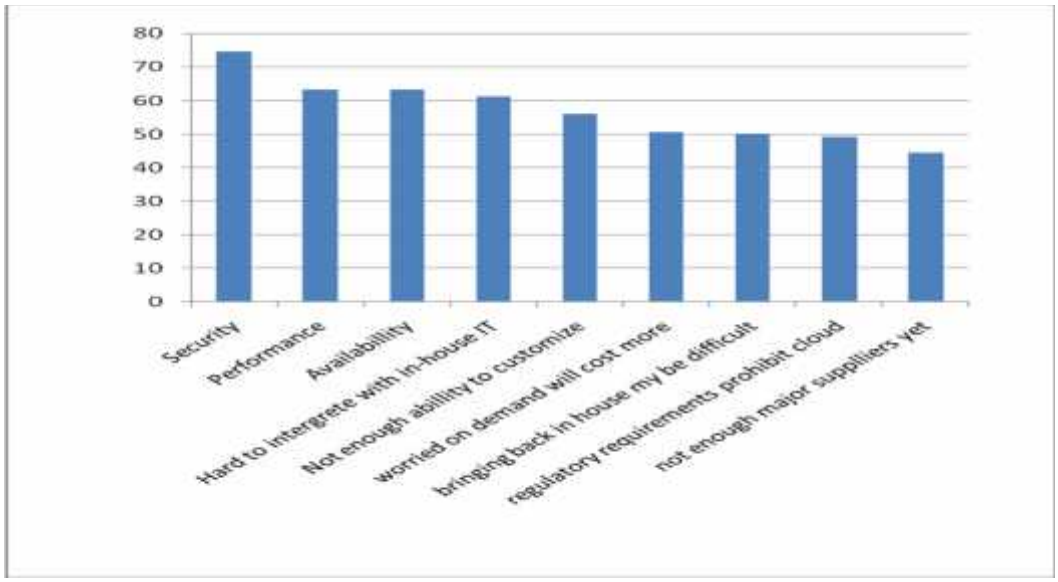
a. **Cryptography**: Most employed practice to secure sensitive data, thoroughly required by industry, state and federal regulations.
b. **Redundancy**: Essential to avoid data loss. Most business models rely on information technology for its core functionalities and processes[ix] and, thus, mission-critical data integrity and availability must be ensured.
c. **Disposal**: Elementary data disposal techniques are insufficient and commonly referred as deletion. In the cloud, the complete destruction of data, including log references and hidden backup registries, is an important requirement.

Importance of Security in Cloud Computing

The security controls and protocols in clouds are those which are used in other IT environments but in cloud environment the security control is performed by the providers instead of the users. An issue which can contain a lot of risks because the security provisions might not be paid enough attention during data – transmission by the CSP or ever the SLAs might not include all necessary rules for security services.

The given statistical resulted graph represents the results of the survey which was conducted by the International Data Corporation in August, 2008 amongst senior business executives and IT professionals regarding the challenges / issues which mainly affect the performance of Cloud Computing. And the survey results show security at the top of the list which declares its importance compared to other parameters of Cloud Computing.

The security result shows that the security is the major challenge amongst all the parameters that affect the performance and growth of Cloud Computing[x].



Importance security issues in the cloud

Even though, the virtualization and cloud computing delivers wide ranges of dynamic resources, the security concern is generally perceived as the huge issue in the cloud which makes the users to resist themselves in adopting the technology of Cloud Computing[xi]. Some of the security issues in the Cloud are discussed below:

Integrity: Integrity makes sure that data held in a system is a proper representation of the data intended and that it has not been modified by an authorized person. When any application is running on a server, backup routine is configured so that it is safe in the event of a data-loss incident. Normally, the data will backup to any portable media on a regular basis which will then be stored in an off-site location[xii].

Availability: availability ensures that data processing resources are not made unavailable by malicious action. It is the simple idea that when a user tries to access something, it is available to be accessed. This is vital for mission critical systems. Availability for these systems is critical that companies have business continuity plans in order for their systems to have redundancy[xiii].

Confidentiality: Confidentiality ensures that data is not disclosed to unauthorized persons. Confidentiality loss occurs when data can be viewed or read by any individuals who are unauthorized to access it. Loss of confidentiality can occur physically or electronically. Physical confidential loss takes place through social engineering. Electronic confidentiality loss takes place when the clients and servers aren't encrypting their communications[xiv].

Trust:- "Trust is a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behavior of another". Trust can be classified by hard trust (security oriented) and soft trust (non-security)[xv].

Related work: There are three ways of data lose due to the cloud computing systems. Like Network security, Software security and Data Security systems. The three ways has to occur the data loss but we should use different types of Encryption and Decryption algorithms using for secure the data.

Conclusion: Cloud computing is waste and tremendous systems. We will implement and prevent protect will the systems. The analysis conclusion is the major factors are security is the major three environment of software, hardware and data security are to have the necessary level of functional.

Reference

[i] Cloud Computing: Web-Based Applications That Change the Way You Work and Collaborate Online, by Michael Miller.
[ii] A Security Aspects in Cloud Computing by Gurudatt Kulkarni & Jayant Gambhir 978-1-4673-2008-5/12 ©2012 IEEE
[iii] Cloud Computing book by Gavin O Donnell, Nigel McKelvey and Kevin Curran.
[iv] A quantitative analysis of current security concerns and solutions for cloud computing NelsonGonzalez, CharlesMiers, FernandoRed´ıgolo, MarcosSimpl´ıcio, TerezaCarvalho, MatsN¨aslund and Makan Pourzandi, JournalofCloudComputing: Advances, Systems and Applications 2012,1:11 http://www.journalofcloudcomputing.com/content/.
[v] TompkinsD(2009) Security for Cloud-based Enterprise Applications. http://blog.dt.org /index. php/2009/02/security-for-cloud-based enterprise-applications/.
[vi] Jensen M, SchwenkJ, Gruschka N, IaconoLL (2009) On Technical Security Issues in Cloud Computing. In:IEEE Internation Conference on Cloud Computing. pp109–116.
[vii] GenoveseS(2009)AkamaiIntroducesCloud-Based Firewall. http:// cloudcomputing.sys-con.com /node/
[viii] Google(2011)GoogleQueryLanguage(GQL).
[ix]LyleM(2011)Redundancy in Data Storage. Define the Cloud
[x]ENISA,Cloud Computing:benefits, risks and recommendation for information security", www.enisa.europa.eu/act/ rm/files/delivarables/cloud-computing-risk-assesment/at_download/full Report.
[xi] Cloud computing Alliance(CSA) http://www..cloud securityalliance.org/.
[xii] Peter Mell, and Tim Grance, "The NIST Definition of Cloud Computing," Version 15, 10-7-09, http://www.wheresmyserver.co.nz / storage /media/faq-files/cloud-def-v15.pdf.
[xiii] Ramgovind S, Eloff MM, Smith E, "The Management of Security in Cloud Computing"2010 IEEE.
[xiv] Mather, T., Kumaraswamy, S., & Latif, S. (2009). Cloud Security and Privacy. O'Reilly.
[xv] McFedries, P. (2008). The Cloud Is The Computer. IEEE Spectrum, 42–50.