IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Research Paper on Cyber Security in Cloud Infrastructure

[1] Aniket Ghate

[1] PG Scholar

[1] Computer Science & Engineering

[1] Sipna College Of Engineering And Technology,

Amravati, Maharashtra, INDIA

Abstract

Cloud computing is predicted to vary the way information technology (IT) is employed and managed better cost efficiency, faster innovation, faster time-tomarket, and therefore the ability to scale Application on Demand (Leighton, 2009). per Gartner, while the hype grew rapidly Released from 2008 and onwards, it's clear that the cloud computing model has undergone a serious change. And the benefits will be significant (Gartner HypeCycle, 2012). However, because cloud Computing is emerging and rapidly evolving conceptual and real, legal/contractual, Financial, quality of service, interoperability, security, and privacy issues are still significant challenges. In this paper, we describe the varied services and deployment models of cloud computing and identify the key ones. challenges. Specifically, we discuss three serious challenges: regulatory, security, and privacy issues in cloud computing.

Keywords

Cloud Computing, Security Metrics, Security Threats, Security Measurement Frameworks

I. Introduction

In this Research Paper we recognize the risks and security features that apply to cloud computing & also choose one Appropriate framework for the identification of information security metrics. In addition, we identify SLA-based Information security metrics in the cloud in conjunction with the COBIT framework. We conducted a systematic literature review (SLR) that focused on studying Information Security Threats in Cloud Computing & also used SLR to select the available infrastructure To identify security metrics we used Engineering Village and Scopus Online Quotes Database as the primary source of data for SLR. The study was selected on the basis of inclusion/exclusion. The criteria define a suitable framework was selected based on the selection criteria of the defined framework. We identified SLAs based on a conceptual review of the selected framework and the COBIT framework. Based on information security metrics in the cloud definitive study objectives that point us towards achieving our objectives:

i) Identify relevant information security properties for cloud computing

ii) Identify information security risks for cloud computing

iii) Choose the right framework for developing security metrics

iv) Identify SLA based information security metrics aligned in cloud computing COBIT Framework

II. Literature survey

Cloud computing is clearly one of the most enticing technology areas of the current times due, at least in part to its costefficiency and flexibility. However, despite the surge in activity and interest, there are significant, persistent concerns about cloud computing that are impeding the momentum and will eventually compromise the vision of cloud computing as a new IT procurement model. Despite the trumpeted business and technical advantages of cloud computing, many potential cloud users have yet to join the cloud, and those major corporations that are cloud users are for the most part putting only their fewer sensitive data in the cloud. Lack of control is transparency in the cloud implementation – somewhat contrary to the original promise of cloud computing in which cloud implementation is not relevant. Transparency is needed for regulatory reasons and to ease concern over the potential for data breaches. Because of today's perceived lack of control, larger companies are testing the waters with smaller projects and less sensitive data. In short, the potential of the cloud is not yet being realized.

In recent years, cloud computing is a technology of rapid development, however, the security problems have become obstacles to make the cloud computing more popular which must be solved. This paper analyzed the present situation of the development of cloud computing, and the security problems, and proposed a cloud computing security reference model. The model put forward a series of solutions for the present security problems cloud computing meet, but technology realization needs more organizations and individuals to join into the cloud computing security research. At the same time, cloud computing security is not just a technical problem, it also involves standardization, supervising mode, laws and regulations, and many other aspects, cloud computing is accompanied by development opportunities and challenges, along with the security problem be solved step by step, cloud computing will grow, the application will also become more and more widely.

We have learnt that electronic citation databases works based on semantic analysis. However, overtime concepts especially in technology changes. Therefore, researchers need to be aware of these changes in order to obtain reliable search results. We found that the security in cloud computing architecture is challenging as the subject of cloud computing itself is still developing and evolving. Considering the case of Europe, cloud computing is emerging in the region. This situation has necessitated us to obtain information of this study only based on systematic literature review of published academic studies. Nevertheless we believe cloud computing gains attention from IT professionals in industry now and even much more in the future. Several researchers also believe that cloud computing will be widely integrated in the industry. In spite of immature state of cloud computing, the study identified SLA based information security metrics in cloud computing environment as the end results. As a potential future work we can demonstrate the output of this study in academia or industry for validation.

Security estimation of software must be a mandatory feature of software at early stage of development life cycle. Unifying security attributes, security models, security metrics and software characteristics, security estimation is possible at the early stage of software development life cycle [7, 19]. For the security estimation mechanism, there is a need to develop efficient security metrics, and for the development of security metrics, a metric development framework is required. A framework for the identification of security metrics has been proposed. The framework includes all issues related to security metrics, which are contributing to security quantification.

III. Current Design and Future Approach

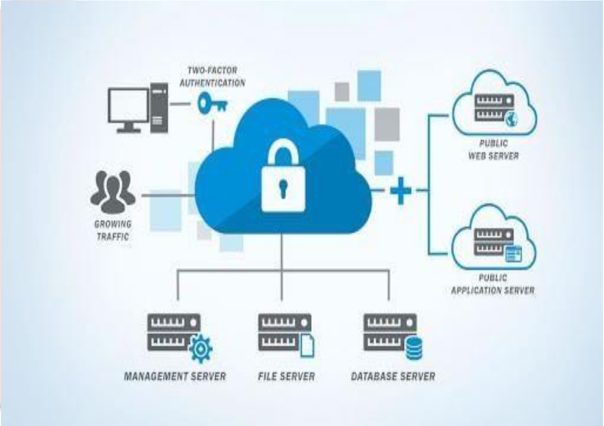

Fig : Cyber Security on Cloud Information

Cloud computing solutions support corporate processes by leveraging an Internet-based service." Because secrecy and security are among the most questioned aspects of cloud computing, there is always the possibility that user data will be viewed by others. Data has become particularly sensitive to a variety of risks due to its abundance and quantity, as well as the ability of computer systems or software to interchange and utilize it. The move to the cloud has introduced new security concerns. Because cloud computing services are accessible via the internet, anyone with the appropriate credentials can use them.

Improving security on cloud infrastructure strategy requires meeting specific cybersecurity standards and objectives.

Typically, services are assigned to standard ports, allowing them to be attacked even without assumption. We propose dynamically assigning ports to servers, as well as finer-grained whitelisting of IP addresses and other improvements. This allows firewalls to have a stronger impact on server access.

IV. Conclusion

We discuss the above research paper & hence we concluded the system which proposed security merits of cloud. This paper contains all security metrics which are contributing to protect cloud from threats. The further improvisation of system is possible as the classifier and datasets are trained.

Reference

[1]. Somani, U., Lakhani, K., Mundra, M.: Implementing digital signature with RSA encryption algorithm to enhance the Data Security of cloud in Cloud Computing. In: 1st International Conference on Parallel Distributed and Grid Computing (PDGC 2010), p. 211 (2010)

[2]. Ting Chen, Hongtian Zhao Xiaowei Yan The Research and Design of Cloud Computing Security Framework

[3]. B. R. Kandukuri, V. R. Paturi, and A. Rakshit, "Cloud security issues," 2009 IEEE [International Conference on Services Computing (SCC). pp. 517-20.

[4]. S. Chandra, and R. A. Khan, "Software security metric identification framework (SSM)," Proceedings of the International Conference on Advances in Computing,

Communication and Control, ICAC3'09. pp. 725-731.

[5] K. Jeffery, and B. Neidecker-Lutz, The Future of Cloud Computing Opportunities

for European Cloud Computing Beyond 2010, European Commission Information

Society and Media.

[6] R. Barga, J. Bernabeu-Auban, D.

Gannon et al., "Cloud computing architecture and application programming," SIGACT News, vol. 40, no. 2, pp. 94-5, 2009.

[7] B. R. Kandukuri, V. R. Paturi, and A.

Rakshit, "Cloud security issues," 2009 IEEE

International Conference on Services Computing (SCC). pp. 517-20.

[8] S. I. Hayes, "Metrics for IT outsourcing Service Level Agreements,"

http://www.clarityconsulting.com/MetricsforITout sourcing.pdf , 2004].

[9] GoGrid, "GoGrid Service Level Agreement (SLA),"

http://www.gogrid.com/legal/sla.php, [August 10, 2010, 2010].

[10] R. Clarke, "User Requirements for Cloud Computing Architecture," Proceedings

2010 10th IEEE/ACM International Conference on Cluster, Cloud and Grid Computing

(CCGrid). pp. 625-30.

[11] D. Winder, “What's in store for 2010?,” Infosecurity, vol. 7, no. 1, pp. 10-15, 2010. [12] M. Peter, and G. Tim. "The NIST Definition of Cloud Computing," 19 June, 2010.

[13] T. Mather, S. Kumaraswamy, and S. Latif, Cloud Security and Privacy An

Enterprise Perspective on Risks and Compliance: O'Reilly, 2009.