iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** XII **Month of publication:** December 2017

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 5 Issue XII December 2017- Available at www.ijraset.com

Study of Different Security Solutions for Cloud Environment

Anand Singh[1], Prof. (Dr.) Amod Kumar Tiwari[2]
[1]*Ph.D. Research Scholar, Department of Computer Science and Engineering, Sai Nath University, Ranchi, Jharkhand, India*
[2]*Director, Naraina College of Engineering and Technology, Kanpur, Uttar Pradesh, India*

Abstract: ***The security of the cloud is ensured in many levels, but the scope of intrusions makes it necessary to understand the factors that affect cloud security. In this paper we review the different security solutions which are currently being used now a day.***
Keywords: Cloud Computing, Cloud Security, Data Security, Cloud Privacy

I. INTRODUCTION

Cloud computing utilizes three delivery models by which different types of services are delivered to the end user. The three delivery models are the SaaS, PaaS and IaaS which provide infrastructure resources, application platform and software as services to the consumer. These service models also place a different level of security requirement in the cloud environment. IaaS is the foundation of all cloud services, with PaaS built upon it and SaaS in turn built upon it. Just as capabilities are inherited, so are the information security issues and risks. There are significant trade-offs to each model in the terms of integrated features, complexity vs. extensibility and security. If the cloud service provider takes care of only the security at the lower part of the security architecture, the consumers become more responsible for implementing and managing the security capabilities.

A recent survey by Cloud Security Alliance (CSA) and Institute of Electrical and Electronics Engineers (IEEE) indicates that enterprises across sectors are eager to adopt cloud computing but that security are needed both to accelerate cloud adoption on a wide scale and to respond to regulatory drivers. It also details that cloud computing is shaping the future of IT but the absence of a compliance environment is having dramatic impact on cloud computing's growth. Organizations using cloud computing as a service infrastructure, critically like to examine the security and confidentiality issues for their business critical insensitive applications. Yet, guaranteeing the security of corporate data in the "cloud" is difficult, if not impossible, as they provide different services like SaaS, PaaS, and IaaS.

SaaS is a software deployment model where applications are remotely hosted by the application or service provider and made available to customers on demand, over the Internet. The SaaS model offers the customers with significant benefits, such as improved operational efficiency and reduced costs. SaaS is rapidly emerging as the dominant delivery model for meeting the needs of enterprise IT services.

IaaS completely changes the way developers deploy their applications. Instead of spending big with their own datacentre or managed hosting companies or colocation services and then hiring operations staff to get it going, they can just go to Amazon Web Services or one of the other IaaS providers, get a virtual server running in minutes and pay only for the resources they use.

PaaS is one layer above IaaS on the stack and abstracts away everything up to OS, middleware, etc... This offers an integrated set of developer environment that a developer can tap to build their applications without having any clue about what is going on underneath the service. It offers developers a service that provides a complete software development lifecycle management, from planning to design to building applications to deployment to testing to maintenance. Everything else is abstracted away from the "view" of the developers. The dark side of PaaS is that, these advantages itself can be helpful for a hacker to leverage the PaaS cloud infrastructure for malware command and control and go behind IaaS applications.

II. APPLICATION AND DATA TRANSMISSION SECURITY

Security in cloud is a promising topic of research, already addressed in many research and academic publications. A good overview of the issues in cloud is provided by Molnar and Schechter [1] who investigated the pros and cons of storing and processing data by the public cloud provider with regards to security. They detail about the new forms of technological, organizational, and jurisdictional threats resulting from the usage of cloud, as they also provide a selection of countermeasures.

The different threat and attack models given by Akhawe et al[2] can be used to formally analyze the attacks in cloud

computing scenarios. However, their approach is limited to HTTP communication only. The model does not take into account application layer messages.

Youngmin Jung and Mokdong Chung[3] proposed an Adaptive security management model for cloud computing algorithm. They suggest an adaptive access algorithm to decide the access control to the resources using an improved Role Based Access Control (RBAC) technique. The proposed model determines dynamically security level and access control for the resources. But this model is based on provision of security based on cloud providers' decision and mainly considers different types of resources to arrive at the security level and access control. This model is targeted towards decisions of the client and services along with the resources to arrive at security levels. Also, this model is framed considering the cloud provider also as an third party untrusted provider, thus making the system non-vulnerable even at the hands of the provider.

Gruschka and Lo Iacono[4] showed how XML Signature wrapping attacks can be performed to attack Amazon's EC2 service. They detailed a vulnerability that enabled an attacker to execute operation on the cloud control, while having possession of a signed control message from a legitimate user. Manal and Yunis[5] outlined six security considerations for cloud computing namely resource sharing, data ownership, reduced encryption in favor of speed, refusal of services, data loss due to technical failure and attackers going after provider or the implementation. He also proposes a theoretical model for overcoming these issues through management of policies. For example, he proposes to classify the policies based on different types of data, like Client financial data, Intellectual property and so on. But creation and management of these policies are practically cumbersome and inefficient. Though many of the security issues in the past were due to inefficient policies, enabling an efficient policy is next to impossible. Policies can only be an additional measure but as long as the security framework is not efficient, even the most strategically created security policy will fail. One of the recently exploited vulnerability is the Cloudburst exploitation of vulnerability in VMware display functions in order to execute code from within a guest VM into the controlling host. Once exploited, the exploit tunnels a connection over the frame buffer of the guest to communicate with the host (Immunity 2017[6]). Our framework provides a different solution to tackle this situation which is irrespective of the policies being executed in the guest or host VM's. The finest security solution for web applications is to develop a development structure that has strong security architecture. Tsai et al [7] put forth a four-tier framework for web-based development that though seems attractive, only implies a security feature in the process. "Towards best practices in designing for the cloud" by Berre et al[8] is a road map toward cloud-centric development and the X10 language is one method to attain improved use of cloud capabilities of substantial parallel processing and concurrency as acknowledged by Sarawat and Vijay [9]. Raj et al [10] suggest resource seclusion to guarantee security of data during processing, by separating the processor caches in virtual machines, and isolating those virtual caches from the hypervisor cache. Hayes points out that there is no way to know if the cloud providers correctly deleted a client's purged data, or whether they saved it for some unidentified reason.

III. DATA STORAGE SECURITY

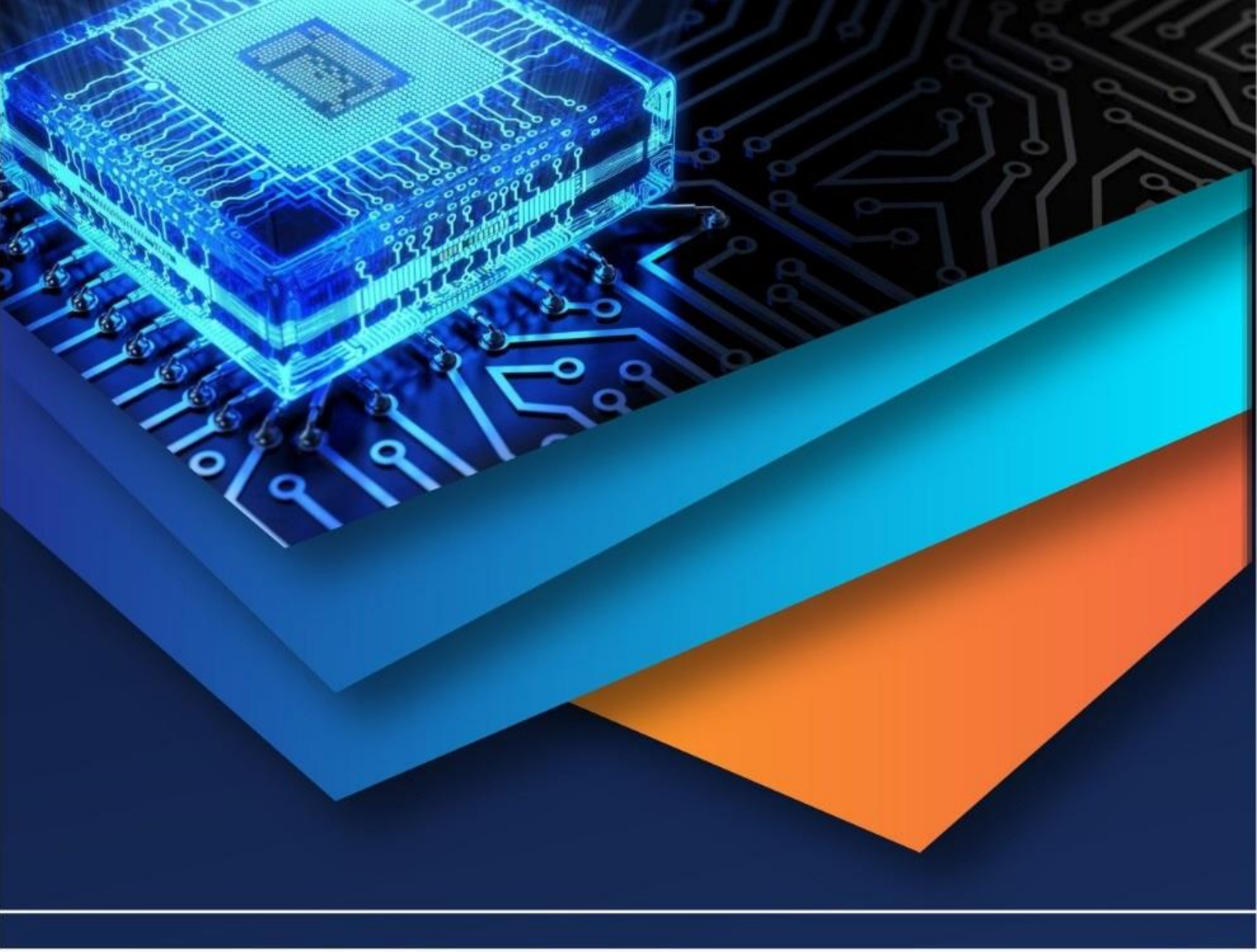
Hayes[11] points out an attractive crinkle here, "Permitting a third-party service to take custody of personal documents raises awkward questions about control and ownership: If you move to a competing service provider, can you take a data with you? Could you lose access to documents if you fail to pay a bill?" . The issues of privacy and control cannot be resolved, but only assured with tight service-level agreements (SLAs) or by keeping the cloud itself private. One straightforward solution, to be a extensively used solution for UK businesses is to simply use in-house "private clouds". Nurmi et al[12] illustrated a preview of one of the available home-grown clouds in their presentation "The Eucalyptus Open-Source Cloud-Computing System". Ignoring fragmentation with respect to providing security, data fragmentation is not a new concept. Concepts like these are already in use for providing optimization of data access in distributed systems. But most of them do not take security as the concern for fragmentation. One such work is regarding fragmentation and allocation of data in distributed database systems done by Katja et al[13]. Here they propose a model to fragment data horizontally or vertically with relation to the tuples so that data can be accessed or updated in an optimized manner. Another work is related to enhancement of Adaptive Data Replication Algorithm (ADRW) algorithm to achieve dynamic fragmentation and object allocation in distributed databases is done by Azzam et al (2007). Here they deal more about the cost involved in accessing data fragments from remote sites. These algorithms provide optimal ways to re-arrange and access data that are fragmented and stored in different locations. The main concerns in these works are to fragment data on the basis of easy retrieval but not relating to providing security to the data under consideration. Fragmentation of data based on relevance to data value is not targeted in any of the works. Fragmentation based on meta data is used in some works but those considerations are truly based on relevance to optimize data access rather than to the security of the data itself.

IV. CONCLUSION

Cloud security is not to be confused with security software offerings that are "cloud- based". The scope of the cloud security spans across all the three service delivery models deployed in any of the four cloud deployment models (private, public, hybrid and community cloud) and exhibiting the five essential characteristics of the cloud. It is this span of the scope of security in the cloud that makes it very important and at the same time much complicated. In this paper we reviewed and analysed various solutions which are being used now a days for securing cloud applications.

REFERENCES

[1] Molnar, D. and Schechter, S. "Self hosting vs. cloud hosting: Accounting for the security impact of hosting in the cloud", In Proceedings of the Ninth Workshop on the Economics of Information Security (WEIS), 2010
[2] Akhawe, D., Barth, A., Lam, P. E., Mitchell, J.C. and Song, D. "Towards a formal foundation of web security", CSF, pp. 290-304,2010.
[3] Youngmin, J. and Mokdong, C. "Adaptive security management model in cloud computing environment", In the 12th International Conference on Advanced Communication Technology (ICACT), pp 1664-1669,2010
[4] Gruschka, N. and Iacono, L. "Vulnerable Cloud: SOAP Security Revisited", In Proceedings of the IEEE International Conference on Web Services , IEEE Computer Society, pp. 625-631, 2009.
[5] Manal, M.Y. "A 'cloud-free' security model for cloud computing", In the International Journal of Services and Standards, Vol.5, No.4, pp. 354-375, 2009
[6] "Immunity CANVAS Professional", http://immunityinc.com/news- latest.shtml, (accessed : 10 Nov 2017), 2017
[7] Tsai, W., Jin, Z. and Bai, X. "Internetware computing: issues and perspective", In the Proceedings of the First Asia-Pacific Symposium on Internetware, ACM, Beijing, China, pp. 1-10, 2009.
[8] Berre, A.J., Roman, D., Landre, E., Heuvel, W.V.D., Skar, L.A., Udnaes, M. and Lennon, R. "Towards best practices in designing for the cloud", In Proceeding of the 24th ACM SIGPLAN conference companion on Object oriented programming systems languages and applications, Orlando, Florida, USA, pp. 697-698, 2009
[9] Saraswat, Vijay. "Report on the Programming Language X10", x10- lang.org, http://dist.codehaus.org/ x10/documentation/languagespec/ x10-latest.pdf, (accessed on: 17 June 2017), 2017
[10] Raj, H., Nathuji, R., Singh, A. and England, P. "Resource management for isolation enhanced cloud services", In proceedings of the 2009 ACM workshop on Cloud computing security, Chicago, Illinois, USA, pp. 77-84, 2009.
[11] Hayes, B. "Cloud computing", Commun, ACM, pp. 9-11, 2008
[12] Nurmi, D., Wolski, R., Grzegorczyk, C., Obertelli, G., Soman, S., Youseff, L. and Zagorodnov, D. "The Eucalyptus Open-Source Cloud- Computing System", In Proceedings of the 2009 9th IEEE/ACM International Symposium on Cluster Computing and the Grid, pp. 124-131, 2009
[13] Katja, H. and Ralf, S. "Distributed Database Systems-Fragmentation and Allocation," Cluster of Excellence MMCI, October 2010.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY