ISSN:0975-9646

Juhi Sharma et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 3 (3) , 2012,4514-4515

Cloud Security Challenges

Juhi Sharma [#], Kshitiz Saxena [*]

[#]*Department of Computer Science*
Meerut Institute of Engineering & Technology
Meerut, INDIA
[*]*Department of Computer Science*
Bharat Institute of Technology
Meerut, INDIA

***Abstract*— As more and more industries are moving towards Cloud Computing, with tremendous data being generated every hour, the need of the hour is not just 24X7 availability but also security. In this paper we shall discuss security concerns in Cloud Computing and shall also suggest some measures to improve security.**

***Keywords*— Cloud Computing, Hypervisor, Intrusion Detection.**

I. INTRODUCTION

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction[4]. There are three service models of Cloud computing namely Software as a Service (*SaaS*), Platform as a Service (*PaaS*), and Infrastructure as a service *(IaaS*). As per NIST's recommendations, four deployment models of Cloud Computing have been proposed, namely Private Cloud, Community Cloud, Public Cloud and Community Cloud. Since it is relatively inexpensive and less time consuming to deploy existing applications over the latter three deployment models, serious security issues need to examined. Our research paper is an attempt to investigate these issues and suggest solutions in order to maximize the benefits of Cloud Computing.

II. ADDRESSING CLOUD SECURITY CONCERNS

A. Securing Hypervisor

A hypervisor, also called a *virtual machine manager*, is a program that allows multiple operating systems to share a single hardware host. Each operating system appears to have the host's processor, memory, and other resources all to itself. However, the hypervisor is actually controlling the host processor and resources, allocating what is needed to each operating system in turn and making sure that the guest operating systems (called virtual machines) cannot disrupt each other.

All applications in a Classsic Data Center must be moved into a Virtual Data Center before they can be ported in to a Cloud and a hypervisor is an agent that plays a key role in making applicatons run or allocating resources on-demand in a cloud. An hypervisor can be implemented at the host operating system level or can run on its own (*bare metal hypervisor*). Security breaches have been uncovered in both approaches – an infected hypervisor (virus/worm) or heavily loaded hypervisor will affect the performance and stability of the entire system. There could be even a possibility of having a *rogue hypervisor* being installed by mallicious users thereby resulting in total denial of service to users.

Several approaches have been suggested to mitigate these threats including providing multiple layers of security (Defense in Depth) and regularly patching the hypervisor with latest updates.

B. Side-channel Attacks

These techniques allow an attacker to monitor the analog characteristics of power supply and interface connections, thus they can be used to access the chip surface directly, so we can observe, manipulate, and interfere with the device.

Use of solid state devices to improve memory access time and using them to integrate with the caches available in storage arrays/ servers (~ GB) improves I/O but Semi-Invasive and Non-Invasive attacks have been reported [3] and it has been proved that side-channel attacks pose serious threat to hardware security as such attacks involve low-cost setup, have small attack time and are easy to reproduce.

C. Data encryption for the Cloud

Confidentiality, *Integrity* and *Availability* are concerns that need to be addressed before applications are ported into Cloud. Deploying data encryption can address these concerns but the choice of techniques can baffle any customer. Data can be encrypted while *it is at rest* (in the Storage Array) or while *it is in transit* (at the Network Level).

Organizations such as *CipherCloud* offering Cloud enabled services have implemented strong software-based cryptographic key management based on the NIST SP 800-21 standard that included key rotattion, split custodians, key encrypting keys and many other capabilities. In addition, customers have the option to integrate with FIPS 140-2 compliant networ attached Hardware Security Modules (HSM). Since the encrypttion keys are stored locally and managed by customers themselves, the risk of an external party gaining unauthorized access to data is completely eliminated.

Additionally we propose the use of an *open-source infrastructure* to protect sensitive data which may have two components namely a key manager, which resides in the

Cloud and an agent which is a patch in the existing client's kernel operating system. This solution could be deployed as a *PaaS* solution. SMB's or starter companies which cannot place the key manager in the cloud due to security/regulatory reasons can install this software component just behind the company's firewall. The second component will actually do the encryption (using AES-256 or similar strong encryption technique). Such an implementation could eventually create a *Virtual Encrypted File System* which offers high security without compromising on performance.

D. Deploying Intrusion Detection Systems

Attacks on systems and data are a reality in the world we live in. Detecting and responding to those attacks has become the norm and is considered due diligence when it comes to security. As a matter of fact, most of the standards and regulations applied in the technology space today have explicit instructions regarding the need for monitoring and alerting, or intrusion detection. Deploying Intrusion Detection Systems offers a lot of choices namely deployment at guest OS level, as a separate Virtual Machine, at hypervisor level, at virtual network level or at physical network level.

The ability to perform intrusion detection in the cloud is heavily dependent on the model of Cloud Computing being used. With SaaS, the Cloud Service Provider's (CSP) will excclusively perform intrusion detection leaving the customers with the option of getting some logs or alternatively some customized monitoring or alerting (based on those logs) could be made available. With PaaS, since intrusion detection systems are typically outside the applications, the customer relies on the CSP's to deploy it. However a customer has more flexibility in terms of configurability of applications to monitor and alert in case of security breaches. IaaS gives more options to the customer and is most flexible model for intrusion detection deployment.

In reality, intrusion detection in the Cloud is best performed by the provider as the CSP's have a complete understanding and availability of sufficient expertise to mitigate security threats. In our opinion, intrusion detection based on Virtual Machine appers to be the most promising technology for Cloud security. We strongly believe that future of the Cloud IDS would imply a definitive service license agreement (SLA) with the CSP's ability to provide high availability and security of information.

III. CONCLUSION AND FUTURE WORK

It has now been established that the business is taking a leading role in adopting cloud. This is because ever more the businesses realise that cloud computing is helping to achieve business goals. Public Software as a Service (*SaaS*) is the dominant cloud type in use and that Platform as a Service (*PaaS*) and Infrastructure as a Service (*IaaS*) are catching up. The understanding of the market with respect to cloud computing is lacking and confusion exists on the service descriptions. What is nevertheless clear, is that cloud computing is here to stay.

Through this paper we have studied various aspects related to Cloud Security. We have identified potential weak-links in the Cloud implementations of various CSP's and have suggested measures to mitigate the security threats.

We have also envisioned a road map for future work related to Cloud Computing which involves identifying the main challenges when migrating services to the cloud. We further aim to identify the security issues and the problems which can derive from loss of control. We shall also attempt at a possible implementation of a reliable monitoring tool which shows the mapping of the client's services to the underlying virtualized and physical layers wherein the status and performance of these services could be monitored near real-time.

REFERENCES

[1] EMC^2 Academic Alliance Faculty Community Portal, https://community.emc.com/ ", retrieved 12-May-2012.

[2] Syed A. Ahson,; Mohammad Ilyas, Florida Atlantic University, Boca Raton, USA, "Cloud Computing and Software Services: Theory and Techniques" , CRC Press, 2010.

[3] S. Skorobogatov, "Side-channel attacks: new directions and horizons", ECRYPT2 School on Design and Security of Cryptographic Algorithms and Devices, 29 May-03 June 2011, Albena near Varna, Bulgaria.

[4] "The NIST Definition of Cloud Computing". National Institute of Science and Technology. Retrieved 24 July 2011.

[5] D Kyriazis, A Menychtas, G Kousiouris, K Oberle, T Voith, M Boniface, E Oliveros, T Cucinotta, S Berger, "A Real-time Service Oriented Infrastructure", International Conference on Real-Time and Embedded Systems (RTES 2010), Singapore, November 2010

[6] "Gartner Says Worldwide IT Spending On Pace to Surpass Trillion in 2008", Gartner, 2008-08-18. Retrieved 2009-09-11

[7] "Sun CTO: Cloud computing is like the mainframe". Itknowledgeexchange.techtarget.com. 2009-03-11. Retrieved 2010-08-22.

[8] Armbrust, M; Fox, A., Griffith, R., Joseph, A., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Zaharia, (2010). "A view of cloud computing.". *Communication of the ACM* **53** (4): 50–58.

[9] Anthens, G. "Security in the cloud". *Communications of the ACM* **53** (11)

[10] Ko, Ryan K. L. Ko; Kirchberg, Markus; Lee, Bu Sung (2011)."From System-Centric Logging to Data-Centric Logging - Accountability, Trust and Security in Cloud Computing".*Proceedings of the 1st Defence, Science and Research Conference 2011 - Symposium on Cyber Terrorism, IEEE Computer Society, 3–4 August 2011, Singapore*.