International Journal of Research and Development in Applied Science and Engineering (IJRDASE)
ISSN: 2454-6844

Analysis of Security Issues in Cloud Computing and Associated Techniques

Pankaj Gugnani
Computer Science
S.R.C.E.M., Banmore, (M.P.)
pankaj88gugnani@gmail.com

Aparajit Shrivastava
Dept of Computer Science
S.R.C.E.M., Banmore, (M.P.)
aparajit2k5@gmail.com

***Abstract*-- Cloud computing offers massive scalability, immediate availability, and low cost services as major benefits, but as with most new technologies, it introduces new risks and vulnerabilities too. Despite the fact that different cloud structures and services are expanding, the cloud computing penetration has not been as envisioned. Some specific concerns have stopped enterprises from completely joining the cloud. One of the major disadvantages of using cloud computing is its increased security risks. In this paper we conduct an in depth analyses of the different aspects of security issues in cloud computing and study few possible solution to alleviate those security risks.**

Keywords--Cloud Computing, Cloud Security, SQL Injection, Encryption

1. Introduction

Putting business-critical data in the hands of an external provider still petrifies of most managers. Only by relinquishing some control over the data will companies then capture the cost economies that are available after joining the cloud computing technology. The truth of the matter is that holding the data in the cloud is not really any less secure than leaving it on internal servers connected to the Internet. Companies need to be realistic about the level of security they may achieve inside of their own business, and how that might compare to a cloud provider. There is still much work to be done before more formalized standards are place. Organizations such as the Cloud Security Alliance are at the forefront of addressing these issues.

Security is usually defined as saving data and program from danger and vulnerability.

2 Security Requirements

Applying security protocols includes both the “software side” security and the “hardware side” security. A good cloud computing provider must have secure enough policies in place to keep the data safe from the dangers and vulnerabilities stated in the previous section. Some of the important security requirements are:

Confidentiality: Ensuring that information is not disclosed to any unauthorized parties.

Integrity: Ensuring that information held in a system, is a proper representation of the information intended and that it has not been modified by an unauthorized person.

Availability: Ensuring that information processing resources are not made unavailable by malicious action.

Non-repudiation: Ensuring that agreements made electronically may be proven to have really transpired.

Physical security: On the “hardware side” of security there are several well defined protocols in the industry, such as the professional security staff utilizing video surveillance, state of the art intrusion detection systems, and other electronic means for guarding a datacenter. Furthermore, when an employee no longer has a legitimate business purpose for accessing the datacenter, that employee’s privileges for accessing the datacenter should be immediately revoked, Physical security protocols should be applied to all datacenters and backup centers and wherever user data is stored or used.

Data sanitization: Sanitization is the process of removing sensitive information from a storage device. What data sanitization practices does the cloud computing service provider propose for implementing redundant and obsolete data storage devices when and if these devices are retired or discontinued.

The “software side” of security has guided us to a deeper and newer era. For more than a century, physical security has existed and has been developed day after day and has continuously evolved, but on the “software security side,” science is still young and evolving. This makes it a challenge for cloud computing developers.

3 Dynamic Information Security

Information security, as static information residing on hard disks at datacenters or backup centers should be fulfilled by physical security protocols, but what about data that is being transferred from one host to another? Security related to the information exchanged between different hosts or between hosts and users is provided by transfer protocols and middleware. These are security issues pertaining to secure communication, authentication, and issues concerning single sign on and delegation. Secure communication issues include

security concerns that arise during the communication between two entities, and these include confidentiality and integrity issues. Confidentiality indicates that all data sent by users should be accessible only to "legitimate" receivers, and integrity indicates that all data received should only be modified by "legitimate" senders.

4 Virtualization Security

The virtualization layer (or hypervisor), is effectively another operating system in the data center. Hypervisors tend to carry a much smaller footprint than a traditional operating system with a correspondingly lower potential for security holes. Plus, no hypervisor will be found surfing the Internet and downloading code or used as a station by any means. Yet, at the same time, it is still a relatively immature product, and vulnerabilities are still repeatedly discovered. These vulnerabilities are usually quickly rectified, but should be monitored and tracked [4]. The maturity of hypervisor technology also shows in its vetting and certificating infrastructure. It is theoretically possible for hackers to attack the hypervisor layer specifically, or to take over a VM and use it to attack other VMs.

Another aspect of a virtualization security risk is the communication between virtual machines. Virtual machines have to communicate and share data with each other, and as noted by Ruykhaver [5], if these communications aren't monitored or controlled they are ripe for attack**.** As virtualization becomes more and more popular in market, it also will become more and more popular as a target for malicious attacks. As virtualization administrators, there is a necessity to ensure that these virtualized systems are as secure as or even more secure than our physical systems. Plus, there needs to be a demand for more and more security features from the manufactures of the hypervisors and virtualization management interfaces. In summary, virtualization is truly invaluable to us all; it is here to stay. Similar to wireless LANs, virtualization is a young technology and it needs more maturity in the area of security [5].

5 Security Risk Prevention

A Virtual Machine Monitor (VMM) is a host program that allows a single computer to support multiple, identical execution environments. According to [6]**,** a good VMM should support the following properties:

Isolation: Software running in a virtual machine may not access or modify the software running in the VMM or in a separate VM.

Inspection: The VMM has access to all of the state of a virtual machine: The CPU state (e.g. registers), all memory, and all I/O device state such as the contents of storage devices and register the states of I/O controllers, so that VMM may monitor VM.

Interposition: Fundamentally, VMMs need to interpose on certain virtual machine operations (e.g. executing privileged instructions).

6 Encryption Scheme

A critical aspect of a security system is that every security system uses an encryption schema; the more secure this schema is the more accurate and safe a system may be in order to serve its purpose. Encryption accidents may cause data to be corrupted and totally unusable; they may complicate accessibility and availability of data. In some cases, encryption may prevent applications from their normal functionality. The cloud computing company or the service provider is responsible for designing and testing an encryption schema and putting that in a virtual machine in order to make data safe.

7 Related Work

Suleyman Kardas *et al.[7]* authors studied RFID is a leading technology that has been rapidly deployed in several daily life applications such as payment, access control, ticketing, and e-passport, which requires strong security and privacy mechanisms. However, RFID systems commonly have limited computational capacity, poor resources and inefficient data management. Hence there is a demanding urge to address these issues in the light of some mechanism which can make the technology excel. Cloud computing is one of the fastest growing segments of IT industry which can provide a cost effective technology and information solution to handling and using data collected with RFID. As more and more information on individuals and companies is placed in the cloud, concerns are beginning to grow about just how safe an environment it is. Therefore, while integrating RFID into the cloud, the security and privacy of the tag owner must be considered. Motivated by this need, the researchers first provide a security and privacy model for RFID technology in the cloud computing. In this model, we first define the capabilities of the adversary and then give the definitions of the security and privacy. After that they propose an example of an RFID authentication protocol in the cloud computing. They proved that the proposal is narrow strong private_+ in our privacy model In their work, they provided a new security and privacy framework for RFID technology that is integrated into cloud service to leverage the availability and scalability of the system. In their framework, they defined the capabilities of the adversary and then give the definitions of the security and privacy..

Kun Ma *et al* [8] Nowadays, the cloud computing owners lack management and monitoring tools to ensure the performance, robustness, dependability, and security. To address this limitation, researchers described their experience with a lightweight monitoring framework using some extra development work. Their framework performed end-to-end measurements at virtual machine instances and software in the public cloud. It monitors quality of service parameters of the IaaS and SaaS layer without modifying the implementation of the monitored object. In addition, they discussed the manager-agent and modulecentralized architecture in details. All the modules make up the entire proposed framework to improve the performance of applications in public clouds. In their research, they first listed the monitoring methods and tools. Then they focused on the popular metrics of the guest in the

public clouds. Towards their goal of building such a lightweight and scalable framework, they integrate some open-source monitoring tools, and do some extra significant secondary developments work to archive some modules. In addition, they discuss the manager-agent and module-centralized architecture to perform end-to-end measurements at virtual machine instances and software in the public cloud.

Tim Waizenegger, *et al.* [9] The researchers focused on the adaptability aspect of Cloud. As the adoption of Cloud Computing is growing, the automated deployment of cloud-based systems is becoming more and more important. New standards, such as TOSCA (OASIS), allow the modeling of interoperable Cloud services. It is now possible to build reusable and portable cloud services that can be (semi-) automatically deployed by different cloud-deployment-engines at various Cloud environments. However, there is still an acceptance problem among potential users, especially in the enterprise segment, that stems from security issues like data security. To improve security in automatic Cloud management engines, this they proposes a framework for processing non-functional requirements of Cloud services. The contribution of their research is to introduce and establish aspects of policies in the context of Cloud service definition and to present a first architecture realizing these aspects in a Policy-Framework. They proposed framework supports non-functional aspects in Cloud service models that are built using TOSCA. Security is a major concern in using Cloud Computing for outsourcing data and services especially in the enterprise segment. It is, therefore, important to agree upon a common standard for describing, implementing, and realizing security policies in Cloud service models.

8. Conclusion

Because of the cloud computing structure, investigating and searching for malicious activities or virus attacks is a complicated and difficult action, logging and data for multiple customers may be co-located and also may be geographically spread across an ever-changing set of hosts and data centers. A known solution to this issue is to secure a contractual commitment in order to support specific forms of investigation, along with evidence that the vendor has already successfully supported such activities [6], but even with having this legal advantage, technical difficulties still remain and hinder an effective, cost efficient investigation process. Therefore, it is extremely difficult for the customer to actually verify the currently implemented security practices and initiatives of a cloud computing service provider because the customer generally has no access to the provider's facility which can be comprised of multiple facilities spread around the globe.

References:

[1] Kynetix Technology group, (2009), "Cloud Computing Strategy Guide", [Accessed 12-02-2010]: https://sites.google.com/site/cloudmanual/success-factors.

[2] McKendrick J., (2011), "Loud Divide: Senior Executives Want Cloud, Security and IT Managers are Nervous", [Accessed 04-20-2011]: http://www.zdnet.com/blog/serviceoriented/cloud-divide-senior-executives-want-cloud-security-and-it-managers-are-nervous/6484

[3] IDC data survey source, (2008), IDC Enterprise Panel, survey number=244

[4] Lynch D., (2008), "New Security Issues Raised by Server Virtualization", [Accessed 03-01- 2011]:http://www.itworld.com/virtualization/59445/new-security-issues-raised-servervirtualization

[5] Petri D., (2009), "What You Need to Know about Securing Your Virtual Network", [Accessed 09-14-2010]: http://www.itworld.com/virtualization/59445/new-security-issuesraised-server-virtualization

[6] Suuburah J. , (2010), "Security Issues in Cloud Computing", [Accessed 02-07-2011]: http://www.computerweekly.com/Articles/2010/01/12/235782/Top-five-cloud-omputingsecurity-issues.htm

[7] Suleyman Kardas,_, Serkan C¸ Muhammed Ali Bing, (2012) "A New Security and Privacy Framework for RFID In Cloud Computing" , Faculty of Engineering and Natural Sciences, ˙Istanbul, Turkey

[8] Kun Ma□, Runyuan Sun, Ajith Abraham, (2012) "Toward a lightweight framework for monitoring public clouds" IEEE

[9] Tim Waizenegger, Matthias Wieland, Tobias Binz, Uwe Breitenbücher, Frank Leymann , (2013), "Towards a Policy-Framework for the Deployment and Management of Cloud Services" SECURWARE : The Seventh International Conference on Emerging Security Information, Systems and Technologies.

[10] S. Sahay et. al., " On the use of ANFIS for Ground Water Level Forecasting in an Alluvium Area" International Journal of Research and Development in Applied Science and Engineering, Volume 2, Issue 1, November 2014.