ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 2, pp: (123-126), Month: April-June 2014, Available at: www.researchpublish.com

SECURITY ISSUE IN CLOUD COMPUTING

Ms. Priyanka, Mr. Kapil Kumar Kaswan

Department of Computer Science and Application
Chaudhary Devi Lal University
Sirsa, Haryana, India

Abstract: **Cloud computing is known as one of the big next things in information technology world. Cloud computing has been envisioned as the next generation architecture of IT Enterprises. It offers great potential to improve productivity and reduce costs. In contrast to traditional solutions, where the IT services are under proper physical, logical and personnel controls, cloud computing moves the application software and databases to large data centers, where the management of the data and services may not be fully trustworthy. Cloud computing has gained great attention from industry but there are still many issues that are in their primitive stage which is hampering the growth of Cloud. Security is as much of an issue in the cloud as it is anywhere else. This paper investigates few major security issues with cloud Computing. In this paper we investigate some prime security attacks on clouds: Wrapping attacks, Malware Injection attacks and Flooding attacks, and the accountability needed due to these attacks.**

Keywords: **Cloud computing security, Wrapping attack, Flooding attack**

I. INTRODUCTION

Today‟s Cloud computing is a most important and reasonable technology. Cloud Computing is a way of computing in which dynamically scalable and often virtualized resources are provide as a services over the internet. Internet is not only a communication medium but, because of the reliable, affordable and ubiquitous broadband access, is becoming a powerful computing platform rather than running software and managing data on the desktop computer or server, user are able to execute application and access data on demand from the cloud (internet) anywhere in the world. This new computing paradigm is referred as a cloud computing.

Cloud computing has been introduced as providing a large framework that is beneficial for clients which utilize all or some aspects of it. Cloud computing can be thought of as composed of different layers, depending on the distribution of the resources. In this view, the CPU, memory and other hardware components reside at the bottom-most layer, called the Infrastructure as a Service (IaaS) layer. The layer which is responsible for hosting different environments for customer specific services is the middle layer, known as the Platform as the Service (PaaS) layer. Finally, the topmost layer is the Software as a Service (SaaS) layer, where cloud service accessing takes place through the Web service and web browsers. Amazon EC2 is a well known example of IaaS, Google App engine is an example of PaaS and salesforce.com is an example of SaaS.

II. SECURITY ISSUES AND CHALLANGES

A. ***Security:*** While leading Cloud services providers employ data storage and transmission encryption, user authentication, and authorization (data access) practices, many people worry about the vulnerability of data to criminals like hackers, thieves, and disgruntled employees. Cloud providers are enormously sensitive to this issue and apply substantial resources to mitigating concern. Mostly, the uniqueness of the Cloud computing security is not recognized.

Some researchers think that Cloud computing security is not much different from existing security practices and the security aspects can be well managed with the existing techniques such as digital signature, encryption, firewalls, and/or the isolation of virtual environments, etc .

B. Privacy: Privacy is an important issue for cloud computing, both in terms of legal compliance and user trust and this need to be considered at every phase of design. The key challenge for software engineers to design cloud services in such a way as to decrease privacy risk and to ensure legal compliance. There are various forms of privacy like "control of information about us". In Cloud Computing, data is processed and stored remotely so privacy is always an issue in the minds of customers. Since, Cloud services process users' data on machines that users do not own or operate, this introduces privacy issues .

C. Reliability: Some people also worry about whether a Cloud service provider is financially stable and whether their data storage system is trustworthy. Most Cloud providers attempt to mollify this concern by using redundant storage techniques, but it is still possible that a service can crash or go out of business, leaving users with limited or no access to their data. A diversification of providers can help alleviate this concern, albeit at a higher cost.

D. Data portability and conversion: Some people are concerned that if they wish to switch providers, they may have difficulty transferring data. Porting and converting data is highly dependent on the nature of the Cloud provider's data retrieval format, particular in cases where the format cannot be easily discovered. As service competition grows and open standards become established, the data portability issue will ease, and the conversion processes will become available supporting the more popular Cloud providers. Worst case will be when a Cloud subscriber will have to pay for some custom data conversion.

Challenges in security in cloud computing:

There are several challenges in cloud.

1. **Cloud Migration/ Security:** Foremost thing that should be tackled efficiently is the process of migrating confidential data from the internal server to one big cloud server. An exceptionally experienced and profound work force should be present to deal with and handle such issues smoothly and with ease.
2. **How Reliable Cloud Environment is?** Whenever a new technology is innovated or developed, next thing after security that comes to mind is whether it is reliable. Similar notions have been felt for cloud architecture as well. The recent outages ranging from Amazon EC2.
3. **Can Cloud be Available?** As per industry reports cloud managers assure or 100 % availability and round the clock assistance. But, is it rightly said? Providing users with 99.99% uptime and highly scalable environment is possible.
4. **Monitoring Measures can be Vague:** Once your data is migrated on the cloud, it becomes prime concern for the managed cloud providers to monitor your cloud 24 x 7. This is only possible if your cloud provider has enough and strong infrastructure to do so, else your money invested in it can be simply in vain.
5. **Lack of Communication:** Communication plays a vital role in promoting anything that can bring a change. Technically, speaking, it does have importance in grooming cloud technology as well.

Now we describe the security challenges in cloud computing.

a) **Authentication and identity management**: In cloud services user can easily access their personal information and make it available across the internet. Identity management can help authenticate the user.

b) **Access control and accounting**: The access control services should be flexible enough to capture dynamic, context, or attribute and to enforce the principle of least privilege.

c) Trust management and policy integration: A trust framework should be developed to allow for efficiently capturing a generic set of parameter required for establishing trust and to manage evolving trust and interaction requirement.

d) **Privacy and data protection:** It is the core issue in all challenges in this the need to protect identity information policy component during integration and transaction histories.

III. ATTACKS IN A CLOUD

We identify different kinds of attacks in a cloud: a) Wrapping attack, b) Malware-Injection attack, c) Flooding attack, and in the face of these attacks the need for Accountability checking.

1. Wrapping attack: Due to the fact that clients are typically able to connect to cloud computing via a web browser or web service, web service attacks also affect cloud computing. XML signature element wrapping is the well-known attack for web service. Although Cloud security uses XML signature in order to protect an element's name, attributes and value from unauthorized parties, it is unable to protect the particulars in the document. An attacker is able to manipulate a SOAP message by copying the target element and inserting whatever value the attacker would like and moving the original element to somewhere else on the SOAP message. This technique can trick the web service to process the malicious message created by the attack.

2. Malware-injection attack: In the cloud system, as the client's request is executed based on authentication and authorization, there is a huge possibility of meta data exchange between the web server and web browser. An attacker can take advantage during this exchange of metadata. Either the adversary makes his own instance or the adversary may try to intrude with malicious code. In this case, either the injected malicious service or code appears as one of the valid instance services running in the cloud. If the attacker is successful, then the cloud service will suffer from eavesdropping and deadlocks, which forces a legitimate user to wait until the completion of a job which was not generated by the user. This type of attack is also known as a meta-data spoofing attack.

3. Flooding attack problem: In a cloud system, all the computational servers work in a service specific manner, with internal communication between them. Whenever a server is overloaded or has reached the threshold limit, it transfers some of its jobs to a nearest and similar service-specific server to offload itself. This sharing approach makes the cloud more efficient and faster executing requests. When an adversary has achieved the authorization to make a request to the cloud, then he/she can easily create bogus data and pose these requests to the cloud server. When processing these requests, the server first checks the authenticity of the requested jobs. Non legitimate requests must be checked to determine their authenticity, but checking consumes CPU utilization, memory and engages the IaaS to a great extent, and as a result the server will offload its services to another server an analysis of the IDT contents and the hash values of inmemory code blocks can determine the running OS in the VM. Finally, using the information of the running OS with the appropriate algorithms, all the running instances can be identified and then validated by the Hypervisor. It is observed that the OS of the VM2 can be easily detected.

4. Denial of Service (DoS) attacks: A DoS attack is an attempt to make the services assigned to the authorized users unavailable. In such an attack, the server providing the service is flooded by a large number of requests and hence the service becomes unavailable to the authorized user. Sometimes, when we try to access a site we see that due to overloading of the server with the requests to access the site, we are unable to access the site and observe an error

5. Accountability check problem: The payment method in a cloud System is "No use No bill". When a customer launches an instance, the duration of the instance, the amount of data transfer in the network and the number of CPU cycles per user are all recorded. Based on this recorded information, the customer is charged. So, when an attacker has engaged the cloud with a malicious service or runs malicious code, which consumes a lot of computational power and storage from the cloud server, then the legitimate account holder is charged for this kind of computation. As a result, a dispute arises and the provider's business reputation is hampered

IV. POSSIBLE SECURITY APPROACHES

In this section we discuss possible solutions for the three mostly probable attacks: wrapping attacks, malware-injection attacks and flooding attacks, as well as an accountability check for the Cloud system.

1. Wrapping attack solution: In this regard some additional precautions should be considered for the reliability of the SOAP message. Two approaches can be adapted by the registered users in this message passing:

a. A Self signed Certificate and RSA key can be generated for convenience.
b. Registering a public certificate with the provider.

These certificates will be authenticated by a trusted CA.

We propose that the Security Header must be signed while passing this message through an unsecured transport layer. When it is received in the destination, the validation is checked first. If the Timestamp is not reasonable, then it can be assumed that security has been breached, actions can be taken accordingly and the SOAP message can be ignored.

2. Malware-injection attack solution: The client's VM is created and stored in the image repository system of the cloud. These applications are always considered with high integrity. We propose to consider the integrity in the hardware level, because it will be very difficult for an attacker to intrude in the IaaS level. Our proposal is to utilize a FAT-like (File Allocation Table) system architecture due to its straightforward technique which is supported by virtually all existing operating systems. From this FAT-like table we can find the application that a customer is running. A Hypervisor can be deployed in the provider's end. The Hypervisor is responsible for scheduling all the instances, but before scheduling it will check the integrity of the instance from the FAT-like table of the customers VM.

3. Flooding attack solution: For preventing a flooding attack, our proposed approach is to consider all the servers in the cloud system as a fleet of servers. Each fleet of servers will be designated for a specific type of job, like one fleet engaged for file system type requests, another for memory management and another for core computation related jobs, etc. In this approach, all the servers in the fleet will have internal communication among themselves through message passing. So when a server is overloaded, a new server will be deployed in the fleet and the name server, which has the complete records of the current states of the servers, will update the destination for the requests with the newly included server.

4. Accountability check solution: The provider does not know the details of the customer's applications and it does not have the privilege to test the integrity of the application running in the cloud. On the other hand, customers do not know the infrastructure of the provider's cloud. If a customer is charged due to a malware attack or a failure, then the customer has no option to defend himself.

In some cases, there can be a conflict between privacy and accountability, since the latter produces a detailed record of the machines' actions that can be inspected by a third party. An accountable cloud can maintain separate logs for each of its customers and make it visible to only the customer who owns it. Also, the log available to customers will not have any confidential information about the infrastructure of the provider from which the IaaS can be inferred by the AUDITOR.

V. CONCLUSION

Cloud computing is revolutionizing how information technology resources and services are used and managed, but this revolution comes with new problems. We have depicted some crucial and well known security attacks and have proposed some potential solutions in this paper. The concepts we have discussed here will help to build a strong architecture for security in the field of cloud computation

REFERENCES

[1] Meiko Jenson, Jorg Schwenk, Nils Gruschka, Luigi Lo Iacono. On Technical Security Issues in Cloud Computing. IEEE International Conference on Cloud Computing 2009.

[2] D. Kormann and A. Rubin, "Risks of the pass [7] Mark C. Chu-Carroll, "Cloud computing," http://scienceblogs.com/goodmath/2009/05/Cloud_computing.php, May 2009.

[3] B.D. Payne, M. Carbone, M. Sharif, and W. Lee. Lares: An architecture for secure active monitoring using virtualization. Security and Privacy, IEEE Symposium on, 0:233-247, 2008.

[4] Amazon Elastic Compute Cloud (Amazon EC2). http://aws.amazon.com/ec2.

[5] M. Christodorescu, R. Sailer, D. L. Schales, D. Sgandurra, D. Zamboni. Cloud Security is not (just) Virtualization Security, CCSW'09, Nov. 13, 2009, Chicago, Illinois, USA.

[6] Saurabh, "Security issues in cloud Computing", http://serl. iiit. ac. in/cs6600/saurabh. ppt, 2009.