Security Problems and Possible Security Approaches In Cloud Computing

R. Balasubramanian, Dr.M.Aramuthan,

Abstract - In this paper we are going to discuss about the security issues of cloud computing which includes storage security, data security and network security. The major security challenge with clouds is that the owner of the data may not have control of where the data is placed. This is because if one wants to exploit the benefits of using cloud computing, one must also utilize the resource allocation and scheduling provided by clouds. Therefore there is need to safeguard the data in the midst of un-trusted processes. The emerging cloud computing model attempts to address the explosive growth of web-connected devices, and handle massive amounts of data.

Key words: Security, Malware-injection, Flooding, Hypervisor, Accountability, Virtual Machine, Interrupt Descriptor Table.

1. INTRODUCTION

The need to augment human reasoning, interpreting, and decision making abilities have resulted in the emergence of the Web, which is an initiative that attempts to transform the web from its current, merely human-readable form, to a machine executable form. This in turn has resulted in numerous social networking sites with massive amounts of data to be shared and managed. Therefore there is urgently need a system that can scale to handle a large number of sites and process massive amounts of data. Due to the extensive complexity of the cloud, it will be difficult to provide a holistic solution to securing the cloud at present. Therefore there is needed to make increment enhancements to securing the cloud that ultimately results in a secure cloud. So cloud system:

- ✓ support efficient storage
- ✓ store, manages and query massive amounts of data
- ✓ support fine grained access control and
- ✓ support strong authentication.

• Research Scholar, Manonmanium Sundaranar University,Tirunelveli, Tamilnadu,India.
Email: bala.rec@gmail.com

• Perunthalaivar Kamarajar Institute of Engineering& Technology,Karaikal, Pondicherry,India.
Email: aranagai@yahoo.co.in

2. SECURITY

There are numerous security issues for cloud computing as it encompasses many technologies including networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing and memory management. Therefore, security issues for many of these systems and technologies are applicable to cloud computing. For example, the network that interconnects the systems in a cloud has to be secure. For example, mapping the virtual machines to the physician machines has to be carried out securely. Data security involves encrypting the data as well as ensuring that appropriate policies are enforced for data sharing. In addition, resource allocation and memory management algorithms have to be secure.

Security threats on cloud users are both external and internal. Many of the external threats are similar to the threats that large data centers have already faced. This security concern responsibility is divided among the cloud users, the cloud vendors and the third party vendor involved in ensuring secure sensitive software or configurations. If the application level security is the responsibility of the cloud user, then the provider is responsible for the physical security and also for enforcing external firewall policies. Security for intermediate layers of the software stack is shared between the user and the operator. The lower the level of abstraction exposed to the user, the more responsibility goes with it. Besides the external security issues, the cloud does possess some internal security issues as well. Cloud providers must guard theft or denial-of-service attacks by users. In other words, users need to be protected from each other. Virtualization is the primary mechanism that today's clouds have adapted because of its powerful defense and protection against most of the attempts by users to attack each other or the underlying cloud infrastructure. However, not all the resources are virtualized and not all virtualization environments are bug free. Virtualization software contains bugs that allow virtualized code to "break loose" to some extent. Incorrect network virtualization may allow user code access to sensitive portions of the provider's infrastructure or to the resources of others.

The cloud should also be protected from the provider. By definition, the provider controls the bottom layer of the software stack, which effectively circumvents most known security techniques. The one important exception is the risk of inadvertent data loss.

In addition, if any kind of failure occurs, it is not clear who is the responsible party. A failure can occur for various reasons:

1) due to hardware, which is in the Infrastructure as a Service layer of the cloud
2) due to malware in software, which is in the Software as a Service layer of the cloud or
3) due to the customer's application running some kind of malicious code,

the malfunctioning of the customer's applications or a third party invading a client's application by injecting bogus data. Whatever the reason, a failure can result in a dispute between the provider and the clients.

3. SECURITY PROBLEMS

3.1 Malware-injection attack problem

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.

3.2 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. Again, the same thing will occur and the adversary is successful in engaging the whole cloud system just by interrupting the usual processing of one server, in essence flooding the system.

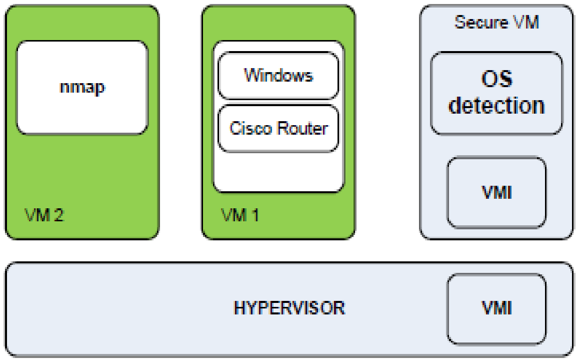
3.3 Accountability check problem

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.

4. POSSIBLE SECURITY APPROACHES

4.1 Malware-injection attack solution

The client's Virtual Machine (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 customer's VM.

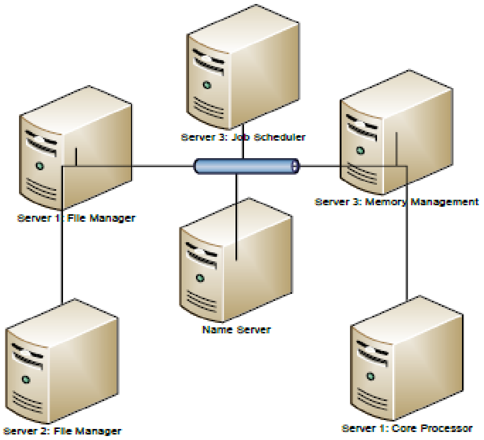


Now the question is how the FAT-like table will be utilized to do the integrity checking. The IDT (Interrupt Descriptor Table) can be used in the primary stage to detect. Firstly, the IDT location can be found from the CPU registers; then an analysis of the IDT contents and the hash values of in-memory 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.

4.2 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.

As mentioned in the previous section, a Hypervisor can also be utilized for the scheduling among these fleets. The Hypervisor will do the validity checking and if any unauthorized code is interrupting the usual computation in the cloud system, then the system will detect the instance by introspection.



In this way, the flooding attack can be mitigated to an extent. If the Hypervisor is locally breached, which would require a misfeasor, then further analysis and efforts will be required to secure the Hypervisor. Additionally, a PID can be appended in the messaging, which will justify the identity of the legitimate customer's request. The PID can be checked by the Hypervisor in the assignment of instances to the fleet of servers. This PID can be encrypted with the help of various approaches, such as implementing hash values or by using the RSA.

4.3 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. There can be unusual phenomenon, such as a dramatic increase in a current account usage balance all of a sudden or charges for instances at a specific time when the customer was away from the cloud. In this case, an investigation should take place before charging the customer, because an adversary may be responsible for these unusual activities. In our approach the following features will be ensured in the provider's end before launching any instance of a customer:

- Identities
- Secure Records
- Auditing
- Evidence

Firstly, before starting the instance, the identity of the legitimate customer should be checked by the Hypervisor. Secondly, all the message passing and data transfer in the network will be stored securely and uninterrupted in that specific node. Hence, when the auditing takes place, all the necessary information can be retrieved. Also, the evidence must be strong enough to clarify the recorded events, so the AUDIT will have the following properties: completeness, accuracy and verifiability. These properties ensure that when there is a security attack it is reported immediately, no false alarm will be reported and the evidence can be scrutinized by a trusted third party who will commit the task of AUDIT from a neutral point of view.

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.

5. CONCLUSION

There are several security challenges including security aspects. There believes that due to the complexity of the cloud, it will be difficult to achieve end-to-end security. So security issues for cloud are important. These issues include storage security, data security, network security and application security. The main goal is to securely store and manage data that is not controlled by the owner of the data. Then there is focused on specific aspects of cloud computing. In particular, taking a bottom up approach to security where working on small problems in the cloud, that there is one hope to solve the larger problem of cloud security.

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, such as utilizing the FAT-like table and a Hypervisor.

In the future, we will extend our research by providing implementations and producing results to justify our concepts of security for cloud computing. The concepts we have discussed here will help to build a strong architecture for security in the field of cloud computation. This kind of structured security will also be able to improve customer satisfaction to a great extent and will attract more investors in this cloud computation concept for industrial as well as future research farms. Lastly, we propose to build strong theoretical concepts for security in order to build a more generalized architecture to prevent different kinds of attacks.

6. REFERENCES

[1] 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.

[2] L. Litty and D. Lie. Manitou: a layer-below approach to fighting malware. In ASID '06: Proc. of the 1st workshop on Achitectural and system support for improving gsoftware dependability, pages 6-11, New York, NY, USA, 2006. ACM.

[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] VMware. Virtual Appliance Marketplace. http://www.vmware.com/appliances/.

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

[6] M. A. Rahaman, A. Schaad, and M. Rits. Towards secure SOAP message exchange in a SOA. In SWS '06: Proceedings of the 3rd ACM workshop on Secure Web Services, pages 77–84, New York, NY, USA, 2006. ACM Press.

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

[8] D. Kormann and A. Rubin, "Risks of the passport single sign on protocol," Computer Networks, vol. 33, no. 1–6, pp. 51–58, 2000.