Security Aspects in Cloud Computing

Apurva Shitoot[1], Sanjay Sahu[1], Rahul Chawda[1]

[1.] *School of Information Technology, MATS University, Raipur, C.G, INDIA-493447.*

***Abstract*— Cloud computing, sometime known as on-demand computing is one of the newest developments in the computer technology. Security in Cloud computing is a significant and critical aspect, associated with many issues and problems to use or deployment of it. The objective of this research contribution is to focus on various security issues occurs from the usage of Cloud services. As well as to discover probable problems, based on existing researches; finally observe and present appropriate key solution for each problem.**

***Keywords*— Cloud Computing, cloud security, public cloud**

I. INTRODUCTION

Cloud computing is a technology that make use of the internet and central remote servers to retain data and applications. Cloud computing permit consumers and company to use applications without installation and access their private files at any computer with internet access. It provides the full scalability, consistency, high performance and comparatively low cost possible solution as compared to devoted–infrastructures [1]. This technology let for much more capable computing by compact storage, memory, processing and bandwidth. Many researchers are looking forward to use the cloud approach for many different applications. Since it is a new proposed model and new to the technology world, managing security is still a main issue [2].

II. CLOUD COMPUTING SCENARIO

The two most significant influencing elements leading the future uptake of public cloud computing are the accessibility of public cloud infrastructure and the trust put into security and compliance. The public cloud computing infrastructure will need to be available and accessible around the globe. If such an extensive infrastructure is going to be used, enterprises will have to be sure that their data will be safe and compliant.

As per as the research papers [3] [4], cloud computing is defined as:

- The **happy cloud** scenario is the scenario that most cloud providers are banking on. In this scenario there is a extensively accessible public cloud transportation and it turns out that public cloud is truly more safe and obedient than legacy IT implementations. Business clients will gladly get their IT from the cloud and there will be only some responsibilities missing for the IT department.
- The **patchy cloud** scenario is a scenario in which there is a broadly accessible public cloud infrastructure but there are genuine matter around security and compliance. In this scenario, only request that are non important and have no conformity requests will be put into the public cloud. The IT department will make private clouds and will state cloud access.
- The **exclusive cloud** is a scenario where there is a partial accessibility of public cloud transportation and public cloud has establish to be more safe and obedient than legacy IT working. In this scenario, the Internet is no longer content neutral and as a result there will be less public cloud transportation. Those that can give it will be able to get it, but at a value. There will be demand for public cloud because of its higher availability and on-demand feature.
- The **blue skies** scenario is a scenario where there is a partial accessibility of public cloud transportation and there stay real concern around security and observance. In this scenario, the Internet is no longer content neutral and as a result there will be fewer public cloud transportation. In addition, the custom of the transportation that is there is loaded by security and conformity problems. The IT department will make private clouds and there will be small to no cloud access.

III. CLOUD COMPUTING ATTACKS

Nowadays most of the companies use cloud computing services for confidential data sharing, many attackers is also trying to breach the security to access cloud resources. Some of the probable attacks that attackers may attempt to damage data are as follows:

Denial of Service (DoS) attacks

Some security professionals have dispute on that the cloud is more disposed to DoS attacks, since it is shared by various users, which makes DoS attacks much more destructive. When the Cloud Computing operating system observes the high workload on the flooded service, it will start to offer additional computational power (more virtual machines, more service instances) to supervise the additional workload [6]. Hence, the server hardware restrictions for maximum workload to process do no longer hold. In that sense, the Cloud system is annoying to work adjacent to the attacker (by providing additional computational power), but in

fact-some area-even sustain the attacker by permitting him to do most of the probable damage on a service's accessibility, initially from a single flooding attack entry point. Therefore, the attacker do not have to flood every *N* servers that provide a certain service in target, but simply can flood a single, Cloud-based address in order to execute a full loss of accessibility on the proposed service.

Malware-Injection Attack Problem

In a malware-injection attack, a challenger tries to inject malicious service or code, which appears as one of the applicable instance services running in the cloud. If attacker succeeds, then the cloud facility will endure from eavesdropping in. Here the attacker gets his first step by implementing his malicious service in such a mode that it will run in Iaas or SaaS of the cloud servers. This type of attack is also famous as a meta-data spoofing attack [7]. When an instance of a justifiable user is ready to run in the cloud server, then the respective service allows the instance for calculation in the cloud. The only inspection done is to verify if the instance matches a legitimate existing service. The just checking done is to determine if the instance matches a justifiable alive service. However, the reliability of the occurrence is not checked. By penetrating the instance and replacement it as if it is a valid service, the malware movement will be successful in the cloud.

Wrapping Attack Problem

For a wrapping attack, the challenger does its trick during the translation of the SOAP message in the TLS (Transport Layer Service) layer. The body of the message is copied and sent to the server as a genuine user [8]. The server ensures the authentication by the Signature Value and integrity checking for the message is done. As a result, the challenger is able to interrupt in the cloud and can run malicious code to interrupt the common working of the cloud servers.

Flooding Attack Problem

In a cloud system, all the computational servers work in a service definite manner, with inside communication among them. Whenever a server is loaded, it reassigns some of its work to a adjacent and similar service-specific server to offload itself. These sharing approaches create the cloud efficient and faster executing requests.

Data Stealing Problem

The most traditional and common approach to breach a user account is data stealing. The user account and password are stolen [9]. As a result, the consequent stealing of private data or even the destroying of data can obstruct the storage space and security of the cloud. The source faces the first strike of such kind of problem.

IV.PROBABLE SOLUTION FOR ABOVE ATTACKS

DoS Attack Solution

Use advance automatic switches which provides packet rate inspection and bogus IP filtering (Bogon filtering).Intelligent hardware that is Application Front end hardware device is placed on the network which analyzes the data packets entering in network system and identifies that whether they are based on priority ,regular or dangerous . Protecting the Denial of Service attacks mainly include the use of a combination of attack exposure, traffic categorization and reply tools, plan to block traffic that they classify as unauthorized and permit traffic that they classify as authorized[8].

Malware-Injection Attack Solution

Generally when a client opens an account in the cloud, the supplier creates an copy of the client's VM in the image storehouse system of the cloud. The applications that the client will run are measured with high effectiveness and integrity. We propose to judge the integrity in the hardware stage, because it is extremely complicated for an attacker to impose in the IaaS level[9].Utilize of the File Allocation Table (FAT) system architecture, since its uncomplicated method is maintained by virtually all alive operating systems. From the FAT table we can be familiar with about the code or application that a client is going to run. It make sure with the earlier instances that had been already executed from the client's machine to verify the legality and integrity of the latest instance. For this reason, it required to deploy a Hypervisor in the provider's side. This Hypervisor will be measured the mainly secured and complicated part of the cloud system whose protection cannot be breaked by any means. The Hypervisor is responsible for arrangement of all the instances, but before arrangement it will test the integrity of the instance from the FAT table of the client's VM. one more approach is to store the OS type of the client in the initial phase when a client opens an account. As the cloud is entirely OS platform independent, before initiation of an instance in the cloud, inspection can be complete with the OS type from which the occurrence was demanded from with the account holder's OS type.

Wrapping Attack Solution

Since an adversary can impose in the TLS layer; according to this paper boost the security during the message passing from the web server to a web browser by using the SOAP message. particularly, as the signature value is appended, we

can add a disused bit (STAMP bit) with the SOAP header. This bit will be controlled when the message is hampered with by a third party throughout the transfer. When it arrives towards the target, the STAMP bit is make sure first and if it is found controlled, then a new signature value is created in the browser end and the new assessment sent rear to the server as confirmation to alter the authenticity checking. The challenger can no longer disrupt the customer request with a copying of the SOAP body because the earlier signature value is previously changed[9]. For this purpose, only a arbitrary signature value creator is needed in the browser end and only the additional message transparency of one bit is essential for an authenticity test.

Flooding Attack Solution

For avoiding a flooding attack, our projected approach is to categorize all the servers in the cloud system as a cluster of fleet of servers. Each fleet of servers will be elected for particular type of job, In this, all servers in the fleet will have inside communication along with themselves through message passing. So when a server is loaded, a latest server will be installed in the fleet and the name server, which has the entire records of the existing states of the servers, will renew the target for the requests with the latest included server.[10] As point out in the above segment, a Hypervisor can also be consumed for the scheduling between these fleets, determining the legitimacy of the requests and avoiding the fleets from being burdened with fake requests from an adversary. In this way the flooding attack can be moderated to an extent .Also, a PID can be joined in the messaging, which will validate the identification of the valid client's request and be tested by the Hypervisor in the obligation of instances to the fleet of servers. This PID can be transform with the help of variety of approaches, such as applying hash values or by using the RSA.

Data Stealing Solution

At the end of each session, the client will send an e-Mail regarding the usage and duration with a unique digit. In this manner, the client will be aware of the procedure and charges as well as be availed with a unique number to be utilize all the time to access the system. In Amazon EC2, a key is used to validate the authenticity of the client, but this approach only requires the special number attach with the Username. There will be an overhead for transferring an e-Mail to all the clients with an arbitrarily generated amount when their session will terminate. It is mentioned earlier that the PID generator within the Hypervisor can be assigned to commit the task.

V. Conclusions

Cloud computing is the latest technology in computing world. Though cloud-computing brings many advantages to organizations, yet organizations require to understand the security measures provided by the cloud service provider. It also offers enhanced and easier management of data security, since all the data is placed on a central server, so administrators can manage who has and doesn't have access to the files. It is broadly accepted today because of its economic benefits. These research papers have pointed out some critical and well known security attacks and have proposed some possible solutions.

References

[1] P. Arora, R.C. Wadhawann, and E.S. P. Ahuja, "Cloud computing security issues in infrastructure as a service," *International Journal of Advanced Research in Computer Science and Software Engineering*, Vol. 2, no. I, January 2012.

[2] A.Goel and S.Goel "Security Issues in Cloud Computing" *International Journal of Application or Innovation in Engineering & Management (IJAIEM)*, Vol.1, Issue 4, December 2012.

[3] G.Singh and V. K.Sachdeva "Impact and challenges of cloud computing in current scenario" *International Journal of Social Science & Interdisciplinary Research* ,Vol.1 Issue 10, October 2012

[4] D. Probhuling L, Dept. of computer science, Shivaji Plytechnic, Karad, India, "Current Scenario in Architect and applications of Cloud" *International Journal of Advanced Computer and Mathematical Sciences. Vol.4, Issue3, 2013*

[5] A.Singh and Dr. M.Shrivastava **"**Overview of Attacks on Cloud Computing**",** *International Journal of Engineering and Innovative Technology (IJEIT)* Vol. 1, Issue 4, April 2012.

[6] M. Jensen, J. Schwenk, N. Gruschka, and L. Lo Iacono,"On technical security issues in cloud computing," in *Proc.* IEEE International Conference on Cloud Computing, 2009, .

[7] Nils Gruschka1 and Meiko Jensen2 "Attack Surfaces: A Taxonomy for Attacks on Cloud Computing", 3rd International Conference on Cloud Computing, 2010.

[8] T.Siva and E.S.Phalguna Krishna "Controlling various network based A DoS Attacks in cloud computing environment: By Using Port Hopping Technique" *International Journal of Engineering Trends and Technology (IJETT) – Vol.4Issue5- May 2013*

[9] Kazi Zunnurhain and Susan V. Vrbsky Department of Computer Science The University of Alabama"Security Attacks and Solutions in Clouds"Nov2009.

[10] M. Christodorescu, R. Sailer, D. L. Schales, D. Sgandurra, D. Zamboni. "*Cloud Security is not (just) Virtualization Security"*, CCSW '09 Proc.2009 ACM workshop on Cloud computing security, P. 97-102 Nov. 13, 2009, Chicago, Illinois, USA.

[11] Harit Shah, Shrikanth , Sharma Shankar Anandane "Security Issues on Cloud Computing". eprint arXiv:1308.5996, 08/2013.