

Cloud Computing Attacks: A Discussion With Solutions

Shikha Singh^{1*}, Binay Kumar Pandey², Ratnesh Srivastava³, Neha rawat⁴, Poonam rawat⁵, Awantika⁶

^{1,4,5,6}College of Technology, GBPUAT, Pantnagar, Uttarakhand-263145, India

^{2,3}IT Department, GBPUAT, Pantnagar, Uttarakhand-263145, India

*Corresponding author: shikhasingh097@gmail.com

Abstract:

Future will be going to be the world of Cloud Computing because of its vastitude. It provides a lot of services at very low cost. Due to its emergence a number of attacks can be performed over the cloud by the attackers or intruders. In this paper different types of attacks on cloud computing and their respective solutions are discussed. Security of cloud is of great concern hence care must be taken to provide secure cloud and secure cloud services.

Keywords:

Authentication; Denial-of-service, Malware-Injection Side-channel; Man-in-the-middle Attacks

1. INTRODUCTION

CLOUD COMPUTING has become the emerging mechanism of most Internet usage. Most of the services like email, social networks, search engines and many others are now hosted in the cloud. Cloud computing has been defined by the U.S. National Institute of Standards and Technology (NIST) as follows:

A model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three delivery models, and four deployment models [1].

Major benefits of cloud computing are low costs and high convenience. Since cloud computing is accessible and centralized, therefore, new opportunities are created for security breaches. Cloud computing security can be estimated through both the offensive and defensive perspectives. In this paper classification of various attacks in cloud to examine to what degree proposed defenses can address are going to be discussed.

2. CHARACTERISTICS AND ARCHITECTURE

As outlined by Mel and Grance [2], cloud computing generally has five characteristics:

- 1. Resource pooling :** The resources are pooled by the cloud providers and shared between multiple customers according to their requirements.
- 2. Broad network access:** These resources on the cloud are accessible through standard network protocols over the Internet.
- 3. Rapid Elasticity:** In a matter of minutes resources may be provisioned to scale out and released to scale in. Therefore elasticity of resources is very rapid.
- 4. Measured service:** The cloud provider measures and generally charges for usage of CPU, memory, disk, network bandwidth, or other resources.
- 5. On-demand self-service:** Resources can be provisioned via automated mechanisms at the time of their demand only.

To understand the nature and security of cloud computing, we need to understand the architecture of cloud to provide security against different types of attacks, criminals, intruders, etc. Figure 1 describes the standard architecture of cloud infrastructure. This same architecture can be used to describe all the models of the cloud computing which are IaaS (Infrastructure as a Service), PaaS (Platform as a Service), SaaS (Software as a Service).

3. CLOUD COMPUTING ATTACKS

Since companies are moving towards cloud computing, care must be taken against hackers. The attacks which criminals or hackers may attempt include:

3.1 Denial-of-Service attack(DoS)

Cloud is more penetrable to DoS attacks, because so many users are involved in the usage of cloud services and resources, therefore DoS attacks can be more damaging. When workload start increasing on Cloud, Cloud Computing operating system start to provide more computational power in the form of more virtual machines, more service instances to cope with the additional workload. Thus, the server hardware boundaries for more workload start restricting. In that sense, the Cloud system is trying to work against the attacker (by providing more computational power), but actually to some extent even supports the attacker by enabling the attacker to do most possible damage on a services availability, starting from a single flooding attack entry point. Thus, the attacker does not have to flood all n servers that provide a certain service in target, but merely can flood a single, Cloud-based address in order to perform a full loss of availability on the intended service [3].

Some security concerning professionals proposed solution aims to detect and analyze Distributed Denial of Service (DDoS) attacks in cloud computing environments, using Dempster- Shafer Theory (DST) operations in 3-valued logic and Fault-Tree Analysis (FTA) for each VMbased Intrusion Detection System (IDS) [4].

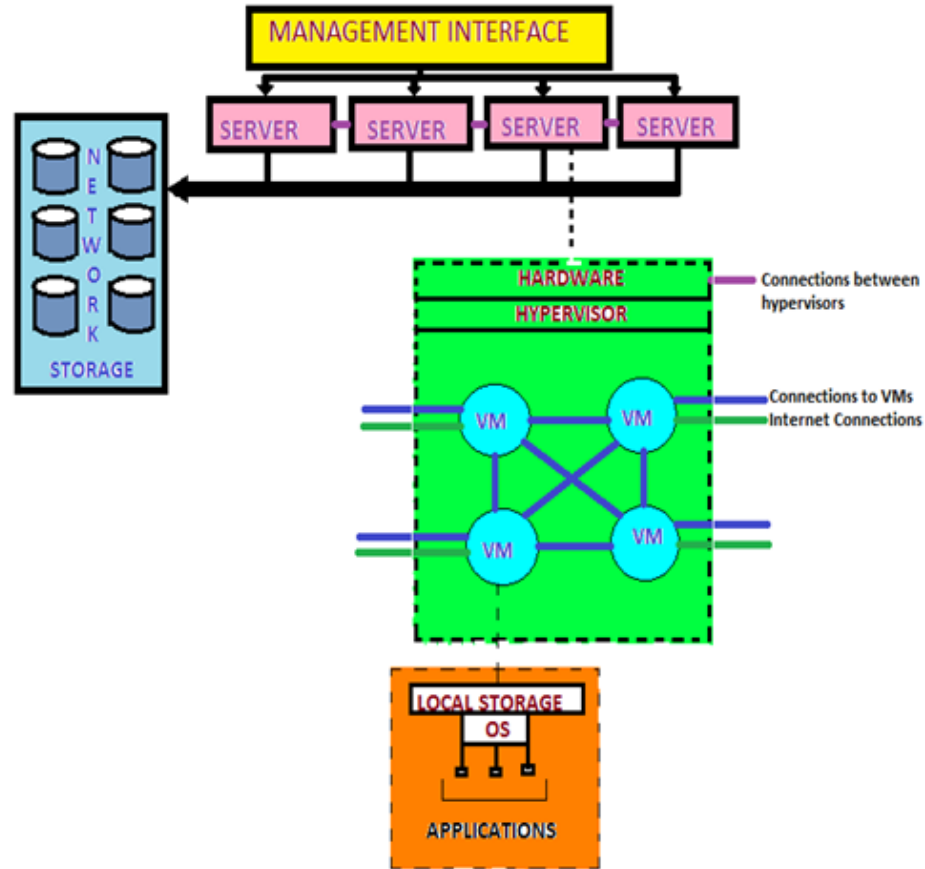


Figure 1. Architecture of Cloud Infrastructure

Solution of DoS attack

The DoS attack grows in stages-Research, Connect/Compromise, Transact/Extract [5]. Each stage depends upon the success of the previous stages while Research stage plays an important role. Some possible solutions against formal DoS can be:

1. Combination of DoS attack detection, classification of traffic and response tools can be used to block traffic as they identify illegitimate/unauthorized and allow traffic as they identify legitimate/authorized.
2. Firewalls can be used to allow or deny access protocols, ports or IP addresses. As if a simple attack is coming from a few unusual IP addresses, a simple rule could be put up in cloud authentication system to drop all unauthorized incoming traffic.
3. Most of the switches have rate-limiting and Access Control List capability and some provide reasonable automatic and/or system-wide rate limiting, deep packet inspection, traffic shaping, delayed binding (TCP splicing), and Bogon filtering (bogus IP filtering) which can detect and amend DoS attacks through automatic rate filtering mechanisms and WAN Link failover and balancing mechanisms.
4. Similar to switches, routers have some rate-limiting and ACL capabilities. They, too, manually set rules and regulations. Most routers can be easily deluged under DoS attack scenario.
5. Front end hardware of the application is intelligent hardware device placed before traffic reaches to

servers side on the network. It can be used on networks in colligation with routers and switches. Cloud Application front end hardware resources analyze data packets as they enter into the network system, then identification based on priority, regular, or dangerous is done.

6. IPS (Intrusion-prevention systems) are effective if the attacks have different signatures. Intrusion prevention systems works on content recognition but cannot block behavior based DoS attacks.

7. Blackholing: All the traffic to the attacked packets are sent to a "black hole" (null interface, non-existent serve). To be more efficient and avoid affecting of network infrastructure connectivity, it can be managed by the ISP systems.

8. Sink holing: It routes to a valid IP address which analyzes network traffic and rejects bad ones. Sink holing is not that much of efficient for most serious server side attacks.

3.2 CLOUD MALWARE- INJECTION ATTACK

It is the first considerable attack attempt that inject implementation of a malicious service or virtual machine into the Cloud. The purpose of malware cloud be anything that the adversary is interested in, it may include data modifications, full functionality changes/reverse or blockings. In this attack adversary creates its own malicious service implementation module (SaaS or PaaS) or virtual machine instance (IaaS), and add it to the Cloud system. Then, the adversary has to pretend to the Cloud system that it is some the new service implementation instance and among the valid instances for some particular service attacked by the adversary. If this action succeeds, the Cloud automatically redirects the requests of valid user to the malicious service implementation, and the adversarys code is executed. The main scenario behind the Cloud Malware Injection attack is that an attacker transfers a manipulated/wrong copy of a victims service instance so that malicious instance can achieve access to the service requests of the victims service. To achieve this, the attacker has to derive control over the victims data in the cloud. According to classification, this attack is the major representative of exploiting the service-to-cloud attack surface [6].

Malware-Injection Attack Solution

1. Generally, when a customer opens an account in the cloud, an image of the customers VM in the image repository system of the cloud is provided by the provider. The applications run by the customer are considered with high efficiency and integrity. Consideration of the integrity in the hardware level should be taken into account, because it is very difficult for an attacker to intrude in the IaaS level. File Allocation Table (FAT) system architecture is utilized, since its straightforward technique is supported by all existing virtual operating systems. From the FAT table information about the code or application that a customer is going to run can be fetched. Check over the previous instances that had been already executed from the customers machine can be put to determine the validity and integrity of the new instance. For this purpose, a Hypervisor at the providers end need to be deployed. This Hypervisor will be considered the most secured and sophisticated part of the cloud system whose security cannot be breached by any means. The Hypervisor is responsible for scheduling all the instance services, but before scheduling it will check the integrity of the instance from the FAT table of the customers VM.

2. Other approach is to store the OS type of the customer in the first phase when a customer opens an account. As the cloud is totally OS platform independent, before launching an instance in the cloud, cross checking can be done with the OS type from which the instance was requested from with the account holders OS type[7].

3.3 Side Channel attack

An attacker attempts to compromise the cloud system by placing a malicious virtual machine in close proximity to a target cloud server system and then debut a side channel attack. Side-channel attacks have egressed as a kind of effective security threat targeting system implementation of cryptographic algorithms. Evaluating a cryptographic systems resilience to side-channel attacks is therefore important for secure system design [8]. Side channel attacks use two steps to attack- VM CO-Residence And Placement i.e., an attacker can often place his or her instance on the same physical machine as a target instance and VM Extraction i.e., the ability of a malicious instance to utilize side channels to learn information about co-resident instances.

Side Channel Attack Solution: Utilizing side-channel attacks, it can be very easy to gain secret information from a device so security against side channel attack in cloud computing should be provided. In order to achieve this, combination of virtual firewall appliance and randomly encryption decryption (using concept of confusion diffusion) is used because security against both front end and back end side of cloud computing architecture is provided by this combination and also provide RAS (Reliability, Availability, and Security).

1. Virtual Firewall Appliance: As per Amazon EC2 service case study it is possible to adversaries or intruders identify the targeted VM in cloud infrastructure and then instantiate new VM to targeted VM and extract confidential information but we implement virtual firewall in cloud server so when adversaries identify targeted VM in cloud infrastructure and then place an instantiate VM to targeted VM, virtual firewall prevent this placement step inside channel attack.

2. Randomly encryption decryption: Now-a-days cloud computing services are already used for e-commerce applications, medical record services, and bank-office business applications , which require strong security guarantees. For providing more security randomly encryption decryption using concept of confusion and diffusion is used to prevent second step extraction of side channel attack. Confusion refers to making the relationship between the plaintext and the ciphertext as complex as possible; diffusion refers to the property that the redundancy in the statistics of the plaintext is "dissipated" in the statistics of the ciphertext. Or we can say, the non-uniformity in the distribution of the individual letters in the plaintext should be redistributed into the non-uniformity in the distribution of much larger structures of the ciphertext, which is much harder to detect.

In randomly encryption decryption, front end side of cloud computing architecture, clients confidential information, important file and documents are encrypted by encryption algorithm which using concept of confusion diffusion like Data Encryption Standard (DES), 3DES, Advance Encryption Standard (AES), Feistel encryption. Randomly encryption decryption means front end side of clients data or information encrypted through different encryption algorithm which used concept of confusion diffusion and as per National Institute Of Standard And Technology (NIST) AES, DES, 3DES are most secure algorithm for encryption decryption. For using randomly encryption decryption each and every time clients data or information encrypted through different encryption algorithm so adversaries or intruders have more difficulties to detect or extract cryptography key and encrypted data sent over internet network to back end side of cloud computing [9].

3.4 Authentication attack

Authentication is a weak issue in the hosted and virtual services and is very frequently targeted. There are so many ways to authenticate users which can be based upon what a user knows, has, or is. The mechanisms and the methods that are used to secure the authentication process are mostly targeted by the attackers. Recently, regarding the architecture of cloud computing, SaaS, IaaS and Paas, there is only IaaS which is able to offer this kind of information protection and data encryption. If the transmitted data confidentiality is under the category high for any enterprise, the cloud computing service based on IaaS architecture will be the most suitable and possible solution for secured data communication. In addition, the authorization of data process or management for those data belonged to the enterprises but stored on the service provider's side must be authorized by the user side (enterprises) to instead of the service providers [10].

Authentication Attack Solution

Most user-facing services today still use simple username and password type of knowledge-based authentication, with the exception of some financial institutions which have deployed various forms of secondary authentication (such as site keys, virtual keyboards, shared secret questions, etc.) to make it a bit more difficult for popular phishing attacks.

3.5 Man-In-The-Middle Cryptographic Attacks

This attack is carried out when an attacker places himself between two users. Anytime attackers can place themselves in the communications path, there is the possibility that they can intercept and modify communications[10].

Man-In-The-Middle Cryptographic Attack Solution

1. This type of attack can be prevented with the help of authentication process to check the identity of customers as discussed in the malware injection attack solution section. This authentication process can be very effective for the authentication of the users.
2. The integrity of the data should be maintained by applying encryption and decryption techniques on the data sent over the network.

4. RELATED WORK

Cloud is a new concept and many security professionals provided a numbers of security schemes till date. Several reviews have already been performed regarding both to the cloud infrastructure and its present state of security. Almorsy et al. [11] break cloud infrastructure down into the component service models Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) (See Section II). Chen et al. [12] go on to review whether or not there are any new threats or protections within cloud security. They make the point that some of the threats seen so far within the cloud infrastructure are new only in the sense that they are being seen in the cloud computing model rather being used to target single machines (e.g. installation of malware). Lastly, Lombardi et al. [13] gave an overview of the current threat model of the cloud, providing both a list of attacks and the requirements for

these attacks. Following their definition of the current threat model of the cloud, they present a detailed framework to categorize the attacks (our attack categorization is similar, but not identical, to theirs). While these reviews have made notable contributions to analyzing the current state of cloud security, none of them cover both cloud attacks and defenses.

5. CONCLUSION

As cloud computing is on the rise, and especially due to its enormous attraction to organized criminals, we can expect to see a lot of security incidents and new kinds of vulnerabilities around it within the decades to come. This paper gives an overview of the cloud computing attacks. Using the notion of attack surfaces, we illustrated the developed classification of cloud computing scenarios. Being a work-in-progress, we can continue with the collection and classification of cloud-based attacks and vulnerabilities in order to prove or controvert our attack taxonomies applicability and appropriateness.

References

- [1] P. Mell and T. Grance, "The nist definition of cloud computing (draft)," *NIST special publication*, vol. 800, no. 145, p. 7, 2011.
- [2] T. Grance and P. Mell, "The nist definition of cloud computing," *National Institute of Standards and Technology (NIST)*, 2011.
- [3] M. H. Sqalli, F. Al-Haidari, and K. Salah, "Edos-shield-a two-steps mitigation technique against edos attacks in cloud computing," in *Utility and Cloud Computing (UCC), 2011 Fourth IEEE International Conference on*, pp. 49–56, IEEE, 2011.
- [4] A. M. Lonea, D. E. Popescu, and H. Tianfield, "Detecting ddos attacks in cloud computing environment.," *International Journal of Computers, Communications & Control*, vol. 8, no. 1, 2013.
- [5] J. Pescatore, "How ddos detection and mitigation can fight advanced targeted attacks," tech. rep., SANS Analyst Program.
- [6] M. Jensen, J. Schwenk, N. Gruschka, and L. L. Iacono, "On technical security issues in cloud computing," in *Cloud Computing, 2009. CLOUD'09. IEEE International Conference on*, pp. 109–116, IEEE, 2009.
- [7] K. Zunnurhain and S. Vrbsky, "Security attacks and solutions in clouds," in *Proceedings of the 1st international conference on cloud computing*, pp. 145–156, Citeseer, 2010.
- [8] Q. Luo and Y. Fei, "Algorithmic collision analysis for evaluating cryptographic systems and side-channel attacks," in *Hardware-Oriented Security and Trust (HOST), 2011 IEEE International Symposium on*, pp. 75–80, IEEE, 2011.
- [9] B. Sevak, "Security against side channel attack in cloud computing," *International Journal of Engineering and Advanced Technology (IJEAT)*, vol. 2, no. 2, p. 183, 2013.
- [10] A. Singh and M. Shrivastava, "Overview of attacks on cloud computing," *International Journal of Engineering and Innovative Technology (IJEIT)*, vol. 1, no. 4, 2012.
- [11] M. Almorsy, J. Grundy, and I. Müller, "An analysis of the cloud computing security problem," in *the proc. of the 2010 Asia Pacific Cloud Workshop, Colocated with APSEC2010, Australia*, 2010.
- [12] Y. Chen, V. Paxson, and R. H. Katz, "Whats new about cloud computing security," *University of California, Berkeley Report No. UCB/EECS-2010-5 January*, vol. 20, no. 2010, pp. 2010–5, 2010.
- [13] F. Lombardi and R. Di Pietro, "Secure virtualization for cloud computing," *Journal of Network and*

Computer Applications, vol. 34, no. 4, pp. 1113–1122, 2011.

About This Journal

MCCC is an open access journal published by Scientific Online Publishing. This journal focus on the following scopes (but not limited to):

- Autonomic Business Process and Workflow Management in Clouds
- Cloud Composition, Federation, Bridging and Bursting
- Cloud Computing Consulting
- Cloud Configuration, Performance and Capacity Management
- Cloud DevOps
- Cloud Game Design
- Cloud Migration
- Cloud Programming Models and Paradigms
- Cloud Provisioning Orchestration
- Cloud Quality Management and Service Level Agreement (SLA)
- Cloud Resource Virtualization and Composition
- Cloud Software Patch and License Management
- Cloud Workload Profiling and Deployment Control
- Cloud Video and Audio Applications
- Economic, Business and ROI Models for Cloud Computing
- Green Cloud Computing
- High Performance Cloud Computing
- Infrastructure, Platform, Application, Business, Social and Mobile Clouds
- Innovative Cloud Applications and Experiences
- Security, Privacy and Compliance Management for Public, Private and Hybrid Clouds
- Self-service Cloud Portal, Dashboard and Analytics
- Storage, Data and Analytics Clouds

Welcome to submit your original manuscripts to us. For more information, please visit our website:

<http://www.scipublish.com/journals/MCCC/>

You can click the bellows to follow us:

- ✧ Facebook: <https://www.facebook.com/scipublish>
- ✧ Twitter: <https://twitter.com/scionlinepub>
- ✧ LinkedIn: <https://www.linkedin.com/company/scientific-online-publishing-usa>
- ✧ Google+: <https://google.com/+ScipublishSOP>

SOP welcomes authors to contribute their research outcomes under the following rules:

- Although glad to publish all original and new research achievements, SOP can't bear any misbehavior: plagiarism, forgery or manipulation of experimental data.
- As an international publisher, SOP highly values different cultures and adopts cautious attitude towards religion, politics, race, war and ethics.
- SOP helps to propagate scientific results but shares no responsibility of any legal risks or harmful effects caused by article along with the authors.
- SOP maintains the strictest peer review, but holds a neutral attitude for all the published articles.
- SOP is an open platform, waiting for senior experts serving on the editorial boards to advance the progress of research together.