Cloud Computing: Threats, Attacks and Solutions

Parveen Kumar
Assistant Professor, Computer Science Department, SPN College Mukerian, India.

Abstract – This paper is aimed to present information about the most current attacks on cloud computing, as well as security measures. Due to its emergence a number of attacks can be performed over the cloud by the attackers or intruders. Cloud computing provide a powerful computing platform that enables individuals and organizations to perform variety levels of tasks such as: use of online storage space, adoption of business applications, development of customized computer software, and creation of a "realistic" network environment. In this paper different types of attacks on cloud computing and their respective solutions are discussed. [1]Security of cloud is of great concern hence care must be taken to provide secure cloud and secure cloud services.

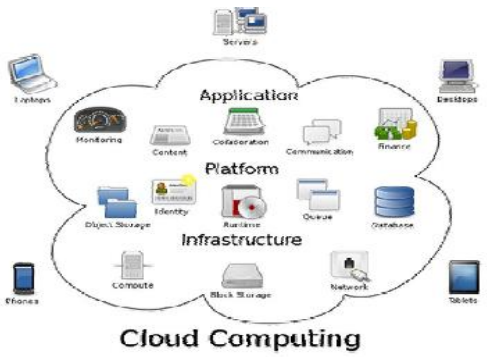
Index Terms – Authentication; Denial-of-service, DDOS, Malware-Injection Side-channel; Man-in-the-middle Attacks.

1. INTRODUCTION

Cloud computing is currently one the most hyped IT innovations. Most IT companies announce to plan or already have IT products according to the cloud computing paradigm. Though cloud computing itself is still not yet mature enough, it is already evident that it's most critical flaw according to public consent is security. In the nearest future, we can expect to see a lot of new security exploitation events around cloud computing providers and users, which will shape the cloud computing security research directions for the next decade[2]. Hence, we have seen a rapid evolution of a cloud computing security discipline, with ongoing efforts to cope with the idiosyncratic requirements and capabilities regarding privacy and security issues that this new paradigm raises. In line with these developments, the authors closely watch cloud computing security on a very technical level, focusing primarily on attacks and hacking attempts related to cloud computing providers and systems.

So the term cloud refers to the web or internet. Cloud computing is a metaphor for transferring the information services from the internet. With the help of web-based tools and applications, information is transmitted to the internet. Cloud computing is a compilation of existing approaches and technologies, Preplaced among a brand infrastructure paradigm that provides improved measurability, elasticity, business process, quicker startup time, reduced management prices and just-in-time accessibility of resources. Resources include database, software, service and server and so on.

In cloud computing, cloud actors play a major role. Cloud actors are referred as cloud agents. Two cloud actors are used. They are cloud provider and cloud consumer. A cloud provider is an organization responsible for providing cloud services to cloud consumers based on service level agreement (SLA). Cloud provider is also referred as data owner. Examples of cloud providers are Google, Amazon Web Service, IBM, Microsoft, eBay, Salesforce.com and os on. Cloud provider offers the owned IT resources to the cloud consumers for lease. Cloud consumer is an organization that uses IT resources based on the contract with a cloud provider. Cloud consumer is also referred as a client. The following Fig1. Illustrates the diagrammatic representation of cloud computing. Referring the diagram, cloud provider hosts the services in the cloud storage Cloud consumer can use the services that have been stored in the cloud storage. With the help of internet, cloud users can access there sources through mobile phone, laptop and other devices.



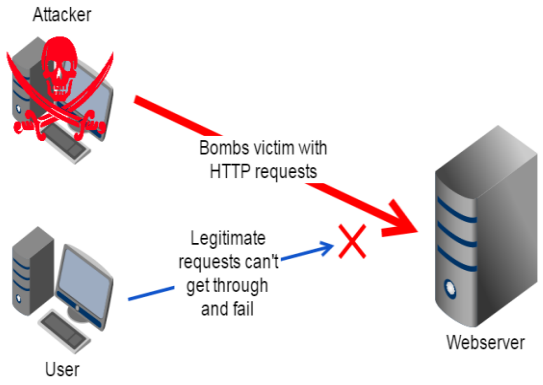
2. SECURITY ATTACK ON CLOUD COMPUTING

At present, many of the organizations uses cloud computing to share the confidential data. Many hackers trying to violate the security to use the cloud resources. Security attack is an intelligent act that attempts to violate the services in the cloud. Different types of attacks are used by the hackers to prevent the cloud users to access the data in the cloud.

2.1 Denial of Service (DOS) attack

In DoS attack, the attacker tries to prevent the legitimate users to access the resources in the cloud. In this attack, bulk messages are sent by the attacker querying the server to verify the requests. While verifying the requests, it has returned invalid addresses. The attacker return address has not been able to find by the network or server. While verifying requests, attackers make the server to pause before ending the connection.[3] When the connection is closed by the server,

the hacker sends more valid messages with invalid addresses. This makes the network or server in a busy state. This attack causes the network traffic and services are not accessible by users. 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 single flooding attack entry point. Thus, the attacker does not have to flood all n servers that provide ascertain 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

2.2. Denial of Service attack solution

DOS attack is prevented by using prior automatic switches that provide the packet rate analysis. DOS attack is mainly used to protect the network traffic against authorized and unauthorized users.

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.

Firewalls can be used to allow or deny access protocols, ports or IP addresses. [4]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.

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.

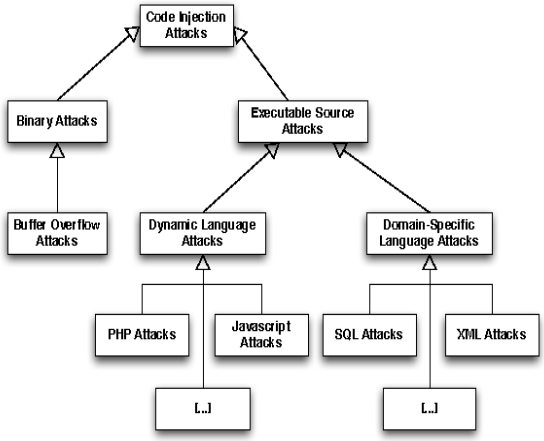
Similar to switches, routers have some rate-limiting and ACL capabilities. They, too, manually set rules and regulations. Most routers can be easily deluged under DoS attack scenario.

Black holing: All the traffic to the attacked packets are sent to a ”black hole” (null interface, nonexistent serve). To be more efficient and avoid affecting of network infrastructure connectivity, it can be managed by the ISP systems[5].

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.

2.3 Malware injection Attack

In a malware injection attack, an attacker tries to insert mischievous code or service which emerges like the existing services executing in the cloud. This attack is also known as driven-by downloading or meta-data spoofing attack. Attackers steal the information from Internet by forcing the users to download the malicious software automatically without the knowledge of users. By doing this, reliability of the service is not verified. 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 adversaries code is executed[6]. 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.

2.4 Malware-Injection attack solution

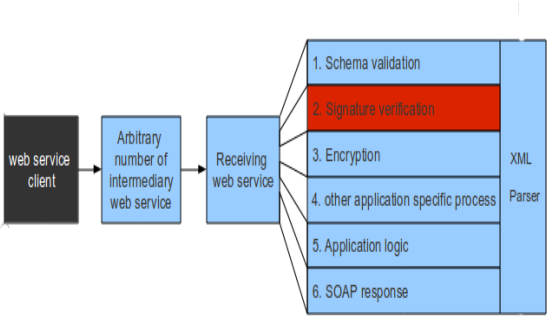
The malware-injection attack is prevented by allowing the cloud users to create an account in the cloud and provider creates the copy of cloud user's VM image in the cloud image storage system. In this file allocation table is used to determine the current code that is being run by the client. Integrity is checked by using File Allocation Table (FAT) from the user's virtual machine. Virtual machine image repositories such as VMware's Virtual Appliance Market Place and Amazon EC2.

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.

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, crosschecking can be done with the OS type from which the instance was requested from with the accountholders OS type.

2.5 Wrapping attack

The attack uses a method known as XML signature wrapping and shows vulnerabilities while executing the web service request[7]. In wrapping attack, the attacker tries to insert the malicious element in the SOAP(Simple Object Access Protocol) message structure in Transport Layer Service(TLS) and after inserting the malicious code fake content of the message is copied into the server and while executing, cloud server working is interrupted by the attacker.

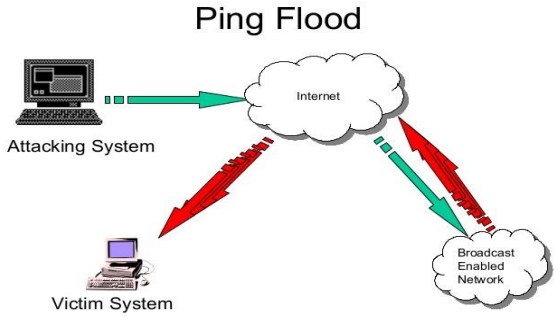


2.6. Wrapping attack solution

The Wrapping attack is prevented by increasing the security while sending the message from a web server to a web browser by using SOAP messages. An extra bit called STAMP bit is added to the signature value and is included in the SOAP header. This extra bit prevents the attacker by changing the signature value. Uses a method known as XML signature wrapping and shows vulnerabilities while executing the web service request. In wrapping attack, the attacker tries to insert the malicious element in the SOAP (Simple Object Access Protocol) message structure in Transport Layer Service (TLS) and after inserting the malicious code, fake content of the message is copied into the server and while executing, cloud server working is interrupted by the attacker.

2.7 Flooding attack

In flooding attack, an adversary can easily create fake data and whenever the server is overloaded, it allocates the job to the nearest server and specific server is itself offload. While allocating, it offers more capable and quicker processing request.



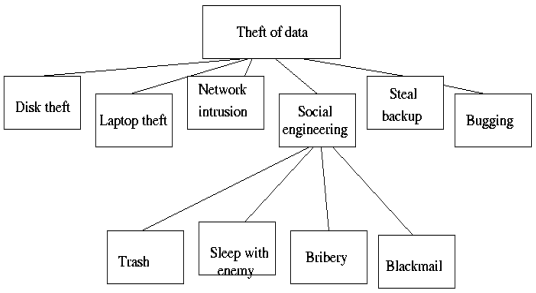
While processing the requests, the server first validates the legitimacy of the requested requests and also invalid requests must be validated to verify the authenticity and also checks the consumption of CPU utilization and memory allocation and causes the flooding of a system.

2.8 Flooding attack solution

Flooding attack is prevented by challenger to add fake data by allocating each server to perform a specific job and all the servers are internally communicating with each other quickly through message passing. When the server is overloaded, a new server is employed with the destination of the requests of the overloaded server. In this PID is appended to the message to identify the requests of the valid customer and PID is encrypted by using RSA or hash value implementation.

2.9 Data stealing attack:

Data stealing attack [8] is the most widely used traditional approach to verify the user account. In this attack, attack steals the information of user account and password. In this attack, confidential information about the user is lost by the activity of the challenger.

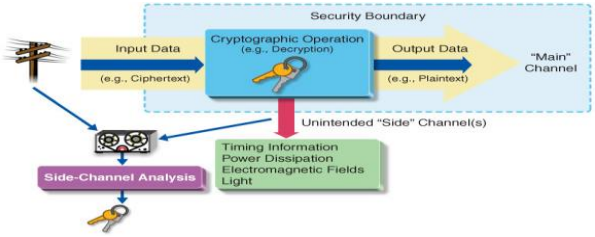


2.10 Data stealing attack solution

The data stealing attack is prevented from generating a unique number to the customer while login every time to use the system. When the session is expired, PID generator is used to commit the task and PID generator is present inside the hypervisor.

2.11 Side Channel attack

An attacker attempts to compromise the cloud system by placing a malicious virtual machine in close propinquity to a target cloud server system and then debut a side channel attack[9]. Side-channel attacks have egresses 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 .



Side channel attacks use two steps to attack- VM CO-Residence And Placement item 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.

2.12 Side Channel Attack Solution

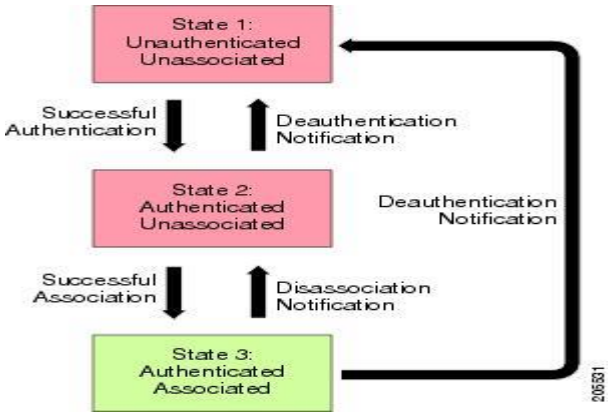
Utilizing side-channel attacks, it can be very easy to gain secret information from a device so security against side channel attack in cloud computing should be provided. In order to achieve this, combination of virtual firewall appliance and randomly encryption decryption (using concept of confusion 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).

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[10].

Randomly encryption decryption: Now-a-days cloud computing services are already used for ecommerce 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 cipher text. 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.

2.13 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[11]. 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.

2.14 Authentication Attack Solution

Most user-facing services today still use simple username and password type of knowledge-base 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 abit more difficult for popular phishing attacks.

3. 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 taxonomy's 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 andTechnology (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] Kalyani Kadam, Rahul Paikrao, Ambika Pawar, "Survey on Cloud Computing Security", IJETAE, Volume 3, Issue 12, December 2013.

[7] AbhinayB. Angadi, Akshata B. Angadi, Karuna C. Gull, "Security Issues with Possible Solutions in Cloud Computing-A Survey", IJARCET, Volume 2, Issue 2, February 2013.
[8] A. N. Suresh, Ch. Sailaja, G. Gayatri, D.V.S. Deepak, "Security Challenges In Cloud Computing", IJERT, Vol. 2 Issue 2, February- 2013.

[8] Dr.Nedhal A. Al-Saiyd, Nada Sail, "Data Integrity in Cloud Computing Security", Journal of Theoretical and Applied Information Technology, 31st December 2013. Vol. 58 No.3
[10] Rushikesh Vilas Belamkar, "Challenges and Security Issues in Cloud Computing", ISRJ, ISSN 2230-7850, Volume-4, Issue-2,March-2014.

[9] M. Almorsy, J. Grundy, and I. Muller, "An analysis of the cloud computing security problem," in ¨ *the proc. of the 2010 Asia Pacific Cloud Workshop, Colocated with APSEC2010, Australia*, 2010.