IJRSET August 2015 Volume 2, Issue 6 Pages: 24-28

ISSN 2394-739X

International Journal for Research in Science Engineering and Technology

A Survey on Cloud Security Issues and Attacks

[1] Mrs. Antony Cynthia, M.sc, MCA., M.Phil., [2] A. Mary Theresa.MCA,
[1] Asst Professor, [2] M.Phil Research Scholar,
[1] Dept of Computer Application, [2] Dept of Computer Application,
[1&2] Hindustan College of Arts and science, Coimbatore.

Abstract:-

Today's world is widely using Cloud Computing because of its global nature. 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 surveyed. Security of cloud is of great concern hence care must be taken to provide secure cloud and secure cloud services.we outline several threat models for cloud computing systems, discuss specific attack mechanisms, and classify proposed defenses by how they address these models and counter these mechanisms. This examination highlights that, while there has been considerable research to date, there are still major threats to cloud computing systems.

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:

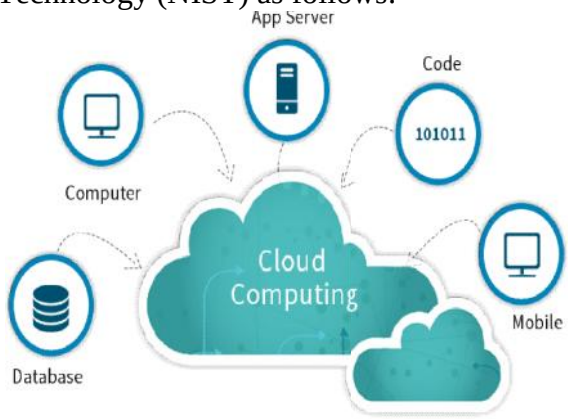

Figure 1: Cloud Architecture

A model for enabling convenient, on-demand network access to a shared pool of configurable computingresources that can be rapidly provisioned andreleased with minimal management effort or service provider interaction. This cloud model promotesavailability and is composed of five essential characteristics, three delivery models, and four deploymentmodels .Many security researchers have studied various aspects of cloud computing security from both an offensive and defensive perspective. In this paper we give a high-level classification of this work in order to examine to what degree proposed defenses

can address different kinds of cloud-specific attacks. Specifically, we organize the cloud security literature into five areas: colocation denial of service, colocation breaches of confidentiality, data integrity and availability, data confidentiality, and infrastructure compromise. As we will show, while there has been significant progress, there remain major shortcomings in cloud defenses, even from the perspective of published research. While therehave been other cloud security surveys and classifications published, ours is the first one organized around cloud-specific attacks and defenses. Our hope is that this survey can help guide researchers to work on areas of cloud security that have been less studied.

The overarching goal of Cloud Computing is to provide on-demand computing services with high reliability, scalability, and availability in distributed environments. Up to date, there is no unified cloud computing definition, the representative definitions of industry and academia are the follows. Cloud computing is computing as it has long been the dream of a new infrastructure of this title, it is the most recent is rapidly into commercial reality .Cloud Computing is defined as: the term used to describe both the cloud computing platform for a system or a type of application. In cloud computing may face different risks. In cloud computing environment, many users participate in the cloud and they join or leave cloud dynamically. The number of user changes dynamically, as well as users use the different services, leading the user can not be classified. Other resources in the cloud computing environments are the same too. They should be able to deal with the changing dynamically. The cloud includes distributed users and resource from distributed local systems or organizes, which have different security policies. According to this reason, how to build a suitable relationship among them is a challenge. Also, Cloud computing environment is a virtualized environment; it cannot be clearly defined boundaries to protect the device user. The proposed research is to analyze the security requirements in cloud computing environment, detail the novelties in cloud threat model, present new problems and new research directions in cloud computing security.

- **Privacy Issues**
- **Data Ownership and Content Disclosure Issues**
- **Data Confidentiality**
- **Data Location Control Issuesλ**
- **Regulatory and Legislative Compliance**
- **Forensic Evidence Issues**
- **Auditing Issues**
- **Business Continuity and Disaster Recovery Issues**
- **Trust Issues**
- **Security Policy Issues**
- **Emerging Threats to Cloud computing.**

2. THE ATTACK CLOUD COMPUTING

A cloud computing scenario can be modeled using three different classes of participants: service users, service instances (or just services), and the cloud provider . Every interaction in a cloud computing scenario can be addressed to two entities of these participant classes. In the same way, every attack attempt in the cloud computing scenario can be detailed into a set of interactions within this 3 class model. For instance, between a user and a service instance one has the very same set of attack vectors that exist outside the cloud computing scenario. Hence, talking about cloud computing security means talking about attacks with the cloud provider among the list of participants. it may also just play

an intermediate role in an ongoing combined attack

(a) Service-to-User
(b) User-to-Service
(c) Cloud-to-Service
(d) Service-to-Cloud
(e) Cloud-to-User
(f) User-to-Cloud

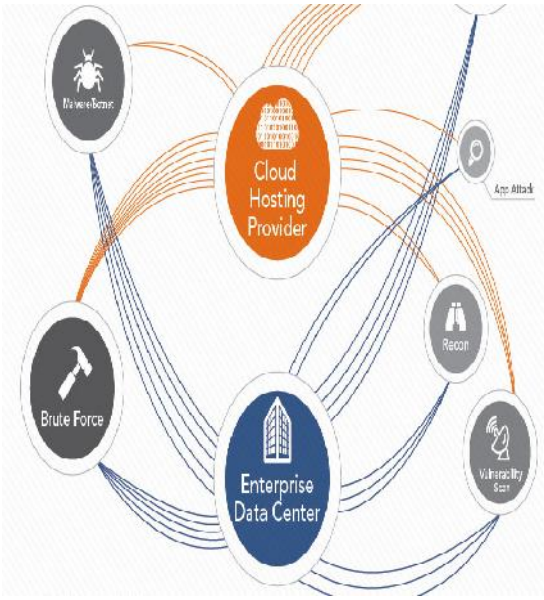

Figure 2: Attack model in cloud

3. Types of Flooding Attacks

There are various kinds of flooding attacks, including: ICMP flooding, UDP flooding, TCP SYN and indirect attacks It is difficult for hackers to understand the infrastructure of a private cloud, so inside attackers are generally the first suspects for any kind of attacks in a private cloud. On the other hand, in a public cloud the flexible infrastructure of public clouds make them easy to penetrate and more vulnerable to outside attackers. We now describe different types of attacks .

3.1 ICMP Flooding:

One example of ICMP(internet control message protocol)flooding is a Smurf attack in which ping requests with a spoof source address are sent asa broadcast message. Many hosts then respond to the ping with an echo to the spoofed source address, which is the victim of the attack. For this type of attack in a cloud, the attacker is masked as an insider, because the spoof IP address can bea registered user of the cloud.

3.2 UDP Flooding/Spoof:

A UDP (user datagram protocol) flooding attack can be initiated by sending a large quantity ofpackets, using UDP or TCP, to randomports on a remote host. In response to a packet received from a port, adistant host will check for an application listening at that port. Since no applications are listening at the random ports, the host will respond to the large quantity of packets by sending many ICMPDestination Unreachablepackets, eventually resulting init beingunreachable by other clients. In a UDP spoof, an attacker sends a UDP packet to a random ort of the victim's system with a spoof source IP address. The attacker then continues to send additional packets. Eventually, the system tries to verify the spoofed IP address with its ACL Access Control List) or legitimate user addresses, and finds nothing about the mentioned address. to this point, the attack has already committed its intentional task of occupying the resources of the system. Following this step, multiple packets are sent and the attacker is successful in occupying he total resources of the sever.Both ICMPfloodingandUDPflooding can occur in clouds.These attack unknowingly propagated from a cloud maycompromise a legitimate ser. Traditional solutions to prevent this type of attack require the use of additional hardware, aall or new devices. Requiring this additional hardware of a customer is not an acceptable solution in a cloud system.Most of the communications in a cloud or grid take place in the transport layerof the network.InTCP/IPthere are fewer

layers with less overhead, smaller packets,and fewer redundant bits than the OSImodel. With fewer bits,utilizing checksumbecomes more complex.As a result, theTCP layers are more vulnerable to attacks and most of he intrusions consider these layers as a medium of transporting their illegal intension to reach the main unitIn a cloud computing environment, the main unitwould include thecloud servers.Such an attack on a cloud system could be catastrophic.

3.3 TCP SYN flooding:

ATCP SYN attackexploits the fact thattotal communication takes place through a three-way handshake protocol. Requester sends a SYN (synchronization) packet to the server, theserver checks the packets and sends a SYN-ACK back to the requester and finally the requester sends an ACK back to the server to complete the communication path for transmitting further traffic. However, theattacker can send a very largenumber of SYN packets to the system and engagethe system with a bulk amount of SYN-ACK packets, whichengages the resources for a long time. These typesof attacks are sometimestraceable if the attacker uses his own IP address and that IP address can then be blocked. This type of attack is known as a direct attack. Indirect Attack: We must also considerwhat happensif the attacker uses some other handlers (zombies) to compel the attack. for example, the attacker machine (master) can commandthe handlers to send SYN packets to the victim machine with spoofed IP addresses. In this case, tracing the spoofed addresses of the handlers exhausts the system.Even if the systemfinds the handlers, it could bedifficult for theadministrators to find the actual attacker(s).While this scenario can occur in cloud systems, allowing the attack to continue in order to tryto trace it back is not a feasible solution. The time taken to trace back the attacker could negatively affect the response time for the customer and the elastic nature of the cloud could allow a tremendous increase in packets. Proxy serverscan be deployedto filter packets with spoofed source IP addresses(indirectly for DoS),but all proxy servers havelimitations. Usually the proxy servers are built for medium-sized industriesand arecapable of handling 15,000 requests/second for a total of 250,000 requests. Thiskind of system has to be adaptable and scalable to a large extent so that even the growthof requests in the system will not let the attackers penetrate the system.Since one of the characteristics of cloud computing is its scalability; deploying aproxy server may not provide the scalability needed by the cloud.

CONCLUSION

In this paper security considerations and challenges which are currently faced in the Cloud computing are highlighted. Cloud computing is still in its infancy, and how the security and privacy landscape changes will impact its successful, widespread adoption. Many enhancements in existing solutions as well as more mature and newer solutions are urgently needed to ensure that cloud computing benefits are fully realized as its adoption accelerates. Security and privacy will remain a major concern until users become fully aware of the “depth” of the cloud: who manages it, how he does it and whether the company can afford to “give away” its information - decision that can only be taken after a careful risks analysis and policy considerations otherwise we may simply get lost in the cloud.

REFERENCES

[1]. Mohamed, A.: A history of cloud computing
(2009),http://www.computerweekly.com
[2]. Gourley, B.: Cloud Computing and Cyber Defense. A White Paper provided to the National Security Council and

Homeland Security Council as input to the White House Review of Communications and Information Infrastructure, Crucial Point LLC (2009)
[3]. Reingold, B., Mrazik, R.: Cloud computing: the intersection of massive scalability, data security and privacy (Part I). Cyberspace Lawyer, [FNa1] 14 No. 5 GLCYLAW
[4]. United States National Standards for Information Technology,http://www.nist.gov/index.html
[5]. Dataline White Paper: Cloud computing for national security applications, http://www.dataline.com/soar.htm
[6]. Merrill Lynch, http://www.ml.com
[7]. Bruening, P., Treacy, B.: The Bureau of National Affairs, Inc. Cloud Computing: Privacy, Security Challenges, Privacy & Security Law. PVLR ISSN 1538-3423 (2009)
[8]. Binning, D.: Top five cloud computing security issues (2009), http://www.computerweekly.com
[9]. Gellman, R.: Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing, World Privacy Forum (2009)