International Journal of Modern Embedded System (IJMES)
Volume No.-5, Issue No.-1, February, 2017
ISSN: 2320-9003(Online)

Security Attacks on Cloud Computing: A Solution based Review

Mandeep Kaur
Astt. Prof. CGC Landran
mandeepkaur.cocse@cgc.edu.in

Dapinder kaur
Astt. Prof. CGC Landran
dapinder.coecse@cgc.edu.in

Simarjot kaur
Astt. Prof. CGC Landran
simarjot.cse@cgc.edu.in

Abstract: The term cloud computing seems to originate from computer network diagrams that represent the internet as a cloud. While cloud computing services have numerous potential benefits, there are also potentially significant privacy and security considerations that should be accounted for before collecting, processing, sharing, or storing institutional or personal data in the cloud. Cloud computing has been developing various applications in various environments. The earlier stages have been deployed by basic lifecycle standards. In the later stages of the product's lifecycle, the errors need to be preset by the newer necessities as this is unavoidable in the evolution of any software. In this paper we are discussing cloud computing attacks on cloud computing and cloud computing challenges.

Keywords: Cloud computing; Attacks, challenges, Ddos attack solutions

I. INTRODUCTION

Recent improvements in the field of cloud computing possess gigantically changed this path of finalizing as well as the perception of computing possessions [2]. Cloud computing, also known as on-demand computing, is a kind of Internet-based computing that provides shared processing resources and data to computers and other devices on demand. It is a model for enabling ubiquitous, on-demand access to a shared pool of configurable computing resources. Cloud computing is a model for enabling ubiquitous, 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[1]. Within a cloud structured processing basis, these possessions will be typically throughout in someone else's premise or maybe system and also got a chance to look at remotely via cloud clients [6].Cloud computing clients basically do not need to own the physical infrastructure of their own; rather the client rented the resources from a third-party provider to perform their tasks. This helps them to avoid huge space, time and the cost for owning the infrastructure.

The customer consumes the resources which they required for their service and pay only according to the resources that they used. Most services of cloud computing infrastructures delivered through common centers and built on servers. Sharing resources along with can improve, as the servers are not unnecessarily left idle, which can reduce the costs significantly on other side it can also increasing the speed of application development.

Fig.1. Features of Cloud Computing

II. Cloud Architecture

Cloud computing architecture comprises of two components "the front end" and "the back-end". The front end of the cloud computing system comprises the client's device it may include computer networks and some applications. These applications are needed for accessing the cloud computing system. The Back end refers to the cloud, which may encompass data storage systems, various computer machines (hardware), and servers. Group of these clouds which contains infrastructure, software and storage together build a whole cloud computing system itself. The whole system is monitored through a hub server that is also used for monitoring client's demand and for ensuring traffic smooth functioning of the system. A special type of software called "Middleware" is used that help or allow the connected computers on the network to communicate with each other. A Cloud computing systems must have a huge storage capability so that it can contain the copy of all client's data

to restore the service, which may be occurs due to a device collapse. The copying of data is called redundancy and cloud computing service providers also provide facility of data redundancy.

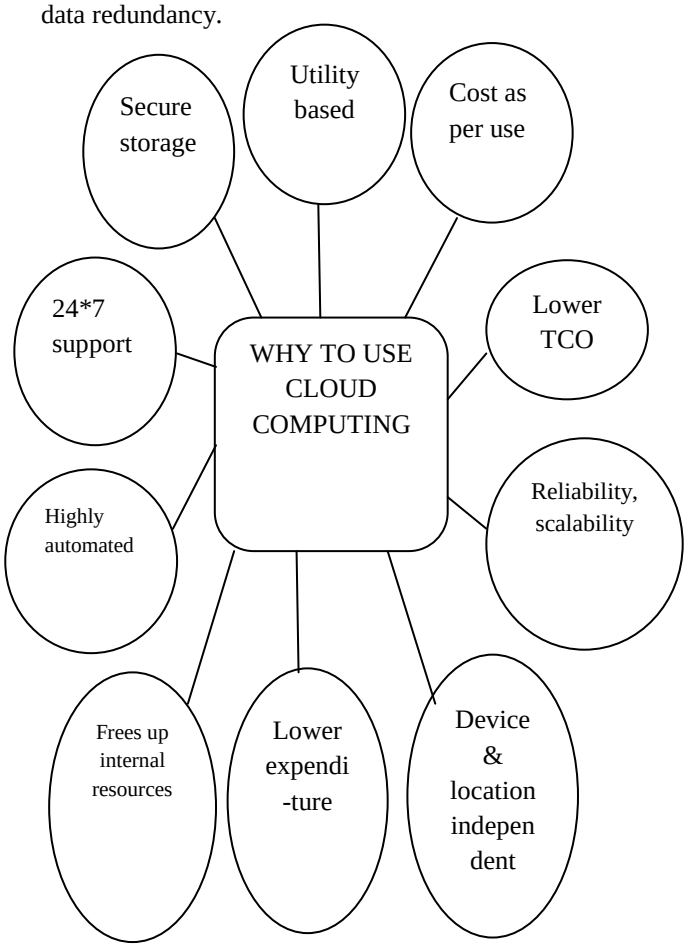

Fig.2. Reason Behind the Popularity of Cloud Computing

2.1 Cloud Computing Applications

Cloud computing might be a basic time period no matter what which includes giving published services over the web. These organizations are usually thoroughly conversing segregated in 3 instructions [12]:

i. Platform-as-a-Service (PaaS),
ii. Infrastructure-as-a-Service (IaaS),
iii. Software-as-a-Service (SaaS).

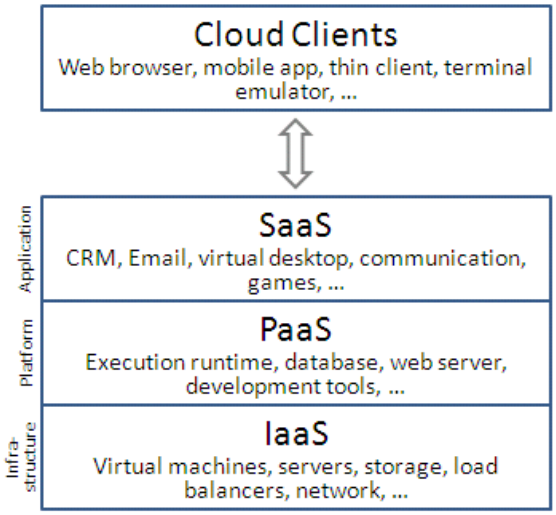

Fig. 3 Working layers of cloud computing

A. Iaas Service

Infrastructure as a Service could be a provision model during which a company outsources the instrumentation accustomed maintenance processes, composed with stowage, hardware, servers and networking parts. The service merchant owns the instrumentation and is liable for housing, running and maintaining it [4] [5]. The shopper usually pays on a per-use basis. IaaS atmosphere generally source additional assets as being a virtual-machine hard disk drive image selection, raw data block stowage, along with file or maybe enterprise stowage, load balancers, virtual native space networks (VLANs), firewalls, IP addresses, and software package bundles. IaaS-cloud merchants provide these resources on-demand [8] from their massive pools installed in information centers. For wide-area connectivity, customers will use either the web or carrier clouds (dedicated virtual non-public networks) [6].

To send their applications, cloud clients introduce working framework pictures and their application programming framework on the cloud foundation. Amid this model, the cloud client fixes and keeps up the working frameworks and hence the application programming bundle. Cloud dealers more often than not bill IaaS benefits on a utility computing premise: cost mirrors the amount of assets apportioned and devoured. Characteristics and modules of IaaS include [12] [20]:

- Efficacy computing service and billing model.
- Automation of administrative jobs.
- Dynamic scaling.

B. Paas Service

In the PaaS models, cloud providers convey a computing platform, normally including working framework, programming dialect execution environment, database, and web server. Application engineers can create and run their product arrangements on a cloud stage without the expense and unpredictability of purchasing and dealing with the

hidden equipment and programming layers [20]. With some PaaS offers like Microsoft Azure and Google App Engine, the basic PC and capacity assets scale consequently to match application request so that the cloud client does not need to apportion resources yourself. The recent has likewise been proposed by a Framework modeling meaning to real-time in cloud environments. Characteristics and components of PaaS include [15] [16]:

- On-demand self-service
- Broad network access
- Resource pooling
- Rapid elasticity
- Measured service

C. Saas Service

In the business model using software as a service (SaaS), purchasers are conveyed induction to application programming and databases. Cloud suppliers deal with the base and stages that run the applications. SaaS is now and again said as "on-interest programming" and is generally valued on a pay-every utilization premise. SaaS shippers all in all worth applications utilizing a membership expense [9].

In the SaaS model, cloud providers install and operate application software in the cloud and cloud users access the software from cloud clients. Cloud users do not manage the cloud infrastructure and platform where the application runs. This eliminates the need to install and run the application on the cloud user's personal pcs, which make simpler to do preservation and backing. Cloud applications are different from other applications in their scalability—which can be achieved by cloning tasks onto multiple virtual machines at runtime to meet changing work request. Burden balancers allocate the job over the set of virtual machineries [9]. This procedure is quite crystal clear to the cloud consumer, who usually sees solitary a single access point. To make available rooms regarding numerous cloud users, cloud purposes can be versatile, which is, virtually any machine will serve several cloud individual corporation.

III. Attacks on Cloud Computing

3.1 Wrapping Attack: Whenever a user makes a request from his VM (Virtual Machine) through the browser, the request is first directed to the web server. In the server, a SOAP message is generated. The message contains the structural information that will be going to be exchanged between the browser and server during the message passing. Before the occurrence of message passing process, the XML (EXtensible Markup Language) document needs to be signed and canonicalization has to be done. Also, the signature values should be attached with the document. At last, the SOAP header should contain all the necessary information for the destination after computation is done.

For a wrapping attack, the opposition does its trick during the translation of the SOAP message in the Transport Layer Service (TLS) layer. The body of the message is duplicated and sent it to the server as a legitimate user. The server checks the authentication by the (SV) Signature Value (which is also duplicated) and integrity checking for the message is done. As a result, the opponent is able to intrude in the cloud and can run malicious code to interrupt and chop up the usual functionalities of the cloud servers.

3.2 Flooding Attack: In a cloud system, all the computational servers work in a specific manner, with an internal communication between them. Whenever a server is overloaded or has reached its threshold limit, it transfers some of its jobs to a nearest and similar service- specific server to get relieve of it. This approach of sharing the burden of services makes the cloud more efficient and faster executing requests. When an adversary or rival has achieved the authorization to make a request to the cloud, then he/she can easily create bogus or fake data and pose these requests to the cloud server.

While processing these requests, the server first checks the authenticity of the requested jobs. Because non-legitimate requests must be checked to determine their authenticity, checking consumes CPU utilization, memory and engages the IaaS to a great extent, so that adversary can be detected. While processing these requests, legitimate services can starve, 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.

IV. DDoS and EDoS attacks

A denial-of-service (DoS) attack is malicious attempt to make a server or a network resource unavailable to users, usually by temporarily interrupting or suspending the services of a host connected to the Internet, the resources may includes the network bandwidth, CPU time, etc. DDoS is simply to flood a network so to denial the authentic user services. To make the network and CPU resources overloaded, attackers tend to use a large number of machines to launch the Distributed DoS(DDoS) attacks. The DDoS attack in a network may not necessarily to disturb the services, but it may contribute to economic loss to the user as well as providers. As the cloud environment is highly scalable, the service will consume more resources during attack to maintain the SLA(service level agreement), which in turn contributes to the revenue loss. Thus the DDoS attack can be converts into an Economic Denial of Sustainability attack (EDoS) in the cloud Environment [12].

- DDoS :DDoS stands for distributed Denial of service, the attack is done with the help of 2 or more machines or system or bots. The attack used is in the form of resistance and usually target high profile web servers such as credit card payment gateways, banks and many other sites.

A very common method for attack is saturating target machine with number of communication request, so it cannot respond to legitimate traffic or may respond slowly as almost unavailable.

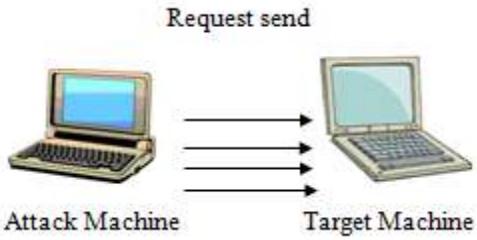

Fig 4. Initial Attack Process

4.1 Working of DDoS attack

DDoSer is the attacker or the controller of the whole attack process. First step of the attacker is to make the handlers, which are basically infected servers. The infected server can be made by launching virus such as Trojan horse or bot(or any other virus)to them. Virus is a small application that allows remote command and control capabilities of computer without user knowledge. These infected servers further help to create zombies/Botnet by making them infected through virus, when ever system communicates through these infected servers. Second step is make the attack to the target by zombies, it perform action when it get the command by the attacker. DDoSer have an access to the command and control, servers can make the zombie available to launch attacks. Zombies are usually performing data flooding to target system.

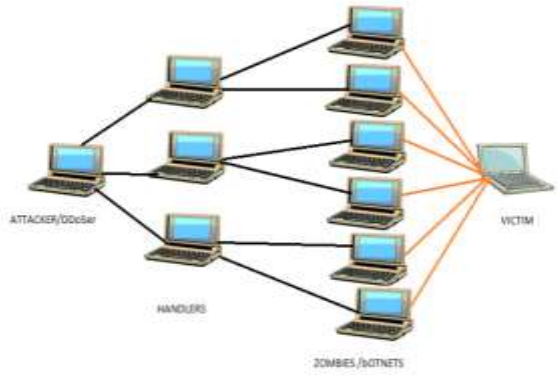

Fig 5. DDos attack by Bots

4.1.1Types of DDoS attacks

A. Smurf

The two main components to the Smurf (DDoS) Denial-of-Service attack are:

- Forged ICMP echo request packets.
- Direction of packets to IP broadcast addresses.

ICMP (The Internet Control Message Protocol) is used to determine whether a machine on the Internet is responding appropriately or has any type of connection problems. ICMP can be used to handle errors and exchange control messages within network. To do this, an ICMP echo request packet is used, which is send to a machine with a return address that the target machine will return an ICMP echo reply packet when receiving the ICMP echo request packet. On IP networks, a packet can be directed to an individual machine or it can be broadcasted to the entire network by using IP broadcast address. In the Smurf attack, attackers are using the ICMP echo request packets intended for IP broadcast addresses from isolated locations to generate DoS attacks. When an attacker sends the ICMP echo request packets, most of the time, they create a forged packet using a spoofed IP address of attacker's intended victim instead of his own IP address in order to hide their identity. The above activity results to when all the machines at the intermediary's network respond to the ICMP echo requests, they all send replies to the victim machine. Although we have not intended to cause a problem on intermediary's network, suffering similar types of traffic outbursts that a victim machine are suffering from can victimize the intermediary [9].

B. TCP SYN Attack

TCP SYN attack is one of the most known notorious and used resource depletion attacks. A SYN flood attack takes place during the "three-way handshake" that symbolizes the beginning of a TCP connection. In the three-way handshake process, a client requests for a new connection by sending a SYN packet to the server. After receiving the request, the server revert a SYN/ACK packet back to the client and put the connection request in a queue. Finally at the third step, the client acknowledges with the SYN/ACK packet. If an attack launched, the attacker sends a plenty of SYN packets to the victim, considering it both to open a lot of TCP connections and to respond to them. After that the attacker does not execute the third step of the three-way handshake that follows, depicting the victim unable to allow any other new incoming connections, because its queue is already full of half-open TCP connections. Mostly the attacker sends a spoofed package to victim, what causes that the SYN/ACK package is send completely to other host, which do not respond because did not sent any SYN packets to the victim [17].

C. UDP flood Attack

This is one of the most popular D-DoS attack methods. The basic idea in the UDP Flood attacks is to exploit UDP services, which are known to reply to packets. The hacker is armed with a list of broadcast addresses, to which sends spoofed UDP packets. These packets are sent to Random and changing ports of the unsuspected target location. However, there are attacks in which the malicious user sends packets to the chargen port. The chargen port is a port, which is used for testing purposes and generates a series of characters for each packet it receives. By connecting a host's chargen service to the echo service on the same or another machine, all affected machines can be effectively taken out of service as an excessively high number of packets are going to be produced. In addition, if two or more hosts are so connected, the intervening network can also become congested and deny service to all hosts whose traffic traverses that network (this attack generally works on NTboxes).It is obvious from the previous analysis that the result from a UDP flood attack is the creation of a nonstop flood of useless data passes between two or more systems. The target host returns ICMP port unreachable messages as a response to each spoofed UDP packets and then slows down because becomes more and more busy processing the

forged IP addresses. This "loop" is responsible for the overload of the network (may crawl to a stop) and the total exhaust of the available bandwidth. Victims of this massive amount of traffic can be also, except networks, individual system, which can lose connectivity to the Internet and in some cases, crash [12].

4.1.2 Solution to the D-DoS attacks:

A. Three-Way Handshake: A simple solution to prevent source spoofing at end systems is to use three-way handshakes at the beginning of an interaction. If a source host spoofs its IP address, it will be unable to finish a three-way handshake. This solution works well to prevent source spoofing at end systems, but attackers are free to spoof the source address of the first packet of a three-way handshake, and they can launch DoS flooding attacks with these packets [9]. It is major drawback of given solution.

B. Ingress /Egress Filtering: Most of DoS and D-DoS attacks use forged or spoofed source IP addresses in order to hide the attacker's originality and also indirectly generate the massive traffic from Intermediary network to target machine. As a result, a machine that the spoofed address is belonging to is also a victim of the DoS attack .A packet leaving to Internet and arriving from Internet must have a source address originating from interior network.

C. E-DoS-Shield - A Two-Steps Mitigation Technique against E-DoS Attacks in Cloud Computing E-DoS-Shield is a mechanism to protect the cloud from the E-DoS attack. This architecture consists of two components they are virtual firewall and the cloud verifier node. The virtual firewall acts as a filter. The VF uses the white list and Blacklist for making decision. The V nodes use the graphic Turing tests such as CAPTCHA to verify legitimate requests at the application.

D. Intrusion Detection System: The Intrusion detection system in a similar way complements the firewall security. The firewall protects an organization from malicious attacks from the Internet and the Intrusion detection system detects the attacker, if someone tries to crack and go through the firewall or manages to break in the firewall security and tries to access on any system in the trusted authorized side. The system alerts the system administrator in case there is a breach in security. Intrusion detection systems are software or hardware systems that automate the process of monitoring the events occurring in a computer system or network, analyzing them for malicious behavior or any policy violations and create reports to a management station. An intrusion detection system (IDS) keeps an eye on the network traffic and monitors for suspicious activity and alerts the system or network administrator if in case there is suspicious activity found.

Intrusion Detection Methods: there are two primary approaches for analyzing events to detect attacks

Signature Based: A signature based IDS keep a regular check on the packets on the network and compares them against a database of signatures or attributes from known malicious threats [3]. This process is similar to the working procedure of most of the antivirus software detects malware or viruses. There is an issue is that there will be a interval between a new threat being discovered in the untamed and the signature for detecting that threat being applied to our IDS. During that interval time IDS would not be able to detect the new threat.

Anomaly Based: In this approach an IDS will examine network traffic and compare it against an established baseline. The baseline will identify that what is normal for that network, what will be sort of bandwidth used, what protocols are going to used, what ports and devices generally need to connect each other and alert the administrator or user whenever traffic is detected which is anomalous, or significantly different from predefined baseline.

V. CONCLUSION

Cloud Computing provides a wide range of services. Existing Security mechanisms are not up to the mark .New approaches are needed which should be a distributed and scalable approach. New form of attacks is possible in the cloud. One such kind of attack is EDoS attack which is a new breed of DDoS attack. The EDoS attack exists only in the cloud so it can be termed as one of the cloud specific attack. A new security EDoS protection frame work is proposed. Also, an experiment is conducted to demonstrate the EDoS attack. The existing approaches are not capable of completely eliminating the EDoS attack. Research is still needed to provide a better mechanism to protect the cloud from EDoS attack

REFERENCES

[1]https://en.wikipedia.org/wiki/Cloud_computing
[2] A. Chaudhary, "A Reliable Solution against Packet Dropping Attack due to Malicious Nodes Using Fuzzy Logic in MANETs," International Conference on Optimization, Reliabilty, and Information Technology (ICROIT), vol. 1, issue 1, IEEE, 2014.
[3]. Cloud kick. [Online]. http://www.cloudkick.com/
[4] A. M. Lonea, D.E. Popescu, H. Tianfield, "Detecting DDoS Attacks in Cloud Computing Environment," International Journal of Computer Communication, ISSN 1841-9836 8(1):70-78, February, 2013.
[5] A. Padmapriya, P. Subhasri, "Cloud Computing: Security Challenges & Encryption Practice," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, issue 3, ISSN: 2277 128X, March 2013.
6] Alzamil, Ibrahim. "Simulation of Cloud Computing Eco-Efficient Data Centre."
[7] Baig, A. Zubair, and F. Binbeshr, "Controlled Virtual Resource Access to Mitigate Economic Denial of Sustainability (EDoS) Attacks against Cloud Infrastructures.," Cloud Computing and Big Data (CloudCom-Asia), International Conference on IEEE, 2013.
[8] D. K. Kumar, "Cloud Computing: An Analysis of Its Challenges & Security Issues," International Journal of Computer Science and Network (IJCSN), vol. 1, issue 5, ISSN 2277-5420, October 2012.
[9] F. Al-Haidari, M. Sqalli, and K. Salah, "Evaluation of the Impact of EDoS Attacks Against Cloud Computing Services, " Arabian Journal for Science and Engineering, pp 1-13, 2014.
[10] F. Al-Haidari, , M. H. Sqalli, and Khaled Salah, "Enhanced edos-shield for mitigating edos attacks

originating from spoofed ip addresses," Trust, Security and Privacy in Computing and Communications (TrustCom), IEEE 11th International Conference on. IEEE, 2012.
[11] H. Sqalli, Mohammed, Fahd Al-Haidari, and S. Khaled. "Edos-shield-a two-steps mitigation technique against edos attacks in cloud computing," Utility and Cloud Computing (UCC), 2011 Fourth IEEE International Conference, IEEE, 2011.
[12] K. Zunnurhain, and S. Vrbsky "Security attacks and solutions in clouds", Proceedings of the 1st international conference on cloud computing, IEEE Conference, pp. 145-156, 2010
[13] L. Yang, Tao Zhang. Jinyu Song, Jinshuang Wang and Ping Chen, "Defence of DDoS attack for cloud computing", In Computer Science and Automation engineering, 2012 IEEE International Conference, vol. 2, pp. 626-629, 2012.
[14] Lo, C-C. Huang, and J. Ku, "A Cooperative Intrusion Detection System Framework for Cloud Computing Networks," In 39th International Conference on Parallel Processing Workshops, pp.280-284, 2010.
[15] M. Patel, A. Meniya, "Prevent DDOS attack using intrusion detection system in cloud," International Journal of Computer Application, issue 3, vol. 2 (April 2013), ISSN: 2250-1797.
[16] N. H. Bhandari, "Survey on DDoS Attacks and its Detection &Defence Approaches," International Journal of Science and Modern Engineering (IJISME) ISSN: 2319-6386, vol.1, issue-3, February 2013
[17] L. Yang, Tao Zhang. Jinyu Song, Jinshuang Wang and Ping Chen, "Defence of DDoS attack for cloud computing", In Computer Science and Automation engineering, 2012 IEEE International Conference, vol. 2, pp. 626-629, 2012.