IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 8, August 2017

Investigation of Intrusion and Denial of Service Attacks in Cloud Computing

Ayman A.A. Ali[1], Prof. Saif Eldin Fattoh Osman[2]

Lecturer, Taif University, Saudi Arabia[1]

Dean, Emirates College for Sciences and Technology, Sudan[2]

Abstract: The most threatening security issues in cloud computing are discussed in this paper. These include cloud intrusion and denial of service attacks. There are numerous intrusion attacks that threaten the cloud. We discuss the main types of them as well as the deployed intrusion detection and prevention techniques. In addition, the denial of service attack that may render the cloud system inoperable are addressed, and the remedy approaches are highlighted.

Keywords: Denial of Service Attacks, Cloud Intrusion, Cloud Computing.

I. INTRODUCTION

We live in cloud computing era that can provide dramatically scalable and virtualized resources, bandwidth, software and hardware on demand to consumers. It is a combination of several key technologies that have evolved and matured over the years. Cloud computing is defined as collections of IT resources (servers, databases, and applications) which are available on an on-demand basis or a pay as you use manner[8], provided by a service company, available through the Internet, and provide resource pooling among multiple users. The national institute of science and technology (NIST) had defined cloud computing as "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 or service provider interaction "[13].Fig. 1 illustrate services provided by cloud. These services are provided over the Internet using known networking protocols, standards and formats under the supervision of different managements. Using cloud computing, consumers can safe cost of hardware deployment, software licenses and system maintenance. Cloud computing is not only attractive to large corporate but also entrepreneurs, startups, medium companies and small companies would benefit greatly as they would have the choice to only rent the necessary computing power, storage space and communication capacity from a large cloud computing provider that has all of these assets connected to the Internet.

Cloud computing is continuously evolving and there are several major cloud computing providers such as Amazon, Google, Microsoft, Yahoo and several others who are providing services such as Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), Storage-as-a-Service and Infrastructure-as-a-Service (IaaS). The SaaS format allows the customer to use cloud service provider's application running on cloud infrastructure via the Internet. In PaaS format, the customers are able to control the applications but do not have any means to manage the underlying infrastructure. The IaaS format allows the customer to deal with computer hardware (network storage, virtual server/machine, data center, processor, and memory) as a service[17]. The applications can be accessed from a client interface such as a web browser or web service. The cloud system owner sells cloud services to consumers. Public Cloud open access to the public where the customer and provider have a strong Service Level Agreement (SLA) to maintain the trust between them. Private cloud is made to a single organization. It can be managed by either the organization or a third party. Community cloud is the cloud infrastructure that is shared by several organizations and supports a specific community. Hybrid cloud is the composition of two or more cloud infrastructures that are bound together[13].

Although, cloud computing has a potential for cost savings to the corporate and allows clients to access their applications and data from anywhere at any time[19], the security risks are also enormous[10]. As more and more information of individuals and companies are placed in the cloud data centers, the questions arise regarding to the safety and security of cloud environment. Cloud Computing can be easily targeted by attackers. Unfortunately, as the connectivity for clod computing is carried out via the Internet, it is the next frontier for viruses, worms, hackers and cyber-terrorists to start probing and attacking. With cloud computing, physical location of data is spread across geographic area that could span over continents, countries or regions. There have been instances where a complete blackout of entire cloud services could happen and make it unavailable for hours and even days due to bugs and hostile behavior of attackers. The lost of business could be catastrophic when a corporate that completely depends on a cloud computing service provider whose system had been disrupted for hours or days.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 8, August 2017

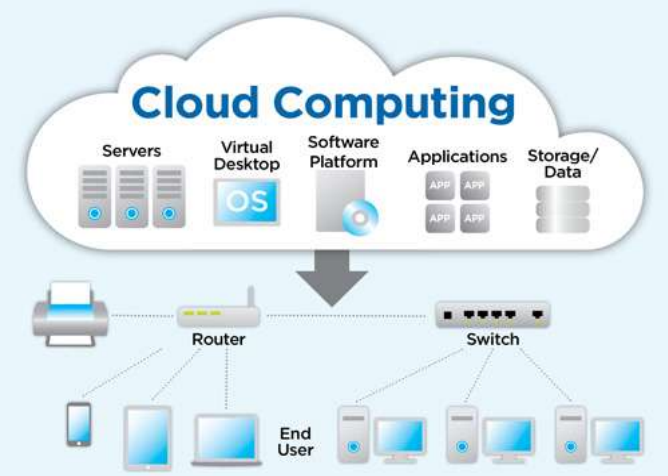

Fig. 1: services provided by cloud computing

Cloud computing faces just as much security threats that are currently found in the existing computing platforms, networks, intranets, internets in corporate. These may include abuse and nefarious use of cloud computing, insecure application programming interfaces, malicious insiders, shared technology vulnerabilities, data loss/leakage, account, service and traffic hijacking, as well as unknown risk profile. In addition, cloud presents the corporate with a number of risks that include securing critical information like the protection of intellectual property, trade secrets, personally identifiable information that could fall into the wrong hands. Furthermore, cloud computing is just as vulnerable as any other technology that uses the public Internet for connectivity. The vulnerability includes eavesdropping, hacking, cracking, malicious attacks and outages[17].
In this paper, we will elaborate on the most serious security issues of cloud security; namely, cloud intrusion and denial of service attacks. These two threats represent the hot spot research areas on the cloud computing arena.

II. CLOUD INTRUSIONS

The major security concern after data security is intrusion detection and prevention in cloud infrastructures. As cloud infrastructure runs through standard Internet protocols, intruders may be attracted to it due to many inherent vulnerabilities involved in the Internet. The intrusions may affect availability, confidentiality and integrity of cloud resources and services through many types of attacks. Efficient intrusion detection systems (IDS) and intrusion prevention systems (IPS) should be incorporated in cloud infrastructure to mitigate these attacks. There are many intrusion attacks that threaten the system. Among these, we can find the following:

- **Insider attack**; where authorized cloud users may attempt to gain and misuse unauthorized privileges.Then, he may commit frauds and disclose information to others; a process that leas to breaking the confidentiality of the information.
- **Flooding attack**; where attacker tries to flood victimby sending huge number of packets from innocent zombie host in the network. This may cause Denial of Service attack that affects the service's availability to authorized user.
- **User to root attack;** where an attacker gets an access to legitimate user's account by sniffing password. This allows him/her able to exploit vulnerabilities for gaining root level access to the system.
- **Port scanning attack;** where attackers can find open ports through port scanning and attack on services running on these ports.
- **Virtual machine and hypervisor attack;** where attacker can gain control over installed virtual machines by compromising the lower layer hypervisor, and compromise installed-hypervisor to gain control over the host.
- **Backdoor channel attack;** where hacker can control victim's, resources using backdoor channels and make it as zombie to attempt Distributed Denial of Service (DDoS) attack. It can also be used to disclose the confidential data of victim.

Those attacks can affect cloud because everyone can access it through Internet, and this may cause Denial of Service (DoS) or Distributed Denial of Service (DDoS) via using of zombies hosts. In this case, cloud can't differentiate between normal usage and fake usage. On the other hand, attacker acquires access to valid user's instances that enables him for gaining root level access to VMs or host or by discovering open ports or throw backdoor channels.
An Intrusion Detection System (IDS) is a software that automates the intrusion detection process and detects possible intrusions [11]. An Intrusion Detection and Prevention System (IDPS) is a software or hardware device that has all the

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 8, August 2017

capabilities of an intrusion detection system and can attempt to stop possible incidents. There is multiple intrusion detection and prevention systems IDS/IPS, the system depends on the technique being used to detect and prevent intruders from abusing cloud resources. Traditional IDS use many techniques such as:

- S**ignature-based detection**: it's used to detect known attacks and fail to detect unknownattacks in cloud computing. It is performed by comparing the known information with the database of signatures.
- **Anomaly-based detection**: it detects attack anomalous in the behavior. It compares current user activities against previously loaded logs of users. It can detect unknown attacks indeferent levels in cloud but it's difficult to detect attacker because cloud using large numbers of events. In addition, it produces a large number of false alarms because of irregular network and user behavior.
- N**etwork level or system level**: which makes monitoring for cloud very difficult.
- **Artificial neural network**: It can generate data from incomplete data to differentiate between normal or intrusive data. It is efficient to unstructured data in network.
- **Fuzzy logic based IDS**: It uses mix of supervised and unsupervised learning.
- **Association rule based**: Association rules can be used to generate new signatures. Using newly generated signatures, variations of known attacks can be detected in real time, (Support vector machine (SVM) based) if limited sample data are given for detecting intrusions, then use of SVM is an efficient solution; since dimensions of data are not affecting accuracy of SVM based IDS.
- **Genetic algorithm (GA) based**: The selection of optimal parameters (network features) forintrusion detection will increase the accuracy of underlying IDS. For that, Genetic algorithm(GA) based IDS can be used in cloud.
- **Hybrid techniques**: that usesa combination of two or more of the above techniques.

III. DENIAL OF SERVICE ATTACKS IN CLOUD

The security is a very big concern to deploy cloud services over Internet. Because of the distributednature of the Internet, the confidentiality, integrity and availability must be taken seriously.One of the top security problems is the Denial of Service (DoS) and distributed denial of service(DDoS) attacks [6]. It affects the availability of cloud services. In this attack, the attacker mustcompare and test many hosts, and select the weakest hosts known as zombie computers illustrated in Fig. 2 to usethem to start his attack [7]. The main objective of the DoS attack is to make services unavailable to itsusers by targeting web servers, CPU, storage, and the other network resources this objective finished by flooding target by superfluous packets to overload targeted system to make it unavailable[1].Distributed denial of service attack aims to overload targeted system by flooding it using many sources, that's make it very hard to stop the attack by block single IP source.The virtualizationand multi-tenant infrastructure used in cloud computing make it an easy target for attackers.Attacker can deploy his denial of service using different attack tools for example (Stacheldraht, LOIC,ReDoS)[1].

Fig. 2: using of Zombies in DoS attack

IV. DENIAL OF SERVICE DETECTION

In this section, we try to focus on denial of service (DoS) detection techniques used in cloud computing.
In [9], authors focus on threats in service as a pointer to DoS attack. They compared between different kind of monitoring frameworks in terms of high cost, and provide special techniques to locate best monitoring framework according to the network requirements. In [3], authors provide a signature-based DDoS detection in cloud computing. They used Snort as IDS sensor, a signature based technique, that is deployed on the virtual interface to analyze both in bound and out-bound traffic in real time in order to counter DDoS attacks. The module is implemented in network/transport layer to counter DDoS attacks, by knowing the IP addresses used to attack and generating an access control list to drop the entire packets from the blacklisted IP addresses. If the generated attacks are from zombie machines, the module can be configured to block such traffic and transfer the targeted application to a VM hosted in

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 8, August 2017

another datacenter. Another strategy was proposed in[21], where a detection approach to trace and identify the source of Distributed DoS attacksin cloud. A filter called Cloud-filterwas offered. In the proposed architecture, firstly all requests go toproposed approach to check, if the request packet identified as normal, services are provided to user.
HX-DoS (combination of HTTP and XML messages that are internationally sent to flood and destroy thecommunication channel of the cloud service provider) is a new type of violation that attacks cloudproviders. A role set based detectionwas proposed in[2] to detect HX-DoS attacks. Rebuild andDrop methods were used to choose which of the influenced packet to be dropped. A VM based IDS was proposed in [12], The authors configured MySQL database for storing alerts received fromVM based IDS to convert it into Basic Probabilities Assignments. They used Barnyard tool to detectattacks, and signature based snort with DDoS rules to prevent known attacks. The detected attackpackets stored in binary unified file and transmitted using a secured channel to a centralized MySQLdatabase at the front-end. Stacheldraht is a DDoS attack tool that generates infrastructure resourcesdepletion attack with ICMP flooding, UDP flooding and TCPSYN. It can be used to simulate attack. The system resulting high detection rate with low false positive, but can't detect unknown attacks. In [20], a technique based on Gaussian model to prevent DDoS attacks on cloud applicationlayerwas provided, which use malicious XML content in a Simple Object Access Protocol (SOAP). Normal profilemodel is founded from the dataset during the initialization before activating the proxy to listen torequests. Firstly, in detection, HTTP header inspection will be carried out to prevent HTTP flooding. Italso assures SOAP action check and size outlier. Then the XML content is processed before checking ifRSOAP Action is spoofed. This model can't detect request from new DDoS techniques, without addingadditional features.The authors in [15] used Cloud confidence DDoS statistical-based Filtering, that use two levels of filtering. Itremoves the header of incoming packet, and compares the TTL value with the stored value in the IP tohop-count (IP2HC) table. The packet will be dropped and categorized as spoofed if their TTL value is notequal the stored value in (IP2HC). The second level is based on the Jensen–Shannon divergenceconcept, which uses a stored normal profile stored in a database to compare incoming packet headerinformation. It's useful in checkingthe information divergence. In [5], a map reduce model (parallel processing model that has been used to expedite batch joboperations) was provided to mitigate application layer HTTP GET DDoS attacks based on data mining. The proposedframework consists of three parts:packet and log collection module that analyses packet transmission and web server logs, pattern analysis module that creates the attack pattern for DDoS detection through analyzing CPU usage, packetsize, load, and information distribution of the packet header, and detection module that uses the normal behavioral pattern to detect DDoS attacks. The map reduce algorithm is used to measure the rates between pattern rule and detection time of the proposed system to external signatures to evaluate the system. The result shows that the proposedmodel can identify new attack profile in a short processing time than Snort. In [4], the authors proposed a network monitoring and threat detection system to secure infrastructure incloud computing. Their system consists of three components, monitoring agents, cloud infrastructureand operation center. In order to increase the speed of data processing, a Hadoop Map Reduce andSpark was used.
A framework based on using artificial bee colony (ABC) swarm approach was proposed in [16],The authors generated the background traffic in CloudSim for testing. The proposed framework is divided into threesteps. In the first step, the basic network features are generated and traffic is recorded in a well-defined manner. In the second step, an ABC algorithm was employed and the working behavior of ABC was determined. A decision making, then,was done using anomaly-based detection technique. The proposed approach can detect most of the attacks in a very short period of time. In [14], the authors used quantum algorithm approach to find the shortest path to overcome the situationwhen DoS attacks between the transmission of any packet sending from source to destination. The authorstested their system using two PCs connected through the same router; one of them act as victim and the otherone is the attacker. Hyenae tool is used to generate a DoS attack, and AthTekNetWalk network tool isused to monitor and capture the network traffic. The traffic sample-by-sample inthe network was analyzed by using quantum algorithm approach. The achieved results were around 90% and 93%,for QEA and QSE respectively.[18] Author provide a framework that is working by monitoring the flow of SYN packets using acorrelation engine and a flow traffic tool like snort, wireshark. The attack is firstly detected by monitoringnetwork flow using snort, wireshark. Then a correlation engine is used to compare the flow of SYNpackets to decide normal and abnormal case. By comparing these flows of SYN packets, the correlationengine confirms and detects that there is a flooding attack going on a virtual machine and bringsnotice to the hypervisor. After detecting attacker IP address, all attacker IP address should be blockedto deal with. Honeypot network is employed where it pings all the IP address used by an attackerand whenever there is a replay, all responded IP address is blocked. This framework doesn'timplement to different cloud environment.

V. CONCLUSION

Security problem is the main issue that restricts the wide deployment of cloud computing. Accordingly, some of the most threatening security vulnerabilities were discussed in this paper.A number of intrusion attacks that threaten the security of cloud computing were addressed, as well as the effective intrusion detection and prevention techniques.

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 8, August 2017

Furthermore, the denial of service attack that affects the availability of cloud system are investigated in order to examine the appropriate remedy technique. The research in cloud computing security is a hotspot field that may lead sooner or later to a secure cloud computing technology.

REFERENCES

[1] Denial-of-service attack, pp. https://en.wikipedia.org/wiki/Denial-of-service_attack.
[2] E. ANITHA and S. MALLIGA, A packet marking approach to protect cloud environment against DDoS attacks, Information Communication and Embedded Systems (ICICES), 2013 International Conference on, IEEE, 2013, pp. 367-370.
[3] A. BAKSHI and Y. B. DUJODWALA, Securing cloud from ddos attacks using intrusion detection system in virtual machine, Communication Software and Networks, 2010. ICCSN'10. Second International Conference on, IEEE, 2010, pp. 260-264.
[4] Z. CHEN, G. XU, V. MAHALINGAM, L. GE, J. NGUYEN, W. YU and C. LU, A cloud computing based network monitoring and threat detection system for critical infrastructures, Big Data Research, 3 (2016), pp. 10-23.
[5] J. CHOI, C. CHOI, B. KO and P. KIM, A method of DDoS attack detection using HTTP packet pattern and rule engine in cloud computing environment, Soft Computing, 18 (2014), pp. 1697-1703.
[6] CLOUDSECURITYALLIANCE, The Notorious Nine, Cloud Computing Top Threats in 2013, (2013), pp. https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf.
[7] R. V. DESHMUKH and K. K. DEVADKAR, Understanding DDoS attack & its effect in cloud environment, Procedia Computer Science, 49 (2015), pp. 202-210.
[8] P. DESHPANDE, S. C. SHARMA and P. S. KUMAR, Security threats in cloud computing, International Conference on Computing, Communication & Automation, 2015, pp. 632-636.
[9] A. HABIB, M. HEFEEDA and B. K. BHARGAVA, Detecting Service Violations and DoS Attacks, NDSS, 2003.
[10] K. HWANG, S. KULKARENI and Y. HU, Cloud security with virtualized defense and reputation-based trust mangement, Dependable, Autonomic and Secure Computing, 2009. DASC'09. Eighth IEEE International Conference on, IEEE, 2009, pp. 717-722.
[11] K. LABIB, Computer security and intrusion detection, Crossroads, 11 (2004), pp. 2-2.
[12] A. M. LONEA, D. E. POPESCU and H. TIANFIELD, Detecting DDoS attacks in cloud computing environment, International Journal of Computers Communications & Control, 8 (2013), pp. 70-78.
[13] P. MELL and T. GRANCE, The NIST definition of cloud computing, (2011).
[14] P. R. K. REDDY and S. BOUZEFRANE, Analysis and detection of dos attacks in cloud computing by using qse algorithm, High Performance Computing and Communications, 2014 IEEE 6th Intl Symp on Cyberspace Safety and Security, 2014 IEEE 11th Intl Conf on Embedded Software and Syst (HPCC, CSS, ICESS), 2014 IEEE Intl Conf on, IEEE, 2014, pp. 1089-1096.
[15] P. SHAMSOLMOALI and M. ZAREAPOOR, Statistical-based filtering system against DDOS attacks in cloud computing, Advances in Computing, Communications and Informatics (ICACCI, 2014 International Conference on, IEEE, 2014, pp. 1234-1239.
[16] S. SHARMA, A. GUPTA and S. AGRAWAL, An Intrusion Detection System for Detecting Denial-of-Service Attack in Cloud Using Artificial Bee Colony, Proceedings of the International Congress on Information and Communication Technology, Springer, 2016, pp. 137-145.
[17] S. SINGH, Y.-S. JEONG and J. H. PARK, A survey on cloud computing security: Issues, threats, and solutions, Journal of Network and Computer Applications, 75 (2016), pp. 200-222.
[18] R. UDENDHRAN, New Framework to Detect and Prevent Denial of Service Attack in Cloud Computing Environment, Asian Journal of Computer Science and Information Technology, 4 (2014), pp. 87-91.
[19] L. M. VAQUERO, L. RODERO-MERINO, J. CACERES and M. LINDNER, A break in the clouds: towards a cloud definition, ACM SIGCOMM Computer Communication Review, 39 (2008), pp. 50-55.
[20] T. VISSERS, T. S. SOMASUNDARAM, L. PIETERS, K. GOVINDARAJAN and P. HELLINCKX, DDoS defense system for web services in a cloud environment, Future Generation Computer Systems, 37 (2014), pp. 37-45.
[21] L. YANG, T. ZHANG, J. SONG, J. S. WANG and P. CHEN, Defense of DDoS attack for cloud computing, Computer Science and Automation Engineering (CSAE), 2012 IEEE International Conference on, IEEE, 2012, pp. 626-629.