Available online at www.ijrp.org

IJRP.ORG
International Journal of Research Publications

International Journal of Research Publications

Study on DOS attack on Cloud Environment with reference to Attacks on Web Environment

"Vidyarthini.A 1, Balaji.S 2" *

[1]Research scholar,
PG & Research Dept of Computer science,D.B.Jain (Autonomous)
[2] Faculty
PG & Research Dept of Computer science,D.B.Jain (Autonomous)

Abstract

Cloud computing is considered to be the computing paradigm that offers numerous flexible and consistent services using virtualization technology that is used in the next generation of the data centers. Cloud computing by means of its capacity, resilience and cost minimization that provides the capability to share resources in a pervasive and transparent way, also it has the ability to perform procedures that meet different needs. The increasing use of cloud services poses threat to security of data and system infrastructure. Security attacks as a result of loss of availability of cloud services can have more significant impact. A critical review of one of those attack Denial of service, their impact and the mechanism to defend is the scope this work.

"Keywords: Cloud computing; Virtualization; Security; Denial of service."

* Corresponding author. Tel.: 9514783830;
E-mail address: vidyarthini.a@gmail.com

1.Introduction

Cloud computing by means of its capacity, resilience and cost minimization that provides the capability to share resources in a pervasive and transparent way, also it has the ability to perform procedures that meet different needs. Moreover, cloud computing offers on-demand services to the users and can have the ability to access common infrastructure [1]. (NIST) which is the National Institute of Standards and Technology, identifies five fundamental specifications of cloud computing as on-demand self-service, broad network, access resource pooling, measured service, and rapid elasticity [2]. It also defines that the cloud offers services in four different deployment models (hybrid and community, private, public). It states that cloud providers provide the services in three service models namely infrastructure as a service (IaaS), platforms as a service (PaaS), and Software as a service (SaaS), and it is on the period of development to provide everything as a service (XaaS) [3].

High availability in cloud computing is essential. The availability in the cloud requires the use of cloud resources and services by authoritative users, based on their demands [5]. However, threats related to data confidentiality and service availability can threaten the cloud environment due to its resource multitenancy and sharing features [4]. The impacts of the non-availability of services and resources in the cloud are calamitous; and this can lead to a partial or even total failure of delivering the required service [5]. The biggest attacks in 2013, 2014, 2015 and 2016 were 300, 400, 500 and 600 Gbit/sec respectively [8]. It believes that a whale of such a DDoS attack can swallow 10 percent of a country's overall Internet traffic. These large DDoS attacks consider being exceptional cases, but even the number of smaller attacks is also rising, which increase and concentrate the threat to businesses.

2.Background work

Now a day countless economic impacts and losses to the victim party are caused by one of the most common cyber-attack methods which are Denial of service (DoS) attack. In network and computer security, generally the expression denial of service is used to indicate to an attack intended to damage or saturate the computer resources or network resources, with intent of making the legitimate users no longer be able to use the provided services [6, 8]. Such an attack is typically achieved by overwhelming the targeted resource or machine with extra and unnecessary requests in an attempt to prevent all or some legitimate requests from being fulfilled which will lead to system overloading [8, 9]. Sometimes when we try to get access to a website, we see that the server hosting this website is inaccessible due to overload and we notice an error message. This happens when the number of requests processed by a server surpasses its maximum capacity.

The most popular method of DoS attack is named as DDoS the Distributed DoS which is officially known as a coordinated attack because it has the ability to cause more serious effects rapidly and easily. DDoS attack will cause extremely large effect on availability in Cloud computing services which can lead to violation of the agreement between the client and the cloud service provider which is called Service Level Agreement (SLA) [10, 17]. Now using the innovative "DDoS as a Service" tools is making it easier for attackers to launch these effective and developed attacks.

3. DDoS Attacks On Web Services

Web service as a definition is a standardized way of communicating between two devices connected with each other by a network. It also utilizes a standardized Extensible Markup Language (XML) to encode all the messages and communications that may occur between the connected devices for a purpose of exchanging data. For example, Simple Object Access Protocol is actually an XML based protocol (SOAP) used for data exchanging purposes. Generally, there are many DoS attacks that conducted against web services and in this part, we briefly define the popular DoS attacks that performed against web services which are as the following:

- **Attack of Coercive parsing:** This kind of attack consider being one of the simplest attacks where the attackers try to attack the web service to exhaust its system resources [21]. They only send a SOAP message and they include in the SOAP body huge number of opening tags. It means that, a very extremely nested XML document is directed by the attacker towards the attacked web server or service. In this attack, this may lead to a high CPU usage in addition to causing error in the memory when the parser trying to process this malicious XML document [21].
- **The Attack of XML attribute count:** This type of attack is similar to Coercive parsing attack where the body of SOAP message includes huge number of attributes that will be directed to the server.
- **The attack of XML element count:** In this attack, several non-nested elements will be included in the body of SOAP messages that will be sent the server [21].
- **Hash collision attack (Hash DoS):** By forwarding one huge POST message that is fully loaded with several types of variables. Then, to process this huge message, the sever needs to use some hashing mechanisms to handle this message [23]. As a result, this operation consumes the processing power of the server and it could take an hour for the server to finish processing this single request. That is what is called a hash denial-of-service (DoS) attack.

- **The attack of XML external entity:** It imposes the server to analyse and parse a very big external entity document that is well-defined in a set of markup declaration called Document Type Definition (DTD) [24].
- **XML entity expansion:** This kind of attack is also called "XML bombing". This attack performed by exploiting one of the XML's capabilities which is called an XML nesting capability [25].
- **Oversized cryptography:** In this attack a big amount of the numerically signed or encoded parts of SOAP message is attached in the message by the attackers [26].
- **Web Services Description Language (WSDL) scanning:** WSDL defined as a document that has an XML format and used to characterizing the services of the network. It is also used to determine the parameters used for linking specific methods. So, the information provided by this document contains critical information, which gives a big chance to the attackers to perform other attacks [27].
- **Metadata spoofing:** in this attack, the attackers have the ability to be aimed to redesign the metadata description of the web service [28].
- **Attack obfuscation:** The attackers have the ability to utilize the encryption of an XML document to hide the content of the message from being message content from being detected by the IDS or the firewall. These encoded XML document can be utilized to perform other kinds of attacks like coercive parsing attack, XML injection attack, or oversize payload attack [29]. The attack of Business Process Execution Language (BPEL) state deviation: BPEL engine have the ability to supply the web service with the endpoints, which can accept every probable incoming request message. A single process of BPEL engine may have several instances working simultaneously. Due to the fact that these endpoints that used for communications are available for any connections arriving at whatever time. Therefore, a malicious Web Service attacker might attack these unlocked endpoints. So, the attackers have the ability to send a huge amount of messages that are not associated with any current process instances [30]. Consequently, by processing such an invalid messages sent by the attackers, the resources that are related to the computational process of the BPEL engine will be overloaded.
- **Instantiation flooding attack:** In this attack, a new instance of the BPEL procedure will be formed for each time a new message or request arrives. Then, the instructions that are existed in the description document of the process will be executed. Thus, the attackers have the ability to attack the BPEL engine through transferring a huge amount of requests messages to the process of BPEL [30].

- **Indirect flooding:** The concept of this attack is to utilize the BPEL engine in-between as an intermediary for an attack on a system targeted backwards the BPEL engine. Think of a process of BPEL that continually invokes a Web Service provided by the system that the attackers intend to attack. By saturating the BPEL engine's process with contaminated messages by the attackers, the BPEL engine will suffer from a massive workload itself. And at the same time, this simply will lead to similarly weighty workload on the side of the system targeted by the attackers. Consequently, if the system targeted indirectly by the attackers is not as strong and robust as the BPEL engine, it will result in a Denial-of-Service of the targeted system [31].
- **Web Service (WS)-addressing spoofing:** The attackers in this kind of attack send the requests of SOAP messages to the targeted server. These messages contain the header of WS-addressing. Thus, in this case, the server distributes the response of SOAP for a various endpoints that can be utilized to overflow another web service [32].
- **The attack of Middleware hijacking:** This kind of attack is similar to attack of WS-addressing spoofing, except that it directs the endpoint URL of the attackers to a system that is already exist. Then, at the specified URL a real service will be run by the attackers. Thus, the server of the web service will continually try to response to the requests that had been sent by the attackers [21].
- **XML-based denial-of-service attacks:** This attack indicates that the saturating XML messages will be sent by the attackers to the web service in order to saturate all the resources of the server side. In other words, the DX DoS attack consider to be the distributed form of the X DoS attack, that utilizes several hosts to perform the attack [33]. Often, in this kind of attack, the content of the message is contaminated to crash and saturate the web server. Due to the parsing process of these messages and since the design of XML documents is complex, even a small distorted message of XML can waste a huge number of server resources [24].
- **The attacks of HX-DoS:** Generally, the web services on the cloud work using XML and HTTP protocols for example SOAP. One of the serious attacks targeting the service provider of the cloud is the HX-DoS attack. This attack performs using two protocols the HTTP and the XML protocol [34]. HX-DoS attack is utilized to saturate the channel of communication of the cloud providers by using messages that are composed of both HTTP and XML messages. In fact, the illegal messages composed by the attackers should be differentiate in order to identify the issue of HXDoS attacks against the web services cloud providers [35].

4. Conclusion

Cisco predicts that by 2020, a much more developed 17 million DDoS attacks annually will happen. According to the huge increasing volume of DDoS attacks and the growth trends being noticed, Cisco believes that DDoS attacks are the greatest serious cyber security attacks toward all the organizations all over the world. With the advent of quantum computing opportunities that provides millions of times more CPU of a single core computation speed, DDoS attack will become more widespread and effective.

5.References

[1]. H. Nemati, Information Security and Ethics: Concepts,Methodologies, Tools, and Applications, New York:IGI Global, 2008, Ch.1.1.

[2]. P. Mell and T. Grance. "The NIST Definition of Cloud Computing". National Institute of Standards and Technology (NIST) Special Publication. Gaithersburg, MD. https://csrc.nist.gov/publications/detail/sp/800-145/final, 2011.

[3]. Z. Chiba, N.Abghour, K. Moussaid, and M. Rida, " A Survey of Intrusion Detection Systems for Cloud Computing Environment", International Conference on Engineering & MIS (ICEMIS) 2016; 1-13.

[4]. U. Oktay and O. K. Sahingoz, "Attack Types and Intrusion Detection Systems in Cloud Computing," 6th *International Information Security & Cryptology Conference*, vol. 9, pp. 71–76, 2013.

[5]. J. Varia, "Best practices in architecting cloud applications in the AWS cloud", Cloud Computing. Principles and Paradigms, John Wiley & Sons, Inc. Jan 2011, pp. 459-490

[6]. K. C. Okafor, J. A. Okoye, and G. Ononiwu,"Vulnerability Bandwidth Depletion Attack on Distributed Cloud Computing Network: A QoS Perspective," International Journal of Computer Applications, vol. 138, no. 7, pp. 18–30, 2016.

[7]. G. Somani, M. Singh, D. Sanghi, M. Conti, and R.Buyya, "DDoS attacks in cloud computing: Issues, taxonomy, and future directions," Computer.Communications., vol. 107, pp. 30–48, 2017.

[8]. H. Kaur and S. Behal, "Characterization and Comparison of Distributed Denial of Service Attack Tools," International Conference on Green Computing and Internet of Things (ICGCIoT), pp. 1139–1145, 2015.

[9]. M. J. Hashmi, M. Saxena, and R. Saini, "Classification of DDoS Attacks and their Defense Techniques using Intrusion Prevention System", International Journal of Computer Science & Communication Networks, vol. 2, no. 5, pp. 607–614.

[10]. A. Khadke and M. Madankar, "Review on Mitigation of Distributed Denial of Service (DDoS) Attacks in Cloud Computing.", 10th International Conference on Intelligent Systems and Control (ISCO), pp. 1-5, 2016.

[11]. K. N. Mallikarjunan, K. Muthupriya and S. M. Shalinie, "A survey of distributed denial of service attack," 10th International Conference on Intelligent Systems and Control (ISCO), Coimbatore, pp. 1-6, 2016.

[12]. B. Prabadevi, "Distributed Denial of service Attacks and its effects on Cloud Environment- a Survey", Networks, Computers and Communications, The 2014 International Symposium, 2014.

[13]. O. Achbarou, M. Ahmed, and S. El Bouanani, "Securing Cloud Computing from Different Attacks Using Intrusion Detection Systems", International Journal of Interactive Multimedia and Artificial Intelligence, pp. 61–64, 2017.

[14]. R. M. Jabir, S. Ismail, R. Khanji, L. A. Ahmad, O. Alfandi, and H. Said, "Analysis of Cloud ComputingAttacks and Countermeasures," Advanced Communication Technology (ICACT), 2016 18th International Conference, pp. 117–123, 2016.

[15]. S. Singh, "Cloud computing attacks: a discussion with solutions". Open Journal of Mobile Computing and Cloud Computing, 2014.

[16]. G. Somani, M. Singh, D. Sanghi, M. Conti, and R.Buyya, "DDoS attacks in cloud computing: Issues, taxonomy, and future directions," Computer.Communications., vol. 107, pp. 30–48, 2017.

[17]. H. Kaur and S. Behal, "Characterization and Comparison of Distributed Denial of Service Attack Tools," International Conference on Green Computing and Internet of Things (ICGCIoT), pp. 1139–1145,2015.

[17]. M. Masdari, F. Salehi, M. Jalali, and M. Bidaki, "A Survey of PSO-Based Scheduling Algorithms in Cloud Computing". Journal of Network and Systems Management, 1–37, 2016.

[18]. M. Masdari et al. "Towards workflow scheduling in cloud computing: a comprehensive analysis". Journal of Network and Computer Applications, 66: 64–82,2016.

[19]. T. Siva, E. S. P. Krishna, "Controlling various networkbased ADoS attacks in cloud computing environment: by using port hopping technique". International Journal of Engineering Trends and Technology (IJETT), 4(5); 2099–2104, 2013.

[20]. F. Palmieri, S. Ricciardi, U. Fiore, M. Ficco, A. Castiglione, "Energy-oriented denial of service attacks: an emerging menace for large cloud infrastructures". The Journal of Supercomputing, 71(5): 1620–1641, 2015.

[21]. M. Jensen, N. Gruschka, R. Herkenhöner, "A survey of attacks on web services". Computer Science-Research and Development, 24(4): 185–197, 2009.

[22]. A. Falkenberg, C. Mainka, J. Somorovsky, and J. Schwenk, "A new approach towards DoS penetration testing on web services". In Web Services (ICWS), 2013 IEEE 20th International Conference on. IEEE, 491– 498, 2013.

[23]. D. Holmes, "Mitigating DDoS attacks with F5 technology". F5 Networks, Inc, 2099–2104, 2013.

[24]. P. Siriwardena, "Security by Design in Advanced APISecurity". Springer, 11–31, 2014.

[25]. I. Siddavatam, J. Gadge, "Comprehensive test mechanism to detect attack on web services". In Networks, 2008. ICON 2008. 16th IEEE International Conference on. IEEE, 2008.

[26]. S. Tiwari, P. Singh, "Survey of potential attacks on webservices and web service compositions". In Electronics Computer Technology (ICECT), 2011 3rd International Conference on. IEEE, 2011.

[27]. P. Lindstrom, Attacking and defending web services. Whitepaper ,https://www.cse.iitb.ac.in/~madhumita/seminar/web%20services/Attacking%20and%20Defending%20Web%20Services.pdf,2004.

[28]. M. Younis, K. Kifayat, "Secure cloud computing for critical infrastructure: a survey". Liverpool John Moores University, United Kingdom, Tech. Rep, 2013.

[29]. A. Masood, "Cyber security for service oriented architectures in a Web 2.0 world: an overview of SOA vulnerabilities in financial services". In Technologies for Homeland Security, 2013.

[30]. A. N. Gupta, D. P. S. Thilagam, "Attacks on web services need to secure XML on web". Computer Science & Engineering, 3(5): 1, 2013.

[31]. M. Jensen, N. Gruschka, N. Luttenberger, "The impact of flooding attacks on network-based services". *In* Availability, Reliability and Security, 2008. ARES 08.Third International Conference on. IEEE, 2008.

[32]. C. Mainka, J. Somorovsky, J. Schwenk, "Penetration testing tool for web services security". In Services (SERVICES), 2012 IEEE Eighth World Congress on. IEEE, 2012.

[33]. A. Chonka, Y. Xiang, W. Zhou, A. Bonti, "Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks". Journal of Network and Computer Applications 2011, 34(4):1097–1107, 2011.

[34]. S. Farahmandian, M. Zamani, A. Akbarabadi, Y. Moghimi, S. M. Mirhosseini Zadeh, S. A.Farahmandian, "survey on methods to defend against DDoS attack in cloud computing". System 2013, 6(22): 26, 2013.

[35]. E, Anitha, S. Malliga, "A packet marking approach to protect cloud environment against DDoS attacks". In Information Communication and Embedded Systems (ICICES), 2013 International Conference on. IEEE,2013.