CURRENT RESEARCH IN
COMPUTER SCIENCE
ISSN 2788-7707
MAY. 2021 VOL. 1, NO. 1

A Method of EDoS Attack Defense in Cloud Computing Environment

Shibwabo Ganiyu
Department of Computer Science, Kwara State Polytechnic, Ilorin, Nigeria

ABSTRACT

Cloud computing offers several benefits to the organization by reducing both capital and operational expenditures CapEx and OpEx. The full adoption of Cloud networks makes it attractive for cyber-criminals to perform illicit acts. The EDoS attack poses the risk of rendering the Cloud environment financially unsustainable for Cloud users. This paper proposes a fourstep lightweight approach of EDoS attack defense in the Cloud computing environment by placing a Fog server that checks the blacklist of IP addresses and each packet's bandwidth threshold at arrival. The research demonstrates how the Fog server adds security enhancement to the Cloud networks.

KEYWORDS

EDoS; Fog Network computing; Cloud computing; Fog computing; DDoS.

1. Introduction

Cloud computing offers several benefits to organizations by reducing their capital and operational expenditures CapEx and OpEx. Among the distinct characteristics also offered range, from measure service, rapid elasticity, resource provisioning, broad access networks, and on-demand self-service (Chandrasekaran, 2015). The rapid elasticity and measured service allow the Cloud users to auto-scale upward, and downward computing resources as-and-when need without the Cloud users involvement. Computing services consumed by the Cloud users are charged based on usage over the network, typically the internet; these make the network environment vulnerable to cyber-crimes (Osanaiye, 2015). Consequently, the Economic Denial of Sustainability EDoS attack that is a flavor of the Denial of Service (DoS) attack, is becoming prominent among Cloud users. The EDoS attack takes advantage of Cloud users vulnerability (i.e., software, protocol, IP addresses) to install malicious codes called "malware" that makes the victims captive and act like "Zombie or handler" which helps the attacker perform illicit acts. The attackers' technique is to send illegal packets to the Cloud servers until the Cloud users subscription becomes exhausted and unable to access the network resources due to large-scale service withdrawal or bankruptcy (VivinSandar et al., 2012). The attackers are usually motivated by different forms of incentives, i.e., revenge, ideological belief, financial, and economic gains, cyber-warfare, and intellectual contest (Mirkovic et al., 2004).

2. Literature Review

The DoS is an attacker's intentional attempt to make network resources (i.e., server, memory, network bandwidth, compute) inaccessible or degraded for legitimate Cloud users by sending unsolicited packets, or information to the victim that trigger crash of resources (Mirkovic et al., 2004). The attackers use two methods to carry out this act: Flood or crash method. The Flood attacks occur when the server buffer can no longer process packets due to excessive unsolicited messages leading to services availability or degradation. The crash method exploits vulnerabilities within the system to shut down the target system or services.

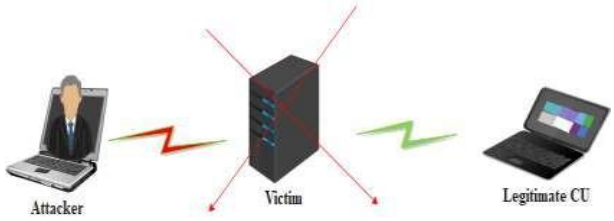

Figure 1. DoS attack DISTRIBUTED DoS (DDoS) attacks

The DDoS is an evolutionary version of the DoS attack. It stands out among all Cloud attacks, mostly vulnerable Cloud users are recruited by installing malware and making them act like "zombies or handler" to perform illicit acts. Consequently, the DDoS exhaust the Cloud resources like memory, storage, virtual machine (VM), networking, etc. make the legitimate Cloud users unable to access the data centers or degrade its services due to packets request higher than available resources (Somani et al., 2017). The DDoS attacks taxonomies are Network/Transport layer attacks and Application layer attacks. These two attacks cause organizations' financial and operational losses. The techniques adopted by attackers is IP spoof, Botnet controller, software vulnerabilities, etc. Detecting DDoS attack is a difficult task because attackers use spoofed (fake) IP addresses to send packets and makes it difficult to detect or trace-back (Somani et al., 2017).

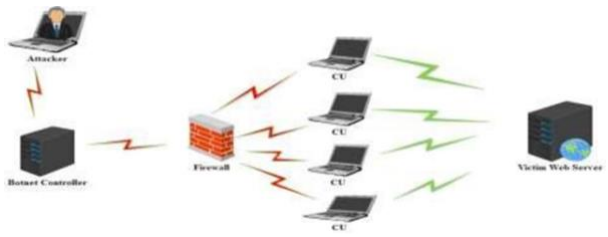

Figure 2. DDoS attack

Under Cloud users' pretense, the attacker uses the Botnet controller to send packets to the victim from a remote location, as shown in figure 2 above. The victim is continuing to receive the packets until its resources become unavailable or degraded. The DDoS flood attack is challenging to trace-back using methods like hop-count or time to live TTL features of the transport control protocol/ internet protocol TCP/IP. The use of a firewall makes attacks to be trace-back to the firewall and not the attacker, therefore protecting the attacker's identity (Somani et al., 2017).

The EDoS attack exploits the rapid elasticity and measured service available in the cloud network to make the environment financially unsustainable to Cloud users and service providers. Attackers mostly target the Infrastructure-as-a-Service (IaaS) of service providers. The EDoS attack takes the usual pattern of DDoS attack method using Cloud users vulnerabilities (i.e., software, protocol, IP addresses) to install malicious software "malware." It makes them act on the attacker's instructions to send unsolicited packets to the targeted system or service until the environment becomes financially unsustainable (VivinSandar, et al., 2012).

Table 1. DoS, DDoS, and EDoS attack differences and similarities.

Attack	**DoS Attack**	**DDoS Attack**	**EDoS**
	1. Single attacker and device are involved.	1. Multiple attackers and devices are used.	1. Multiple attackers and devices are involved.
	2. The attacker in single location.	2. The attackers in multiple locations.	2. The attackers in multiple locations
Similarities	3. The attack is slow and easy to trace.	3. The attack is fast and difficult to trace.	3. The attack is fast and difficult to trace.
And	4. The attack volume is low.	4. The attack volume is high.	4. The attack volume is high.
Difference	5. Attacks both traditional and Cloud networks	5. Attacks both traditional and Cloud networks	5. Attacks only Cloud infrastructure since traditional networks are not scalable
	6. Attacks service model	6. Attacks service model.	6. Attacks billing model.
	7. Attack period is short.	7. Attack period is short.	7. Attack period is long.

3. Computing

To address the challenges of Cloud network CISCO systems introduced Fog computing in 2012; Fog computing is not a replacement for Cloud computing, rather complements the Cloud services. Fog computing center intermediate node between the CS and the data centers, therefore some little computation, storage, processing, et.c can be done within the Fog server otherwise, are forwarded to the Cloud data center (Stojmenovic et al., 2014). The figure below shows the architecture of the Fog to Cloud networks.

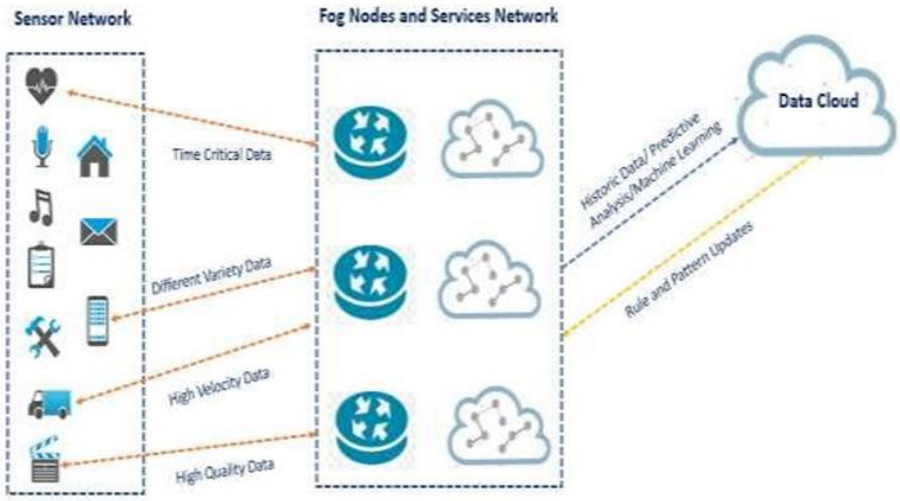

Figure 3. Fog and Cloud architecture (Stojmenovic et al., 2014).

4. Review of Work

Somani et al., (2017) provide a comprehensive and detailed survey of DDoS attacks and defense mechanisms. The researcher divided the DDoS protection strategy into categories. First, The prevention method is a proactive approach using challenge-response, resource limit, restrictive access, etc. Second, the Detection approach is post-active using anomaly detection, source spoof trace, BotCloud detection, resource usage, and lastly, Mitigation is reactive design, i.e., resource scaling, victim migration, software-defined networking, etc. Swati et al. (2019) use a machine learning approach to mitigate EDoS attack in the Cloud environment. Artificial neural networks ANN is used to determine the path and suspected service provider. The ANN is split into training and test the model. Osanaiye (2015) uses fingerprinting of a host-based operating system (OS), which uses passive and active approach methods to compare the incoming packet operating system from

its database. The research incorporates TTL as a second defense mechanism; this also resolves the attacker's problem and legitimate sharing the same OS. Chowdhury et al. (2017) give an overview of mitigation approaches proposed by researchers over the years exclusively for et al., defense. We present a taxonomy of EDoS attack mitigation strategies with circumspect. The taxonomy focus evaluation metric used to mitigate EDoS, along with its applicability in the Cloud environment. Chowdhury et al. (2017) use game theory to model an interactive game between the attacker and the defended; the poison distribution is adopted and validated using MATHEMATICAL simulation. The paper uses the proactive defense stated in Somani et al. (2017) to build a lightweight technique of solving EDoS attacks

5. Mitigation Approach

Fog computing center intermediate node between the CS and the data centers, therefore some little computation, storage, processing, etc. are done within the Fog server else; the packet is forwarded to the Cloud data centers (Zhang et al., 2018). The closeness of Fog servers to the ground offers a great deal of security edge. The Fog server is proposed as an additional firewall for the Cloud data centers where all ingress packet requests are filtered. The following are the four steps needed to ensure EDoS attack in Fog Network.

Step 1: The arrived packet IP address checked in IP Blacklist on the Fog server

Step 2: All requests greater than the specific bandwidth threshold by the cloud service providers.

Step 3: IF the packet request is greater than the bandwidth threshold in step 2: the Fog server sends CAPTCHA for Cloud users to solve.

Step 4: IF CAPTCHA is correct, the packet forwarded to the data center, Else the packet IP address is added to a blacklist and dropped

6. Result

When the packet 1 arrives at the Fog server, as shown above, packet IP address compared with the IP Blacklist the Fog server, if the packet IP exists, the packet is dropped else the passed to the next phase. The Fog server checks the packet request if it is greater than the maximum bandwidth threshold specified by the cloud service provider, a CAPTCHA is sent to the client to solve. The CAPTCHA tends to confirm if the request is coming from a human or machine, ie. Botnet controller. If the CAPTCHA selected correctly, the packet is forwarded to the Cloud web server else, add to the blacklist, and drop.

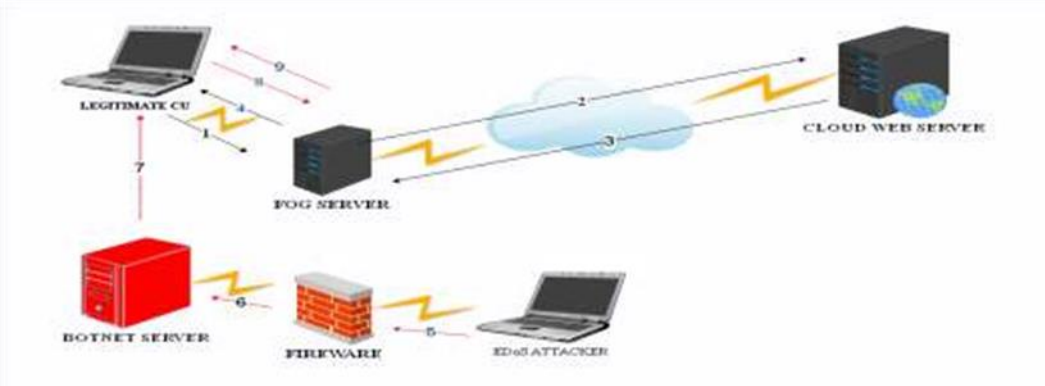

Figure 3. The EDoS attack defense using Fog server

7. Conclusion

Cloud computing offers several benefits to the organization by reducing both capital and operational expenditures CapEx and OpEx. The full adoption of Cloud networks makes it attractive for cyber-criminals to perform illicit acts. The EDoS attack poses the risk of rendering the Cloud environment financially unsustainable for Cloud users. This paper proposes a fourstep lightweight approach of EDoS attack defense in the Cloud computing environment by placing a Fog server that checks the blacklist of IP addresses and each packet's bandwidth threshold at arrival. The research demonstrates how the Fog server adds security enhancement to the Cloud networks.

References

Arif, M., Wang, G., Wang, T., & Peng, T. (2018). SDN-Based Secure VANETs Communication with Fog Computing. Security, Privacy, and Anonymity in Computation, Communication, and Storage, 46–59. https://doi.org/10.1007/978-3-03005345-1_4

Chandrasekaran, K., 2015. Essentials Of Cloud Computing. London: Chapman & Hall, pp.1417.

Chowdhury, F. Z., Kiah, L. B. M., Ahsan, M. A. M., & Bin Idris, M. Y. I. (2017). Economic denial of sustainability (EDoS) mitigation approaches in Cloud: Analysis and open challenges. 2017 International Conference on Electrical Engineering and Computer Science (ICECOS), 1–6. https://doi.org/10.1109/icecos.2017.8167135

Chowdhury, F. Z., Idris, M. Y. I., Kiah, L. M., & Manazir Ahsan, M. A. (2017). EDoS eye: A game-theoretic approach to mitigate economic denial of sustainability attack in cloud computing. 2017 IEEE 8th Control and System Graduate Research Colloquium (ICSGRC), 1–6. https://doi.org/10.1109/icsgrc.2017.8070588

Osanaiye, O. A. (2015). Short Paper: IP spoofing detection for preventing DDoS attack in Cloud Computing. 2015 18th International Conference on Intelligence in Next Generation Networks, 139–141. https://doi.org/10.1109/icin.2015.7073820

Mirkovic, J., & Reiher, P. (2004). A taxonomy of DDoS attack and DDoS defense mechanisms. ACM SIGCOMM Computer Communication Review, 34(2), 39–53. https://doi.org/10.1145/997150.997156

Priyadarshini, R., Kumar Barik, R., & Dubey, H. (2020). Fog-SDN: A light mitigation scheme for DDoS attack in fog computing framework. International Journal of Communication Systems, 33(9), 1–13. https://doi.org/10.1002/dac.4389

Somani, G., Gaur, M. S., Sanghi, D., Conti, M., & Buyya, R. (2017). DDoS attacks in cloud computing: Issues, taxonomy, and future directions. Computer Communications, 107, 30–48. https://doi.org/10.1016/j.comcom.2017.03.010

Stojmenovic, I., & Wen, S. (2014). The Fog Computing Paradigm: Scenarios and Security Issues. Proceedings of the 2014 Federated Conference on Computer Science and Information Systems, 1–8. https://doi.org/10.15439/2014f503

Swati, N., Rama Krishna, C., & Shruti, W. (2019). Mitigating Economic Denial of Sustainability (EDoS) in Cloud Environment using Genetic Algorithm and Artificial Neural Network. VOLUME-8 ISSUE-10, AUGUST 2019, REGULAR ISSUE, 8(10), 3415–3421. https://doi.org/10.35940/ijitee.j9680.0881019

VivinSandar, S., & Shenai, S. (2012). Economic Denial of Sustainability (EDoS) in Cloud Services using HTTP and XML based DDoS Attacks. International Journal of Computer Applications, 41(20), 11–16. https://doi.org/10.5120/5807-8063

Zhang, P., Zhou, M., & Fortino, G. (2018). Security and trust issues in Fog computing: A survey. Future Generation Computer Systems, 88, 16–27. https://doi.org/10.1016/j.future.2018.05.008

Zhou, L., Guo, H., & Deng, G. (2019). A fog computing-based approach to DDoS mitigation in IIoT systems. Computers & Security, 85, 51–62. https://doi.org/10.1016/j.cose.2019.04.017