Securing Cloud Framework from Application DDoS Attacks

N. P. Ponnuviji, M. Vigilson Prem

Abstract*: With the extensive growth of in the size of data transmitted and received in the cloud, there arises the risk of sensitive data prone to different kinds of attacks. The attacks may be in the form of intrusions trying to hack the data or in the form of some fatal attacks. To focus more, after the extensive use of applications and social media apps, there is a rise in Application DDoS (Distributed Denial-of-Service) attacks. These attacks are called as L7 (Layer 7) of the OSI Reference model, as they target the topmost layer – the Application Layer. Various simulations in the Cloud have concluded that the cumulative energy consumption and huge amount of migrations on the VMs are severely affected by the Application DDoS attacks or the EDoS (Economic Denial of Sustainability) attacks. This paper discusses the various forms of Application DDoS attacks, the mitigation mechanisms for the Application DDoS attacks and compares the results in the simulated cloud environment.

***Keywords*: Distributed Denial of Service (DDoS) attack, Economic Denial of Sustainability (EDoS) attack, Layer 7 (L7), Open Systems Interconnect (OSI)**

I. INTRODUCTION

Cloud computing has become an extensive part of the technological services used in our daily lives. Data transmission and data storage has been easy with the help of the cloud computing technology. Apart from the cloud-based websites, the apps used in social media are now dependent on the cloud technology. Even though, new features are added to the cloud day-by-day, new threats also arise in using the technology. The Application DDoS attack is one of the major threat and called as the Layer 7 attack as it tends to target the topmost layer of the OSI Reference Model, the Application Layer [5]. The DDoS/EDoS attacks affect the simulations on the cloud by consuming excess energy with the amount of VM migrations and analyses the factors that depend on the attack quantification including the strength of the DDoS attack [1]. A variety of statistical approaches are conducted using the second-order statistics to identify the HTTP-flooding attacks through a Covariance Matrix approach [2] to detect the intrusions. A hypothesis test has been conducted to represent the Low-rate DDoS (LDoS) attack in a cloud environment [3].

The application DDoS attack takes up several forms in targeting the Application layer. The research studies related to the different IDS approaches in the cloud determine the intensity of the Application DDoS attacks in the cloud environment. This paper focuses on the idea in detecting and preventing the Application DDoS attacks by conducting a detailed analysis and survey of various forms of Application DDoS attacks. It also highlights the various forms of Application DDoS attacks and elaborates the mitigation mechanisms for these attacks

II. RELATED KNOWLEDGE AND RESEARCH STATUS

In section 3, we discuss about the ways in which the DDoS / EDoS attack takes place in the cloud. Especially, when the DDoS attack targets the victim sever by throwing large number of requests for service by either bots or group of clients at similar time or at different intervals. [1]

In section 4, we study about the various types of DDoS attacks that in common making the cloud into an intruded environment. [7]

In section 5, we analyse a multivariate correlation analysis-based detection approach (MADM) [6], which helps to detect the Application DDoS attacks in the form of HTTP-flooding attacks that affects the cloud servers. It further explains the covariance matrix approach in the form of 0-1 matrix.

In section 6, we highlight the use of three entities involved in causing the DDoS attack–Attacker, Handler and Bot. It further elaborates by conducting the hypothesis test for detecting the DDoS attacks at low-rate in the cloud environment. [3]

III. APPLICATION DDoS ATTACK IN THE CLOUD

As we are aware that the Distributed Denial of Service (DDoS) attacks often target and attack the victim server by continuously sending service requests through a group of bots or by a gang of distributed clients. The service requests pour either in a concurrent manner or in a non-coordinated manner. This scenario would result the affected victim to pay expensive bills, as the resources get shrinked and expanded resulting to accounting of 'pay-as-you-go' billing. This application DDoS ultimately leads to Economic Denial of Sustainability (EDoS) attacks of the owner. Usually, it becomes common in targeting the Virtual Machines (VMs) linked to the server.

The diagram below depicts the scenario of the DDoS with various stakeholders.

Revised Manuscript Received on 14 November, 2019.

***** Correspondence Author

N. P. Ponnuviji, Department of CSE, RMD Engineering College, Kavaraipettai, INDIA. Email: ponnuviji@gmail.com

M. Vigilson Prem, Department of CSE, RMK College of Engineering and Technology, Puduvoyal, INDIA. Email: vigiprem@gmail.com

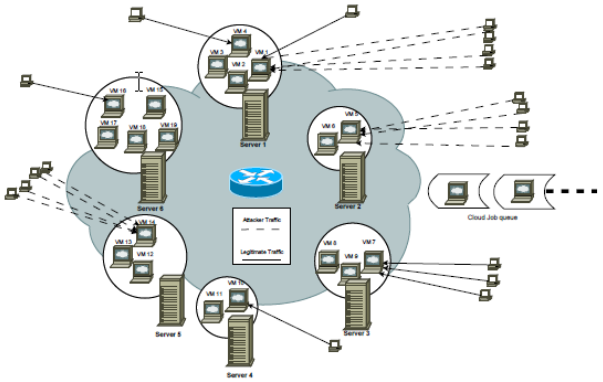


Fig. 1 DDoS setup with few stakeholders

Let us suppose, when VM1 is targeted by the DDoS, it affects many resources like the CPU, internal hard disk, memory, bandwidth, TCP connections, open files and directories, etc. Henceforth, even if the VM1 fails due to the attack, the process may migrate and continue with the remaining servers, which may also get affected and targeted by the DDoS. Therefore, this process of shrinking and expanding of the resources due to the DDoS attack leads to EDoS attacks, as the pay-bill for the resources expanded goes very high. This has been tested under the Infrastructure cloud, wherein the VM owner would only have finite resources. This may get extended to the web server finally reaching to a state in denying to offer and provide the cloud service. Time and Attacker target are the two important metrics dealt to further experiment and handle the problem. The experiments are conducted in two states. With the setup of Single Physical Server and on Cloud Scale, where it handled the features such as auto-scaling, migrating, multi-tenancy, performance interference and resource race. This approach helps to alter the cloud infrastructure to defend the VMs from these attacks.

IV. COMMON DDoS ATTACKS AND MITIGATION STRATEGIES

There are various types of DDoS attacks. We will discuss common DDoS attacks and how they can be mitigated in the cloud. [7]

Memcached DDoS attack: It is a kind of cyber-attack, where the attacker tries to reduce the performance a targeted victim by overloading and inducing with heavy load of internet traffic. The UDP memcached server is spoofed with requests, which floods the target victim with heavy traffic in the internetwork. In this case, new requests are denied, accepted requests go unprocessed and resource utilization in internet cannot be accessed. This attack can be mitigated by disabling UDP, preventing IP spoofing, firewalling memcached server.

NTP amplification attack: Here the attacker exploits the functionality of Network Timing Protocol (NTP) server with amplified amount of UDP traffic and stopping the accessibility to regular traffic. It is a reflection-based volumetric DDoS attack. This attack can be mitigated by verifying the source IP to prevent the spoofed packets going out of the network.

Simple Service Discovery Protocol (SSDP) attack: This is similar to the NTP attack, wherein it utilises Universal Plug and Play (UPnP) networking protocols by sending heavily increased traffic to the victim causing the web resources to go offline. The key way to mitigate is to block the incoming UDP traffic on port 1900 at the firewall.

Domain Name System (DNS) Flood attack: The DNS act as phonebooks of internet. It creates a path for internet devices to access specific webservers to refer the internet content. It is a type of DDoS, where an attacker floods a particular domain's DNS servers to disrupt the DNS traffic flow. It fails to differentiate normal traffic, as large volumes of traffic comes from unique locations, enacting like legitimate traffic. We need to use a large and highly distributed DNS to monitor and block the traffic in real-time situations.

HTTP Flood attack: This is voluminous DDoS attack. It targets the server with HTTP requests. Response comes to a standstill, once the requests reaches the saturated level and disrupts normal traffic. HTTP GET attack and HTTP POST attack are its subforms of attacks. To mitigate, we need to use a web application firewall (WAFF).

SYN Flood attack: It is a half-open attack that refrains the server to respond to authorized traffic by using all server resources, sending the initial connection request (SYN) packets. This makes the targeted device not to avoid responding to authorised traffic. It can be mitigated by re-establishing the partially-opened TCP connection.

UDP Flood attack: This DoS attack, wherein huge numbers of User Datagram Protocol (UDP) packets are sent to a targeted server making the firewall to reach its exhausted state, resulting in DoS to legitimate traffic. One way to mitigate is to limit the response rate of ICMP packets.

PING (ICMP) Flood attack: This DoS attack targets the devices with ICMP echo-request packets, making the affected devices not able to access the normal traffic. When the threat comes from many devices, it is a DDoS attack. This attack can be mitigated by making the targeted router and other devices of the ICMP non-functional.

Application Layer or L7 attack: This attack is a malicious behavioural attack designed to target the 'top' layer in the OSI model. They are effective due to their consumption of server resources and network resources. It can be mitigated by testing with a CAPTCHA to check whether or not it is a bot.

Cryptocurrency attack: This attack paved way for digital currency attacks. It is not authorized or backed or accepted legally by any government. It is always a decentralized international currency. The concept of blockchain can be used to mitigate the cryptocurrency attack.

V. MADM AND COVARIANCE MATRIX APPROACH TO DETECT CLOUD-BASED HTTP ATTACK

As we have seen the various DDoS attacks. Research has been conducted by adopting various strategies to detect the HTTP attack in a cloud-based environment. The study on Multivariate Correlation Analysis-based detection

approach (MADM) [6], helps to detect the HTTP-flooding attacks in number of cloud-based web servers. It is basically a statistical approach and consumes fewer resources for its training and testing algorithms. During its execution, the covariance matrices on the normal dataset is computed. The outcome of this covariance matrix-based detection approach is a 0-1 matrix, where it highlights the degree of the deviation from the normal behaviour and the testing datasets. The MADM calss diagram is given below.

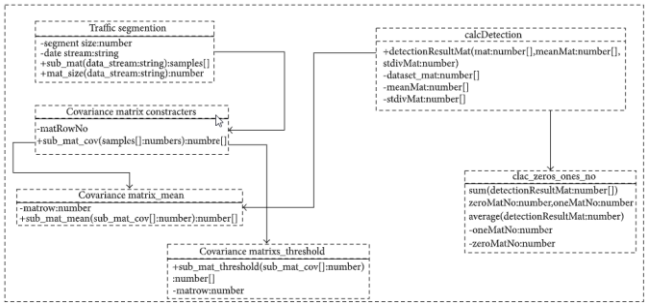


Fig 2. Class diagram – MADM

This implementation evaluates by capturing the normal traffic dataset at the end user by surfing the internet. In its second step, the dataset is preprocessed and converted into MySQL database in a simplified manner, wherein the flooding attacks and normal class data are separated into dependent tables.

The analysis further illustrates that flooding attacks in a secured cloud environment shows that attacker might be a true user meaning both the attacker and affected VM are present in the same subnetwork. The figure given below illustrates it.

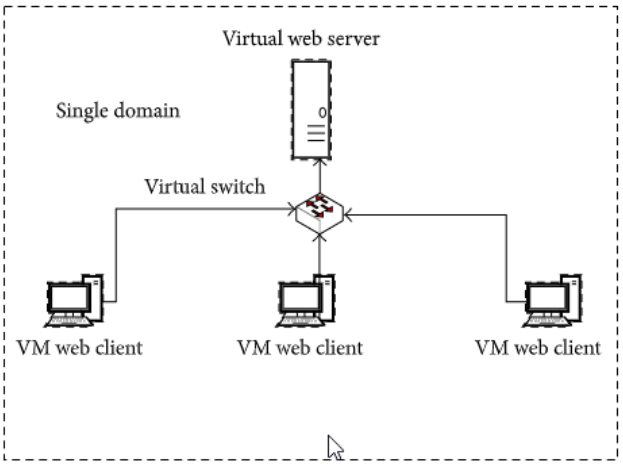


Fig 3. Internal flooding attacks in a cloud

The other form where the attacker may be valid cloud user and affected VM are present in the different subnetwork, causing the external flooding attacks. The architecture of the flooding attacks at the external cloud network is shown.

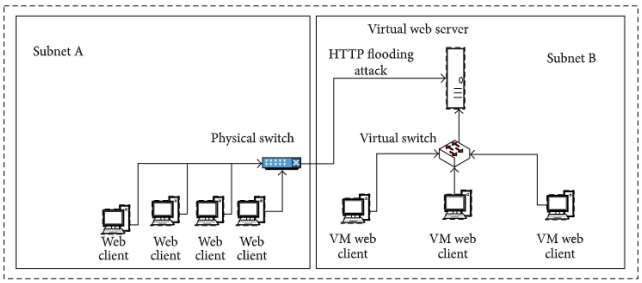
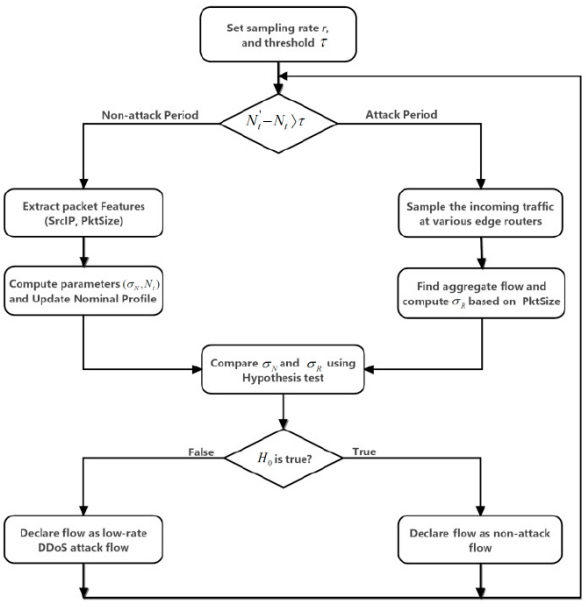


Fig 4. External flooding attacks in the cloud

Hence, through the results obtained in the simulated environment, we encourage to implement the same in real time cloud applications to produce results that detect the HTTP flooding attacks, through a manageable cost and less time consuming approach.

VI. DETECTION OF LOW-RATE DDoS ATTACK IN CLOUD

The Low-rate DDoS attack is subset of the DDoS attack but differs in terms of volumes of attack. These attacks come with low frequency in normal traffic and are capable to go undetected in a DDoS detection system. The foremost of priority of the LDoS attack is to destroy and damage the QoS (Quality of Service) of the victim. In this approach, the incoming traffic is sampled, at the routers' edge of the network. The LDoS attacks can be tracked based on the four parameters. They are the frequency of the LDoS attack, Length of the burst of the attack, Rate of packets collected during the attack burst and the starting time of the attack.
Therefore, to detect the LDoS attack, Gupta et al., [3] has conducted a statistical approach based on the hypothesis test, which follows the student's T-distribution. An overview illustrating the LDoS attack flow detection process is indicated in the flowchart below.



The scheme has used the DARPA dataset and CAIDA dataset to test the DDoS attack. In this approach, all the packets of the DARPA dataset are considered authorised packets and all the packets of the CAIDA dataset are considered as attack packets. The appropriate results are yielded and this mechanism recognizes the LDoS attack flows based on the t-statistic and deals it very efficiently.

VII. CONCLUSION

The security in cloud has been a threat since the adoption of cloud technology. The Application DDoS attacks are dangerous in the cloud as the attacker uses the heavy cloud resources to conduct the attacks by targeting the victim server. In this paper, we have discussed the Application DDoS attack problem in the cloud computing scenario is investigated and discussed. We have elaborately discussed and classified the various Application DDoS attacks and its nature of cause. The properties and capabilities of each of them is highlighted and the steps to mitigate is also illustrated in detail, providing a guideline for further research to proceed. Further the approach of MADM architecture using the covariance matrix approach has been widely discussed. Nextly, the hypothesis test approach to detect the Low-rate DDoS has yielded good results. Thus the main issue should be considered in future researches of the Application DDoS attack detection.

REFERENCES

1. Gaurav Somani, et al, "DDoS/EDoS attack in Cloud: Affecting everyone out there," SIN '15, September 08-10, 2015, Sochi, Russian Federation.
2. Abdulaziz Aborujilah et al, "Cloud-Based DDoS HTTP Attack Detection Using Covariance Matrix Approach", Hindawi Journal of Computer Networks and Communications, Volume 2017, Article ID 7674594, Available: https://doi.org/10.1155/2017/7674594
3. Gupta et al, "Hypothesis Test for Low-rate DDoS Attack Detection in Cloud Computing Environment", *Science Direct, Procedia Computer Science, International Conference on Computational Intelligence and Data Science (ICCIDS 2018).*
4. Fahad Zaman Chowdury et al, "EDoS eye: A game theoretic approach to mitigate economic denial of sustainability attack in cloud computing", Control and System Graduate Research Colloquium (ICSGRC), IEEE 8th International Conference, 2017.
5. Shruti Wadhwa et al., "Prevention of DDoS & EDoS using Hybrid Filtering technique in a Cloud Environment", International Journal of Pure and Applied Mathematics, Vol. 114 No. 12 Pages 383-392, 2017.
6. D. S. Yeung et al., "Covariance-matrix modeling and detecting various flooding attacks," IEEE Transactions on Systems, Man, and Cybernetics Part A:Systems and Humans, Vol. 37, No. 2, pp157-169, 2007.
7. https://cloudfare.com/learning/ddos
8. Shikha Vashisht et al., "Study of Cloud Computing Environment EDoS attack using CloudSim (Modelling and Simulation/Simulator)," Internationaal Journal of Advanced Research in Computer Science, Vol. 6 No. 5, May-June 2015.
9. Mohammad Masdari, et al., "A survey and taxonomy of DoS attacks in cloud computing: DoS attacks in cloud computing," Security and Communication Networks, DOI: 10.1002/sec.1539, July 2016.
10. K. Labs. Global it security risks survey 2014, A Distributed denial of service (ddos) attacks. Available: http://media.kaspersky.com/en/ B2B-International-2014-Survey-DDoS-Summary-Report. Pdf, 2014.
11. R. Pandrangi. Verisign's q4 2014 ddos trends: Public sector experiences largest increase in ddos attacks. http://blogs.verisigninc.com/blog/entry/verisign_s_q4_2014_ddos, 2015.
12. Baig, Z.A., Sait, et al., "Controlled access to cloud resources for mitigating Economic Denial of Sustainability (EDoS) attacks," Computer Networks 97: 31-47.
13. S. Alsowail et al., "An experimental evaluation of the EDoS-shield mitigation technique for securing the cloud," Arabian Journal for Science and Engineering, Vol. 41, no. 12, pp. 5037-5047, 2016.
14. I. Gul and M. Hussain, "Distributed cloud intrusion detection system (H-NIDS) in cloud computing", in Proceedings of the IEEE Symposium on Computational Intelligence in Cyber Security (CICS '13), pp. 23-30, April 2013.
15. R. Miao et al., "Nimbus: Cloud-scale attack detection and mitigation," Proceedings of the 2014 ACM conference on SIGCOMM, pages 121-122, ACM, 2014.

AUTHORS PROFILE

N. P. Ponnuviji, is a Research Scholar in RMD Engineering College in the Department of Computer Science and Engineering. She holds her M.Tech in Computer Science and Engineering from SRM University, Chennai and is currently pursuing her research in Anna University, Chennai. She has 14 years of Academic experience and 3 years of Research experience. She has published her work in National and International journals. She owns a life-term ISTE membership.

M. Vigilson Prem, works as a Professor in the Department of Computer Science and Engineering in RMK College of Engineering and Technology. He holds his Ph.D from Anna University, Chennai. He has over 25 years of experience in Academic and Research. He has published his work in various National and International Journals. He holds a life-term ISTE membership. He has conducted various workshops and seminars in Image Proessing and Cloud Computing.