Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 44 No. 5 (2023)

Novel Light Weight Defense Framework for DDoS Attack in Cloud Environment

[1]Mr. M. Mathiyalagan, [2]Dr. N. Suresh.

[1]Research Scholar, Department of Computer Science, Park's College (Autonomous), Tirupur.
mathi84@gmail.com.
[2]Research Supervisor, Department of Computer Science, Park's College (Autonomous), Tirupur.
bksuresh13013@gmail.com.

Abstract - In order to identify harmful attacks against cyber systems, a monitoring technique is essential. Identifying distributed denial of service (DDOS) and denial of service (DOS) attacks is a critical security issue for network technology. Businesses are turning to the cloud, a highly-available platform, for all of their information technology demands. Because it is a platform that is frequently utilized, cyber-attacks target it frequently. A serious threat to cloud computing is distributed denial of service (DDoS), which involves attacking cloud apps, bandwidth, and resources to make services unavailable. Several botnets attack the victim of a denial-of-service attack (DDoS) by sending a large number of bogus IP requests to the server. Numerous techniques have been put forth for the detection and avoidance of network anomalies since their discovery in 1980. This study provides a background of DDoS attack detection methods in past decade and a survey of some of the latest proposed strategies to detect DDoS attacks in the cloud, the methods are further compared for their detection accuracy.

Keywords: - Denial of Service (DoS), Distributed DoS (DDoS), Attacks, Cloud Environment, Cyber Attacks, and Defense Framework.

1. INTRODUCTION

Cloud Computing has emerged as a modern model that enables consumers to use on-demand software to meet their needs. Security issues however are main obstacles to the wider adoption of clouds. The technical advances that clouds have introduced, such as multi-tenancy, resource sharing and outsourcing, pose new challenges to security research. Distributed Denial of Service (DDoS) attack is the biggest threat to the cloud as it affects the availability of services. A DDoS attack is a malicious attempt to disrupt the normal traffic of a targeted server, service or network by flooding the target or surrounding networks with a flood of Internet traffic. DDoS attacks are effective by using a variety of compromised computer systems as sources of attack traffic. A denial-of-service attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service [1]. A distributed denial-of-service attack deploys multiple machines to attain this goal. The service is denied by sending a stream of packets to a victim that either consumes some key resource, thus rendering it unavailable to legitimate clients, or provides the attacker with unlimited access to the victim machine so he can inflict arbitrary damage. Distributed denial of service (DDoS) attacks in cloud computing environments are growing due to the essential characteristics of cloud computing [2].

During the attack the attacker exhausts all of the cloud resources by using fake resources, resulting in a denial of service to the legitimate user. The consequences of the DDoS attack are more dangerous in the cloud setting compared to conventional networks due to the scalability, resource sharing and multi-tenant properties of the cloud. It is important to remember that there has not been a centralized algorithm designed to prevent and mitigate real-time DDoS attacks [19]. DDoS mitigation refers to the method of successfully shielding a target server or network from DDoS. Through using specially built network equipment or cloud-based security services, the targeted victim is able to minimize the incoming attack.

Security in Cloud Computing is critical when developing services. Updating the operating systems of virtual machines, ensuring availability, isolating users' individual data, implementing authentication mechanisms, encryption or configuring VPN and VLAN are but a few examples of what needs to be considered. Here is a list of the security aspects that challenge Cloud Computing [21].

- Identity, Authentication, Authorization
- Confidentiality
- Integrity

- Isolation
- Availability

In traditional networks, the security strategies are complex, not easy to manage, and the upgrading is time-consuming, which needs the participation of vendors [6]. The proposed taxonomies are complete in the following sense: the attack taxonomy covers known attacks and also those that have not currently appeared but are potential threats that would affect current defense mechanisms; the defense systems taxonomy covers not only published approaches but also some commercial approaches that are sufficiently documented to be analyzed. Along with classification, to emphasize important features of each attack or defense system category, and provide representative examples of existing mechanisms. In cloud computing environment DDoS attacks are continually evolving with intelligent strategies. Low-rate DDoS attack is one such strategy that make it difficult to detect attack. At the same time, cloud infrastructure is also evolving rapidly. Container based technology enables cloud computing to have lightweight approaches in resource utilization and flexibility in scaling services [20]. The existing DDoS attack detection methods used in cloud computing are not adequate when adversaries employ the modality known low-rate DDoS attack. There is need for an approach that not only detects the attack but also defeat the attack as much as possible.

The following is how the paper is structured: Section 2 addresses several similar works and explains why a new approach is needed. Section 3 describes the overview of the proposed and its phases and how the process will contribute to the creation of our novel model and Section 4 conclude and discuss about the future work.

2. RELATED WORK

Denial of Service, or DoS, is a very common form of cyber attack that has become very prevalent in the recent past. It can be defined as the practice of unwanted interruption or prevention to the user's Internet activity. This, almost in all cases, is done with malicious purposes [7]. Now, the objective of this paper is primarily to characterize the many types and varieties in which these attacks are caused, and here discovered several literature reviews that analyzed DDoS attacks prevention, detection and mitigation from various perspectives.

Aydın, H., Orman, Z., & Aydın, M. A. (2022) analyzes the Distributed Denial of Service (DDoS) attacks can exploit, disrupt, change, prevent or damage cloud services. Accurate and timely detection and prevention of these attacks are very important in terms of ensuring information security [3]. During the COVID-19 period, the increase in the use of information technologies and especially the internet has made cyber-attacks a real concern. Deep learning (DL) has become widely used for the purpose of detecting and preventing cyber-attacks to provide information security. In this study, a Long Short-Term Memory (LSTM) based system (LSTM-CLOUD) which was designed for the detection and prevention of DDoS attacks in a public cloud network environment was proposed. The design of the system is based on a signature-based attack detection approach. The LSTM-CLOUD has two modules defined in the study: detection and defense. The function of the first module of the system was determined as detecting the occurrence of DDoS attacks with the LSTM DL model developed in this study with an accuracy rate of 99.83% on the CICDDoS2019 data set. The function of the second module was determined as activating the defense mechanism to protect the cloud systems when attacks are detected. The comparison results showed that our LSTM model had a performance as good as those in the previous studies conducted with different DL algorithms on the same and different datasets. The results obtained show the effectiveness of the LSTM model developed in this study in detecting the occurrence of attacks.

Wang, J., & Wang, L. (2022) addressed the problem with the development of Software Defined Networking (SDN), its security is becoming increasingly important [4]. Since SDN has the characteristics of centralized management and programmable, attackers can easily take advantage of the security vulnerabilities of SDN to carry out distributed denial of service (DDoS) attacks, which will cause the memory of controllers and switches to be occupied, network bandwidth and server resources to be exhausted, affecting the use of normal users. To solve this problem, this paper designs and implements an online attack detection and mitigation SDN defense system. The SDN defense system consists of two modules: anomaly detection module and mitigation module. The anomaly detection model uses a lightweight hybrid deep learning method—Convolutional Neural Network and Extreme Learning Machine (CNN-ELM) for anomaly detection of traffic. The mitigation model uses IP traceback to locate the attacker and effectively filters out abnormal traffic by sending flow rule commands from the controller. Finally, we evaluate the SDN defense system. The experimental results show that the SDN defense system can accurately identify and effectively mitigate DDoS attack flows in real-time.

Venkateshwarlu, V., Ranjith, D., & Raju, A. (2023) proposed the solution for Low-rate DDoS attack is one such strategy that make it difficult to detect attack. At the same time, cloud infrastructure is also evolving rapidly [5]. Container based technology enables cloud computing to have lightweight approaches in resource

utilization and flexibility in scaling services. The existing DDoS attack detection methods used in cloud computing are not adequate when adversaries employ the modality known low-rate DDoS attack. There is need for an approach that not only detects the attack but also defeat the attack as much as possible. Towards this end, in this paper, we proposed a framework named Low-Rate DDoS Attack Detection Framework (LRDADF). Since low-rate DDoS attacks are difficult to be defeated, here proposed a mathematical model to realize mitigation strategy besides employing deep learning methods to have effective means of detecting such attacks. Proposed an algorithm named Hybrid Approach for Low-Rate DDoS Detection (HA-LRDD). The algorithm uses an Artificial Intelligence (AI) enabled methods comprising of deep Convolutional Neural Network (CNN) and deep auto encoder. Another algorithm known as Dynamic Low-Rate DDoS Mitigation (DLDM) is used to minimize the effect of the attack after detection or even defeat the attack by ensuring the smooth functioning of cloud infrastructure which is under attack. Extensive simulation study revealed that the proposed framework is able to detect low-rate DDoS attacks and also mitigate the attacks to ensure there is acceptable quality of service in cloud computing environments.

Priyadarshini, R., & Barik, R. K. (2022) focused on Fog computing (FC). It is a contemporary computing paradigm that gives additional support to cloud environment by carrying out some local data analysis in edge of the devices, facilitating networking, computing, infrastructure and storage support as backbone for end user computing [8]. Still enterprises are not convinced to use this as security and privacy are most of the open and challenging issues. Availability among the security requirements is the one which is about rendering on demand service to different client applications without any disruptions. It can often be demolished by Denial of service (DoS) and distributed denial of service (DDoS) attacks in fog and cloud computing environment. The author proposed a novel Source based DDoS defence mechanism which can be used in fog environment as well as the cloud environment to mitigate DDoS attacks. It makes use of Software Defined Network (SDN) to deploy the DDoS defender module at SDN controller to detect the anomalous behavior of DDoS attacks in Network/Transport level. The proposed work provides deep learning (DL) based detection method which makes use of the network traffic analysis mechanisms to filter and forward the legitimate packets to the server and can block the infected packets to cause further attacks.

Zareapoor, M., Shamsolmoali, P., & Alam, M. A. (2018) discussed on Distributed denial of service (DDoS) attacks have become a serious attack on internet security and cloud computing [9]. This kind of attacks is the most complex form of denial of service (DoS) attacks. This type of attack can simply duplicate its source address, such as spoofing attack, which disguises the real location of the attack. Therefore, DDoS attack is the most significant challenge for network security. In this paper, we present a model to detect and mitigate DDoS attacks in cloud computing. The proposed model requires very small storage and has the ability of fast detection. The experimental results show that the system is able to mitigate most of the attacks. Detection accuracy and processing time were the metrics used to evaluate the performance of proposed model. From the results, it is evident that the system achieved high detection accuracy (97%) with some minor false alarms.

Several studies have been examined that explored, illustrated, and investigated the DDoS prevention, detection and mitigation techniques in cloud environment. Among these, the DDoS attack prevention, detection and mitigation approach is gaining popularity due to its functional applicability. Recently, several complex approaches to prevention, detection, and mitigation in the cloud setting have been suggested. However, only a few complex schemes provide an effective mechanism for preventing, detecting, and mitigating DDoS attacks.

3. PROBLEM DEFINITION

Cloud computing is a rapidly developing technology that many businesses have embraced. However, there are other problems, and DDOS is one of them. It may have an impact on businesses that rely on the cloud for their operations. DDoS attacks seriously disrupt availability. The victim's network connectivity can either be completely destroyed or significantly deteriorated by the attacker. The attacker employs a large number of compromised hosts or agents to launch the assault by exhausting the target network. A DDoS attack's primary goal is to prevent the target from using the resources [10]. Targets could include web servers, CPUs, storage, and other network resources in the majority of the scenarios4. DDoS attacks have the ability to seriously impair cloud service performance by causing harm to virtual servers. Cloud computing has been increasingly prevalent in commercial technologies and academic study in recent years. One of the security risks that jeopardizes availability is DDoS. DDoS is one of the top nine hazards to a cloud computing environment, according to Cloud Security Alliance. In a clod environment, 14% of all attacks are DoS attacks [15].

Four hundred Americans and Europeans participated in the survey. In their firms, 74% of respondents have encountered one or more DDoS attacks. According to a poll on DoS attacks in the cloud, the frequency of DDoS attacks would rise quickly along with the usage of cloud computing. When a service in the cloud experiences an increase in workload, it will begin to provide processing resources to handle the added stress.

This indicates that while the cloud system fights against the attacker, it also partially helps him by allowing him to cause the greatest amount of harm to the availability of services, beginning at a single point of attack.

4. PROPOSED METHODOLOGY

Distributed Denial of Service (DDoS) attacks, which are intended to make the service unavailable for legitimate users, originate in a highly distributed manner providing the illusion of legitimate traffic. The number of attacks and the volume of traffic associated with attacks continue to increase dramatically. At these traffic intensities, the network infrastructure upstream from the intended victim also becomes severely affected necessitating that attack traffic be filtered as close as possible to the attack sources [11]. However, it is difficult to anticipate and identify such nodes as the attacks originate at widely distributed nodes and spread through various routes. To successfully respond by dropping traffic, the mitigating approach must identify routers on traffic paths with significant attack traffic and respond with minimum effect on legitimate traffic [14]. It is must to develop a suite of solutions to address this problem.
The proposed work has been split into three phases.

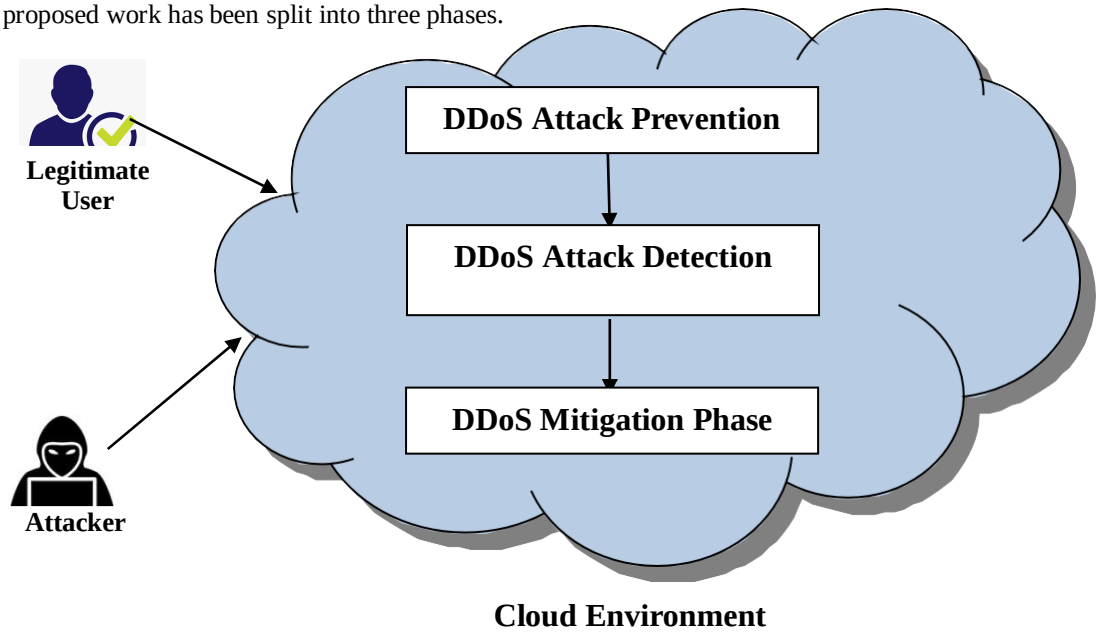

Fig 4.1: - Architecture of the Proposed Work

Phase-1: - DDoS Attack Prevention Phase

This phase is the entry point for the cloud network. A DDoS attack depletes the server resources and increases the server load time. When a DDoS attack hits a server, it may suffer performance issues or crash the server completely by overwhelming the server' resources such as CPU, memory or even the entire network. Here the entire incoming request includes the DDoS attack request and the valid requests are compared to the baseline traffic traces obtained during the training process. Countering DDoS attacks is becoming more challenging with the vast resources and techniques available to the attackers. The proposed work introduces Three-Layer Hop Count Filtering Algorithm. It is improved version of Hop-Count Algorithm. First filter is used for authentication purpose by third party. In the second filter, it compares the current requests with predefined limits of requests from the table. Finally, third filter is used to filter out the spoofed packets.

Phase-2: - DDoS Attack Detection Phase

This phase will separate valid packets from DDoS attack packets that have reached the cloud network. An Entropy based DDoS attack detection method is proposed. Entropy is a statistical measure that shows randomness in packet properties increases more than expected point. Therefore, entropy calculation is helpful measurement method to track these unexpected changes in randomness. Entropy can be calculated for more than one field of IP packets at the same time. By means of this characteristic, it can possible to detect different attacks by using entropy calculation. Even if the number of malicious packets is less than the number of legitimate packets, this method works because the randomness will change sharply as inspected data is intensified at certain points.

Phase-3: - DDoS Attack Mitigation Phase

Once an attack has been detected, the time for mitigation is critical. Most attacks can take a target in a matter of minutes, and the recovery process can take hours. This phase will be done at the monitor agent. The main purpose of the Proposed Hybrid DDoS Attack Mitigation Algorithm (PHDAMA) with Fitness Function (FF) is to mitigate DDoS attacks and to reduce the impact of the DDoS attack on the cloud environment. The purpose of all methods is to distinguish legitimate traffic from malicious traffic by eliminating malicious packets while allowing legitimate packets to reach their destination. It maximizing throughput should be the main goal of the cloud environment; thus the 'fitness' function takes account of maximizing throughput.

The architecture above demonstrates the light weight framework for DDoS attack mitigation in the cloud world. The main objective of this research is to find ways to detect large-scale DDoS attacks in cloud computing. Lightweight mechanisms are used to create a solution that removes the need for complex computing and decreases time consumption.

5. PERFORMANCE EVALUATION

The main goal of this research is to arrive at solutions to detect the DDoS attacks prevailing at large in cloud computing. These attacks lead to the DoS to the cloud consumers by which they are annoyed. To eliminate the hassles created to the end users the cloud consumers, it essential to have solutions to counter the security attacks present in the cloud environment [12].

Lightweight mechanisms are used to create these solutions which eliminate the need of complex computations and reduce the time consumption [13]. These mechanisms are different in three phases of the work. Responsive defense mechanism is evaluated on the basis of three parameters, namely,

- Attack Traffic Detection Rate
- Normal Traffic Detection Rate, and
- Link Utilization Rate.

Attack Detection Rate: Attack traffic detection rate is considered as the percentage of attack dataset that is correctly detected as the attack and cannot pass through the Bloom filter to reach the victim node during the attack time.

Normal Traffic Detection Rate: We use the same logic that was used to identify Attack Traffic Detection Rate to compute these parameters. Normal Traffic Detection Rate is defined as the percentage of normal traffic that can correctly pass through the Bloom filter during the attack period.

Link Utilization Rate: This is defined as the percentage of the network's bandwidth that is currently being Consumed by the network traffic.

5. CONCLUSION

The primary aim of research is to significantly address the DDoS attack prevention, detection and mitigation in cloud environment. Distributed Denial-of-Service (DDoS) attacks utilize the power of thousands, and sometimes tens or hundreds of thousands of compromised, geographically distributed machines, to attack web-services, resulting in their degradation and consequent financial loss. Hence the early and reliable detection of such attacks is an important area of research. Problem faced by current DDoS attack detection and mitigation systems are the heavy volume of traffic flow during the attack. So for the efficient DDoS attack detection system, most appropriate feature must be selected to classify the attack and legitimate request. The best practices that can be incorporated for protecting the cloud against DDoS attacks are briefed. Further research is to detect and defend DDoS attacks in cloud using learning methods.

REFERENCES

[1] Srinivasan, K., Mubarakali, A., Alqahtani, A. S., & Dinesh Kumar, A. (2020). A survey on the impact of DDoS attacks in cloud computing: prevention, detection and mitigation techniques. In Intelligent Communication Technologies and Virtual Mobile Networks: ICICV 2019 (pp. 252-270). Springer International Publishing.

[2] 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.

[3] Aydın, H., Orman, Z., & Aydın, M. A. (2022). A long short-term memory (LSTM)-based distributed denial of service (DDoS) detection and defense system design in public cloud network environment. *Computers & Security*, *118*, 102725.

[4] Wang, J., & Wang, L. (2022). SDN-Defend: A Lightweight Online Attack Detection and Mitigation System for DDoS Attacks in SDN. *Sensors*, *22*(21), 8287.

[5] Venkateshwarlu, V., Ranjith, D., & Raju, A. (2023, February). LRDADF: An AI Enabled Framework for Detecting Low-Rate DDoS Attacks in Cloud Computing Environments. In 2023 Fifth International Conference on Electrical, Computer and Communication Technologies (ICECCT) (pp. 1-8). IEEE.
[6] Deshmukh, R. V., & Devadkar, K. K. (2015). Understanding DDoS attack & its effect in cloud environment. Procedia Computer Science, 49, 202-210.
[7] Potluri, S., Mangla, M., Satpathy, S., & Mohanty, S. N. (2020, July). Detection and prevention mechanisms for ddos attack in cloud computing environment. In 2020 11th international conference on computing, communication and networking technologies (ICCCNT) (pp. 1-6). IEEE.
[8] Priyadarshini, R., & Barik, R. K. (2022). A deep learning based intelligent framework to mitigate DDoS attack in fog environment. Journal of King Saud University-Computer and Information Sciences, 34(3), 825-831.
[9] Zareapoor, M., Shamsolmoali, P., & Alam, M. A. (2018). Advance DDOS detection and mitigation technique for securing cloud. International Journal of Computational Science and Engineering, 16(3), 303-310.
[10] Dong, S., Abbas, K., & Jain, R. (2019). A survey on distributed denial of service (DDoS) attacks in SDN and cloud computing environments. IEEE Access, 7, 80813-80828.
[11] Pandey, V. C., Peddoju, S. K., & Deshpande, P. S. (2018). A statistical and distributed packet filter against DDoS attacks in Cloud environment. Sādhanā, 43, 1-9.
[12] Bakr, A., El-Aziz, A., & Hefny, H. A. (2019). A Survey on mitigation techniques against DDoS attacks on cloud computing architecture. International Journal of Advanced Science and Technology, 28(12), 187-200.
[13] Alanazi, S. T., Anbar, M., Karuppayah, S., Al-Ani, A. K., & Sanjalawe, Y. K. (2019). Detection techniques for DDoS attacks in cloud environment. In Intelligent and Interactive Computing: Proceedings of IIC 2018 (pp. 337-354). Springer Singapore.
[14] Bhardwaj, A., Mangat, V., & Vig, R. (2020). Hyperband tuned deep neural network with well posed stacked sparse autoencoder for detection of DDoS attacks in cloud. IEEE Access, 8, 181916-181929.
[15] Verma, P., Tapaswi, S., & Godfrey, W. W. (2021). A request aware module using CS-IDR to reduce VM level collateral damages caused by DDoS attack in cloud environment. Cluster Computing, 1-17.
[16] Varghese, J. E., & Muniyal, B. (2021). An Efficient IDS framework for DDoS attacks in SDN environment. IEEE Access, 9, 69680-69699.
[17] Bhardwaj, A., Mangat, V., Vig, R., Halder, S., & Conti, M. (2021). Distributed denial of service attacks in cloud: State-of-the-art of scientific and commercial solutions. Computer Science Review, 39, 100332.
[18] Maheshwari, A., Mehraj, B., Khan, M. S., & Idrisi, M. S. (2022). An optimized weighted voting based ensemble model for DDoS attack detection and mitigation in SDN environment. Microprocessors and Microsystems, 89, 104412.
[19] Kautish, S., Reyana, A., & Vidyarthi, A. (2022). SDMTA: Attack detection and mitigation mechanism for DDoS vulnerabilities in hybrid cloud environment. IEEE Transactions on Industrial Informatics, 18(9), 6455-6463.
[20] Mohan, M., Tamizhazhagan, V., & Balaji, S. (2023). A Perspicacious Multi-level Defense System Against DDoS Attacks in Cloud Using Information Metric & Game Theoretical Approach. Journal of Network and Systems Management, 31(4), 1-28.
[21] Gaurav, A., Gupta, B. B., & Panigrahi, P. K. (2022). A novel approach for DDoS attacks detection in COVID-19 scenario for small entrepreneurs. Technological Forecasting and Social Change, 177, 121554.