A Study Of Cloud Based Ddos Mitigation Architecture With Blacklist Filtering Strategy

Ajitesh Kumar Saha[1] , Dr. Akash Saxena[2]

[1]Research Scholar, Department of Computer Science & Engineering, Mansarovar Global University, Sehore, Madhya Pradesh.
[2]Supervisor, Department of Computer Science & Engineering, Mansarovar Global University, Sehore, Madhya Pradesh.

ABSTRACT

DDoS assaults provide a substantial risk to the accessibility and dependability of cloud-based online services, affecting corporations, organizations, and individuals. Conventional DDoS defense methods are frequently ineffective in cloud settings because of their ever-changing characteristics and the financial consequences of service interruptions. This article introduces a proposed architectural solution to reduce DDoS assaults on a cloud-hosted application. This design relies on creating a duplicate of the application in a cloud environment and directing only valid requests to this duplicate. The suggested architecture may filter valid traffic without the requirement to identify hostile consumers, therefore avoiding the associated burden and potential mistakes.

Keywords: Legitimate, Mitigation, Blacklist, Response time, Network.

I. INTRODUCTION

As the dependence on cloud infrastructure continues to increase, it has become increasingly important to take measures to mitigate Distributed Denial of Service (DDoS) attacks in cloud web services. There is a considerable danger that distributed denial of service assaults pose to the availability and dependability of cloud-based applications and services. This risk is exacerbated by the growing number of devices that are connected to the internet and the growing complexity of cyber threats. It is well known that these assaults have the capability of flooding servers and networks with a torrent of malicious traffic, which effectively renders the targeted services unavailable to users who are authorized to use them. The dynamic nature of cloud settings provides unique issues when it comes to properly fighting against distributed denial of service attacks (DDoS). Traditional DDoS mitigation solutions often concentrate on identifying and blocking malicious traffic. Furthermore, the economic

repercussions of downtime brought on by distributed denial of service attacks highlight the urgent need for creative and robust mitigation approaches that are especially targeted to cloud web services.

The introduction of cloud computing has brought about a sea change in the manner in which companies and organizations install and manage their information technology infrastructure. When it comes to hosting online services and applications, cloud platforms are an appealing option since they provide scalability, flexibility, and cost-efficiency. On the other hand, due to the fact that cloud environments are centralized, they are also great targets for distributed denial of service assaults. Not only may a successful distributed denial of service assault (DDoS) disrupt the application that is being targeted, but it can also disturb other services and users that use the same cloud infrastructure, which can result in widespread downtime and financial losses. Therefore, mitigating distributed denial of service attacks in cloud web services is of the utmost importance in order to guarantee the ongoing availability of essential online resources and to keep the confidence and happiness of customers unchanged.

When it comes to detecting and filtering out malicious traffic, traditional DDoS mitigation approaches frequently rely on the deployment of specialized hardware appliances or software solutions at the network perimeter. Even if these strategies have the potential to be successful in on-premises systems, it is possible that they may not offer sufficient security in cloud-based deployments. The dynamic and elastic nature of cloud environments includes the provisioning and deprovisioning of resources on demand in order to meet varying workloads. Cloud environments are distinguished by their dynamic and elastic nature. Because of its dynamic nature, typical DDoS mitigation solutions may have difficulty scaling and adapting to abrupt surges in traffic volume during an attack. its presents a problem for these strategies.

Furthermore, it is impossible to emphasize the economic repercussions that distributed denial of service attacks have on cloud online services. The cost of downtime that can be incurred as a result of a successful distributed denial of service assault can be enormous. This cost includes not only direct financial losses but also harm to the reputation of the brand and the loyalty of customers. Furthermore, typical DDoS mitigation solutions frequently entail additional expenses in terms of the acquisition of hardware, the administration of that gear, and the maintenance of that hardware, which further exacerbates the economic effect of assaults of this nature. For this reason, there is an urgent requirement for DDoS mitigation strategies that are both cost-effective and especially adapted to cloud operating environments.

Innovative strategies for mitigating distributed denial of service attacks in cloud web services have been presented by researchers and practitioners as a reaction to these difficulties. There are several different approaches, one of which is the replication-based architecture, which includes instantiating numerous clones of the application that is being targeted across cloud nodes that are located in different geographic locations. This strategy offers the potential to successfully minimize the effects of distributed denial of service attacks (DDoS) by spreading bad traffic and preventing it from overwhelming any one instance of the application. This is accomplished by splitting the workload over numerous copies. Furthermore, replication-based architectures are able to dynamically modify the number of application copies in response to changing traffic patterns. This allows for maximum performance and resistance against distributed denial of service assaults. This is made possible by exploiting the scalability and elasticity of cloud resources.

The utilization of traffic redirection strategies is yet another viable strategy to mitigating distributed denial of service attacks conducted against cloud web services. Instead of focusing on identifying and filtering out malicious traffic, traffic redirection strategies concentrate on selectively diverting genuine traffic to sections of the infrastructure that are not impacted by the problem. This helps to reduce the impact that distributed denial of service attacks have on the application that is being attacked. In cloud systems, where traffic can be easily diverted through variable networking setups and load balancing methods, this strategy has the potential to be very successful. With this strategy, it is possible to guarantee uninterrupted availability and accessibility for genuine users, even in the face of prolonged distributed denial of service assaults, by intelligently routing traffic away from the application that is being attacked.

II. REVIEW OF LITERATURE

Songa, Asha (2022) In the current situation, cloud computing has developed into a marketable technology that enables customers to readily access resources over the internet. This access is based on a pay-per-use basis. In the capacity of services, these resources are made available to the client. Infrastructure as a Service, Platform as a Service, and Software as a Service are the three service models that are made available by the concept of cloud computing. The vast majority of information technology expenditures are based on cloud computing, which is a result of the enormous advancements that have been made in cloud computing technologies. Cloud computing is utilized by a large number of business applications, industrial applications, and enterprise companies that are committing to multi-cloud architectures. Security, on

the other hand, is the most important obstacle that requires greater attention. According to the findings of recent research, the availability of resources is the most significant security problem that cloud users face. Specifically, the Distributed Denial of Service assault is the primary factor that is affecting this availability issue. A more advanced version of the denial of service assault is known as the distributed denial of service attack. A Distributed Denial of Service attack is carried out with the primary objective of bringing down a particular service. This is accomplished by flooding the servers and network with erroneous packets, which ultimately results in the resources in a cloud being unavailable to users who are authorized to use them. Recently, cloud infrastructures have also been badly disrupted by denial of service assaults because of their widespread nature. Considering that the infrastructure level is responsible for providing the fundamental computing foundation for all cloud delivery models, the attacker will always attempt to breach the security at this level. The purpose of this article is to provide an overview of the various security techniques that may be utilized to defend against distributed denial of service attacks and cloud computing services.

Sahu, Shubham & Khare, Dr. (2020) In today's internet-driven society, a great deal of reliance is placed on cloud services. From email and social media to payment gateways and even traditional data storage for businesses, many rely on these platforms. However, one must ask: is it safe to entrust all sensitive information to these platforms? This paper will examine different DDOS (Distributed Denial of Service) attacks in cloud environments and the strategies used to mitigate them. The goal is to determine which methods are better, which ones could use some improvement, and which ones could harm your clients. After all, the primary goal of DDOS is to ensure that legitimate users have constant access while unauthorized users are blocked. In this article, we'll go over every possible DDOS assault and how to protect yourself from them.

Shahil, U et al., (2019) Cloud Applications that were built to be rich Internet applications that operate on the Internet (also known as the "Cloud") are referred to as computing, which is a common word that is shorthand for these apps. Through the use of cloud computing, it is possible to delegate duties to a mix of software and services that are delivered over a network. The term "cloud" refers to this network of servers. The use of cloud computing may assist organizations in transforming their existing server infrastructures into dynamic environments, allowing them to grow or reduce the capacity of their servers according to their specific needs. In the same manner that it offers services to clients, it also offers facilities to those who are engaged in malicious activity. Cloud computing is susceptible to a number of different forms of assaults, the most

known of which is the Distributed Denial of Service (DDoS) threat. There are many other types of dangers associated with cloud computing. This article presents a comprehensive study of a variety of distributed denial of service attacks and the preventative measures that may be taken against them. It assists in combating distributed denial of service attacks from cloud computing by utilizing techniques such as neif and honeypot.

Bakr, Ahmed et al., (2019) One of the most essential constituents of cloud systems is the availability of services. During the process of building the security architecture, the danger posed by Distributed Denial of Service (DDoS) attacks is a significant factor. A distributed denial of service attack that is successful might result in a deterioration of service or an outage altogether. While the approaches and strategies that are utilized in the cloud environment to combat distributed denial of service assaults (DDoS) are occasionally distinct from those that are utilized within traditional networks, there are also instances in which they are same. In this work, we are going to study the problems and mitigation approaches that are available against distributed denial of service attacks in the cloud, and we are going to compare these techniques in a cloud context. In addition to assisting in the establishment of future research and development projects, this survey will also serve to increase awareness of the techniques that have been presented.

Amjad, Aroosh et al., (2018) The technology had been completely updated up till this point thanks to cloud computing and its staggered and on-demand capabilities. On the foundations of the Pay-as-you-go idea, cloud users are entirely free to utilize the programs and tools that are available to them. The implementation of this idea resulted in a reduction in costs, as well as an increase in the reliability of the services. The ability to provide self-service on demand is among the most significant features of cloud computing organizations. Applications that are hosted in the cloud may be accessible from any location at any time and at a significantly lower cost. The cloud is able to give its customers with its fantastic on-demand services, but in addition to this, it is also able to survive the torturous security difficulties that are directed against the cloud. The servers are susceptible to a wide variety of assaults, each of which has the potential to crash them. DDoS attacks are among the most dangerous kind of attacks. The distributed denial of service assault (DDoS) was discussed in this study, along with the preventative strategy that, as a consequence, makes the server side less vulnerable. One of the scenarios is the delivery of millions and trillions of packets in the form of distributed denial of service attacks (DDoS) to cloud-based websites, which causes it to be differentiated across many hosts. Utilizing operating systems such as ParrotSec in order to

make the attack feasible are examples of this. During the last stage, the process involves the detection and prevention of the problem using the most efficient algorithms, specifically Naïve Bayes and Random forest. Additionally, the sorts of assaults on cloud computing were the major emphasis of this work.

Jaber, Aws et al., (2017) A Distributed Denial of Service assault, often known as a DDoS attack, is an attack that disrupts network performance to a significant degree. The precise placement of intrusion detection systems (IDS) and intrusion prevention systems (IPS) on networks is of major importance for obtaining optimal monitoring and attaining maximum effect in securing a system. Intrusion prevention systems (IPS) are tools for deployment. We suggest utilizing a principal component analysis (PCA) preprocessing and covariance analysis to partition the historical data of a network in order to make predictions about network abnormalities. After that, preliminary set-based rules are implemented for the purpose of predicting the behavior of future data in the network in order to provide the most effective response to the attacks that have been predicted. The approaches that have been developed are designed to be straightforward, enabling flexibility in the manner in which they are applied to networks and anticipating assaults while minimizing the amount of computer resources that are required.

Naseer, Junath & Iyenger, N Ch Sriman Narayana (2016) DDoS attacks pose a significant threat to cloud computing environments by targeting victims and effectively shutting down the Datacenter to prevent legitimate customers from accessing it. This study focuses on assessing various works and recommending the most suitable technique for adapting to a cloud environment in order to enhance detection accuracy. We have conducted a historical comparison of research studies on DDoS mitigation strategies in the context of cloud computing. The comparison includes an evaluation of the detection accuracy of five current research papers based on a synopsis of each.

Khadke, Ashwini et al., (2016) DDoS attacks target victim servers to deplete their resources and hinder the lawful use of their computing capabilities. DDoS assaults are frequently initiated by organized criminals, hacktivists, or other individuals, causing this kind of cybercrime to be a significant worry for several enterprises around. Performance is a crucial factor in cloud computing. The cloud is renowned for its abundant resources, establishing it as a prominent computing platform. This study aims to provide a collaborative defensive system to combat DDoS assaults in cloud environments. Our primary focus is on anomaly detection and filtering malicious traffic to effectively defend against DDoS assaults. We suggested an efficient detection strategy using a time-series

decomposition method to identify early-stage stealthy DDoS attacks. Furthermore, existing security solutions lack scalability for high-speed networks and struggle to protect against attacks from both faked and legitimate source addresses.

III. PROPOSED METHODOLOGY

As with our attackers, eight computers in the lab processed the assaults for the sake of testing, with a network delay ranging from three milliseconds to seven milliseconds. There were 25, 50, 75, or 100 instances of an attacking script running on each of these workstations. The script utilizes the curl command to flood the server with HTTP GET requests. This kind of experiment was repeated several times with consistent outcomes. Regarding hosting, every application made use of a dyno. Dynos are separate virtual server instances in the Heroku cloud that have 512 MB of RAM and four Intel Xeon X5550 CPUs running at 2.67GHz.

IV. RESULTS AND DISCUSSION

After that, an analysis was performed to determine how the DDoS mitigation will affect the response time, followed by the response rate and the overhead. In Figure 1 and Figure 2, with a confidence interval of 95%, it can be observed that the use of the suggested architecture resulted in a reduction in the amount of time required to respond to genuine needs. This is in contrast to Figure 2, which illustrates the amount of time required to fulfill the same number of requests that were made without our mechanism. Using architecture, the blacklist will prohibit an application from responding to the same client multiple times, so ensuring that the genuine client is able to access the new instance. This behavior happens because the blacklist prevents the program from replying to the same client numerous times.

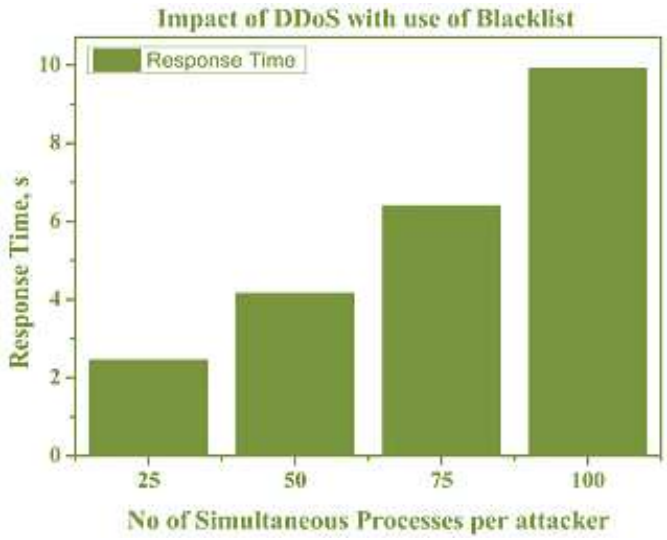

Figure 1: Response Time for Legitimate Customers with Blacklist Usage

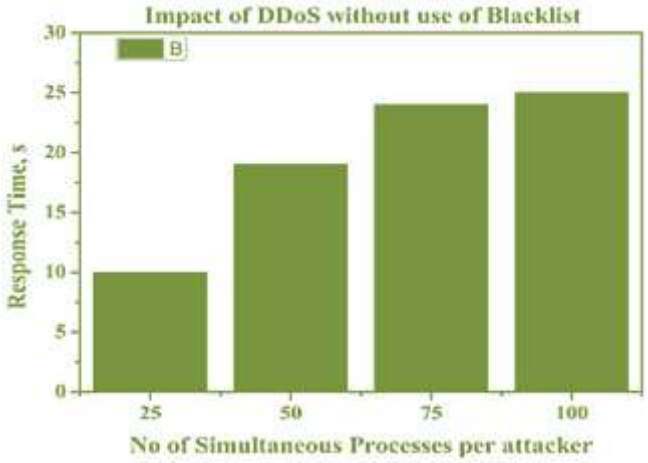

Figure 2: Response Time for Legitimate Customers without Blacklist Usage

Another statistic assessed is the success rate of receiving requested pages, seen in Figure 3 and Figure 4. A decrease in answers occurs only when blacklist filtering and subsequent redirection are not used. In some instances, the application sends a response to the attacker, who promptly disregards it and proceeds with the assault. Delivery rate is impacted by unresolved HTTP request timeouts when the blacklist is not used, since the program is preoccupied with assaulting requests.

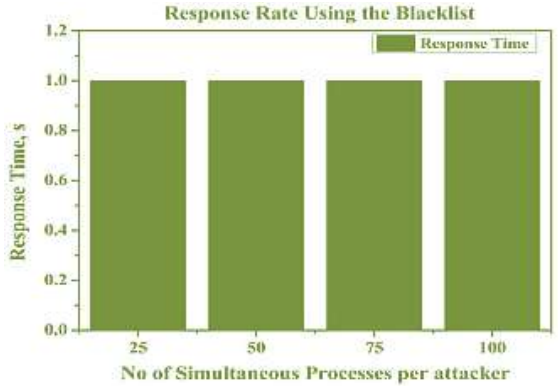

Figure 3: Server Response Rate for Legitimate Clients with Blacklist

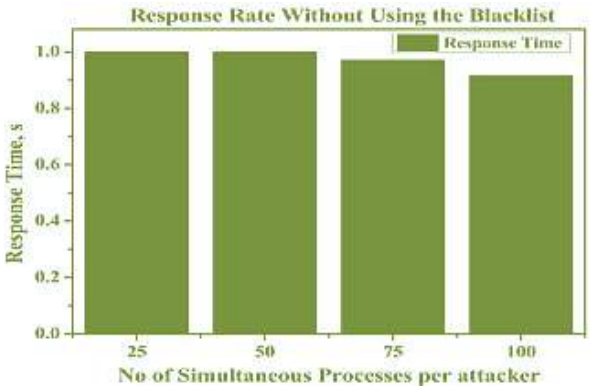

Figure 4: Server Response Rate for Legitimate Clients without Blacklist

V. CONCLUSION

Creating a cloud-based DDoS mitigation system with blacklist filtering is a major step forward in protecting web applications in cloud hosting. This new method utilizes the scalability and flexibility of cloud infrastructure together with a strong filtering system to efficiently address DDoS assaults. The design utilizes the cloud environment's intrinsic properties and a blacklist filtering method to provide legitimate users uninterrupted access to online apps while successfully preventing fraudulent traffic. Moreover, using a blacklist enables the effective detection and reduction of repeat offenders, thereby bolstering the system's overall resilience. The use of new designs is essential to sustain the availability and dependability of online applications in the midst of advancing cyber threats, particularly sophisticated DDoS assaults.

REFERENCES: -

1. Songa, Asha. (2022). A Review of DDoS Attacks and its Countermeasures in Cloud Computing. 10.1109/ISCON52037.2021.
2. Madan, Shefali & Anita, Anita & Ali, Ashif. (2022). DDoS attacks in cloud environment. International journal of health sciences. 5836-5847. 10.53730/ijhs.v6nS4.9457.
3. Sahu, Shubham & Khare, Dr. (2020). DDOS Attacks & Mitigation Techniques in Cloud Computing Environments. GEDRAG & ORGANISATIE REVIEW. 33. 10.37896/GOR33.02/246.
4. Bhardwaj, Akashdeep & Goundar, Sam. (2020). Cloud Computing Security Services to Mitigate DDoS Attacks. 10.5772/intechopen.92683.
5. Shahil, U & Deekshitha, Nuzha & Anam, Madeeha & Basthikodi, Mustafa & Publications, Research. (2019). DDOS Attacks in Cloud Computing and its Preventions. SSRN Electronic Journal. 6. 405-410.

6. Bakr, Ahmed & Ahmed, Abd El-Aziz & Hefny, Hesham. (2019). A Survey on Mitigation Techniques Against DDoS Attacks on Cloud Computing Architecture. Journal of Advanced Science. 28. 187-200.
7. Amjad, Aroosh & Alyas, Tahir & Farooq, Umer & Tariq, Muhammad. (2018). Detection and mitigation of DDoS attack in cloud computing using machine learning algorithm. ICST Transactions on Scalable Information Systems. 6. 159834. 10.4108/eai.29-7-2019.159834.
8. Jaber, Aws & Zolkipli, Mohamad & Majid, Mazlina & Anwar, Shahid. (2017). Methods for Preventing Distributed Denial of Service Attacks in Cloud Computing. Advanced Science Letters. 23. 5282-5285. 10.1166/asl.2017.7359.
9. Naseer, Junath & Iyenger, N Ch Sriman Narayana. (2016). A Review on Distributed Denial of Service (DDoS) Mitigation Techniques in Cloud Computing Environment. International Journal of Security and Its Applications. 10. 277-294. 10.14257/ijsia.2016.10.8.24.
10. Khadke, Ashwini & Madankar Ph.D, Mangala & Motghare, Manish. (2016). Review on mitigation of distributed Denial of Service (DDoS) attacks in cloud computing. 1-5. 10.1109/ISCO.2016.7726917.
11. Daffu, Preeti & Kaur, Amanpreet. (2016). Mitigation of DDoS attacks in cloud computing. 1-5. 10.1109/WECON.2016.7993478.
12. Bharot, Nitesh & Verma, Priyanka & Suraparaju, Veenadhari & Gupta, Sanjeev. (2016). Mitigating Distributed Denial of Service Attack in Cloud Computing Environment using Threshold based Technique. Indian Journal of Science and Technology. 9. 10.17485/ijst/2016/v9i38/98811.
13. Singh, Baldev & Panda, Surya. (2015). An Adaptive Approach to Mitigate Ddos Attacks in Cloud. International Journal of Advanced Computer Science and Applications. 6. 10.14569/IJACSA.2015.061006.
14. Modi, Krishna & Md, Abdul. (2014). Detection and Prevention of DDoS Attacks on the Cloud using Double-TCP Mechanism and HMM-based Architecture. International Journal of Cloud Computing and Services Science (IJ-CLOSER). 3. 10.11591/closer.v3i2.6086.
15. Mann, P. & Kumar, Dinesh. (2010). An Analytical Approach to Mitigate DDoS Attacks and improve Network Performance under Collaborative Software as a Service (SaaS) Cloud Computing Environment. CiiT International Journal of Networking & Communication Engineering.