©NIJSES
Publications

Open Access
ONLINE ISSN: 2992-5819
PRINT ISSN: 2992-6149

NEWPORT INTERNATIONAL JOURNAL OF SCIENTIFIC AND EXPERIMENTAL SCIENCES (NIJSES)

Volume 4 Issue 1

https://doi.org/10.59298/NIJSES/2023/10.4.1000

Understanding and Mitigating Cloud Computing Security Attacks: A Case of DDoS

[1]Joshua John, [2]Okonkwo Obikwelu,[3]Godspower Akawuku and [4]Chika Lilian Onyagu

[1]Institute of Computing & ICT, Ahmadu Bello University, Zaria, Nigeria

[2,3]Department of Computer Science, Faculty of Physical Sciences, Nnamdi Azikiwe University, Awka, Nigeria.

[4]Margaret Lawrence University, Umunede Delta state, Nigeria.

ABSTRACT

Although cloud computing is considered the most widespread technology. Despite of what it offers, the end users still suffers many challenges, especially related to its security issues such as vulnerability to malicious attacks such as Distributed Denial of Service attack (DDoS), that prevents accessing the internet. This paper is design to bring understanding and ways of mitigating DDoS attacks in cloud computing environment by leveraging from the pool of diverse solutions proffered that detect and prevent such attacks from harming network communication.

Keywords: Cloudflare, Firewall, Gateway, Webserver and Zombies

INTRODUCTION

Nowadays, everyone seems to be discussing about Cloud Computing. It is simply the shifting of technology to the cloud which have happened as a result of the move of traditional storage software to the Internet that took place progressively over the past ten years. Cloud computing could be conceived as a way of accessing compute and storage systems without actually owning and doing active management of the resources. It can be described basically as services hosted over the internet rather than onsite servers. These services can be accessed from remote locations and have advantages such as saving time, cost, space and electricity [1]. These services are: Infrastructure as a Service (IaaS): this is a third-party hosts elements of infrastructure, such as hardware, software, servers, and storage, also providing backup, security, and maintenance. Software as a Service (SaaS): Using the cloud, software such as an internet browser or application is able to become a usable tool and Platform as a Service (PaaS): The branch of cloud computing that allows users to develop, run, and manage applications, without having to get caught up in code, storage, and infrastructure and so on. In the recent years, adoption of cloud computing is increasing at an unprecedented pace [2].

We use cloud computing in our everyday life without even realizing it. Sending an email through an online service provider, listening to music, playing games or even just storing pictures and documents in our mobile devices constitute use of cloud computing. Unfortunately, as technology continues to grow, along with these advantages is a

Open Access
ONLINE ISSN: 2992-5819
PRINT ISSN: 2992-6149
key concern about security, which on daily basis is on the increase. Other concern of enforcing security is as a result of the proliferation of cloud devices arousing attractive target for attackers. Cybersecurity ventures expect global cybercrime costs to grow by 15% per year over the next five years, reaching US$10.5tn annually by 2025 [3, 4, 5].
There are several potential security attacks on cloud computing environment, such as, Denial of Service (DoS) attacks, authentication attacks, man-in-the-middle, wrapping attacks, malware-injection attacks, flooding attacks, and browser attacks, etc. The most major threat to cloud security is Distributed Denial of Service Attack (DDoS) [6]. A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic. A simple principle governs a DDoS attack: it takes down websites offline by consuming more resources or occupying all available bandwidth. Attackers with more hijacked cloud devices can consume more resources and launch a more damaging attack. The three main goals of attackers include: To cause consumption of limited resources; to cause destructive changes to network devices and to change or destroy configuration information. This is accomplished by exhausting the computing resources of the server by flooding the network bandwidth, which eventually leads to the non-availability of cloud services or resources, thereby, resulting to massive financial loss [7]. This kind of attack would lead to business lose or even discontinuance to various groups of users including government services, manufacturing, retailers, health care data support and it is launched for various reasons ranging from activism to state-sponsored disruption, with many attacks being carried out simply for profit. DDoS threats are not only becoming more dangerous, but attacks are also increasing in number. Experts predict that there was a 314% increase in overall attacks from the first half of 2022 to the first half of 2023 [8]. That number indicates that nearly every business will face a DDoS at some point, so preparing for this attack type should be at the top of your security to-do list [9, 10, 11]. Attackers seized the opportunity to create large botnets, to large complex DDoS attacks to disable or knock offline a target website. A botnet is a group of infected computers under the control of attackers used to perform various scams and cyber-attacks. Here, the attackers use malware to take control of vulnerable IoT devices to block legitimate users from accessing internet services by executing DDoS attacks.

Review of related work

The adoption of cloud computing has revolutionized data storage and processing. However, it has also introduced unique security concerns that should be understood to enable us improvise solutions to the challenges that could arise from misconfigurations, inadequate access controls, and vulnerabilities in cloud infrastructure which are also responsible for data breaches and unauthorized access to sensitive information. Many studies have been made of how to handle DDoS attacks and many elegant algorithms have been suggested. Some research deals with attack prevention and/or detection, some focus about how to filter DDoS attack and some research considers attack trace back. Here we discuss different research papers. For each of the following research papers we point out the proposed or deployed method and the scope of the method.
[12] proposed an IDS that made use of feature selection and a deep learning model for the categorization of DDoS attacks. They used the jumping gene-adapted NSGA-II algorithm to perform the feature selection. For the deep learning model, they used a convolutional neural network (CNN) integrated with long short-term memory (LSTM). The evaluation results showed the proposed approach to be effective against DDoS attacks.
For [13], real-time recognition of DDoS attacks using an ML classifier which relied on a distributed processing framework was the way to go. The DDoS detection rate was computed using the OpenStack based cloud testbed, through the Apache Spark architecture. A DL based IDS for DDoS attacks was proposed on the basis of 3 methods, namely Convolutional Neural Network (CNN), Deep Neural Network (DNN), and Recurrent Neural Network (RNN). The performance of each method was analyzed on the basis of 2 classification types (multiclass and binary), using 2 real traffic datasets- TON_IoT and CIC-DDoS2019. Based on this analysis, a DL based detection method for DoS attacks was proposed, which used the CNN method to carry out multiclass classification and binary classification, and used RNN method to improve efficiency.
[34], proposed a Mixed Kernel Extreme Learning Machine (MKELM) method integrating the ReliefF algorithm with nature inspired algorithms, for IDS. The MKELMs were developed to predict attacks, with the ReliefF algorithm providing inputs to the MKELM for selecting a suitable feature. The nature inspired algorithm determined the fitness function on the basis of kernel alignment, which was then used to build an optimum composite kernel in the MKELM. A novel approach was presented for evaluating resource consumption through 'scaling down' the resource i.e., through an improvement of the 'scale inside out' approaches. The presented approach utilized two modules- authentication model and elastic load balancing- to detect and mitigate DDoS attacks.
[15], proposed an ML-based model for the detection of DDoS attacks. The authors applied three different machine learning models: K-Nearest Neighbors (KNN), Random Forest (RF) and Naive Bayes (NB) classifier. The

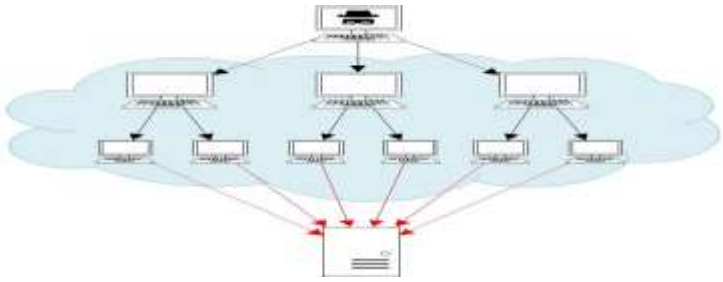
Open Access
ONLINE ISSN: 2992-5819
PRINT ISSN: 2992-6149

proposed approach can detect any type of DDoS attack in the network. The results of the proposed approach showed that the model can detect attacks with an average accuracy of 98.5%. Using the similar hybrid techniques, [16], proposed a hybrid detection method to DDoS attack, using entropy-based methods and custom-tailored methods. Custom tailored methods can only be used for the ones they are specially designed whereas anomaly-based methods can detect a wide range of anomalies and attack. The proposed hybrid method is combination of both feature-based and volume-based detection along with high and low rate attacks which gets a comparison between proposed and previously known methods. Some of the most common DDoS attacks are ICMP flood, SYN flood, DNS amplification attacks and the earlier Smurf Attack and Fraggle Attack. A script file was developed to test the following attacks: ICMP flood attack with a high packet rate attack on the specified target. Using this approach, a real-life botnet is simulated. As in a real-life situation, the attack does not start with all attackers at the same time, but instead with attackers initiated after a random delay period. [17] designed a technique for identifying cloud computing DDoS attacks. This technique employs machine learning algorithms such as support vector machine (SVM), naive Bayes (NB), and random forest (RF) for classification. The study was carried out using Tor Hammer as an attacking tool on a cloud environment, and a new dataset for the intrusion detection technique was developed.

[18], proposed a DDoS detection model that uses two algorithms, namely the power spectral density (PSD) and SVM algorithms, for low-rate DDoS attack classifications. The PSD algorithm calculates the entropy and then compares it with two predefined thresholds. To distinguish traffic patterns, the SVM algorithm is applied to investigate suspicious traffic and recognize similar patterns for the classifications. The experimental results showed that the proposed approach detected 99.19% of all low-rate DDoS attack traffic within a low complexity timeframe. The proposed work must be validated with recent datasets. [19], proposed a hybrid model of intrusion detection system in a cloud computing environment. The model detects violations, using the IP (Internet protocol)/MAC (Media access control) address at the point of entering the network of a cloud-based system. The methodology adopted is Object-Oriented Hypermedia Method (OOHDM) and the programming languages used is PHP, JavaScript, CSS and MySQL. The new system brings about a new method of detecting intruders by the combined use of IP/MAC address. [20] used Neural Networks and Data mining technique to detect DDOS attacks. This model needs less memory and claims that they have faster detection. The result shows that most of TCP attacks are detected. This system helps in detecting layer 7 (Application Layer) attacks and carry a lot of overhead. TTL value low and slow attacks. Packet monitoring in the cloud for TTL value said to have greater advantages in detecting DDOS attacks in the cloud, but it slows down the system performance which creates a limitation for cloud service providers.

Understanding How DDoS attack work?

The DDoS attacks are carried out with networks of Internet-connected machines. These networks consist of computers and other devices (such as cloud devices) which have been infected with malware, allowing them to be controlled remotely by an attacker. These individual devices are referred to as bots (or zombies), and a group of bots is called a botnet. Once a botnet has been established, the attacker is able to direct an attack by sending remote instructions to each bot. When a victim's server or network is targeted by the botnet, each bot sends requests to the target's IP address, potentially causing the server or network to become overwhelmed, resulting in a denial-of-service to normal traffic.



Target

Figure 1: A diagram of a DDoS attack performed with a botnet

Why DDoS is a problem and what does it impact?

Open Access
ONLINE ISSN: 2992-5819
PRINT ISSN: 2992-6149

i. Availability of your applications or websites: Attacks can last for hours or even days and block your users from normal usage of your applications.
ii. The financial impact on your business: Lost revenue, increased expenses on IT infrastructure provisioning.
iii. Security of your data: DDoS attacks can lead to data losses.
iv. The reputation of your applications: The name of your brand takes damage and loses credibility.

Some Types of DDOS Attacks in Cloud Computing Environments

Cloud computing continues to transform the way organizations use, store, and share data, applications, and workloads. It has also introduced a host of new security threats and challenges. With so much data going into the cloud and into public cloud services in particular these resources become natural targets for bad actors. As technology continues to grow, so will these security risks. A very typical example of a DoS or DDoS attack is designed to attack a single server, network or application with an overwhelming number of requests, packets or messages, so that the users of the server cannot connect to it or get the service that they expect from this server. DDoS attack becomes successful and this attack imposes some direct and indirect effects on the services and revenues. It has also led to distributed attacks such as IP spoofing, SYN flooding, buffer over-flow, ping of death, smurf, **U**DP flood attack, ICMP flood, the slowloris, Teardrop, and land attack are some examples of DDoS attacks in the cloud platforms [21].

Neptune (SYN Flood) Attack

Many operating systems have a limit on the number of concurrent half-open TCP connections (i.e. pending connections) on a particular port. Attackers exploit this limit to perform a SYN Flood attack **[22]**. A SYN Flood attack is performed by sending an enormous number of TCP SYNchronize (**SYN**) packets (often with false source IP address) to a server. After the server receives a TCP SYNchronize packet, it replies with a TCP SYNchronize-ACKnowledgement (**SYN-ACK**) packet and then waits to receive an ACKnowledge (**ACK**) packet. However, since the machine at the source IP address did not wish to open a TCP connection to this IP destination and destination port, it does not reply to the SYN-ACK packet. In this way the attacker exhausts the half -open connections limit of the target server's operating system. As a consequence, the server cannot respond to legitimate SYN packets, until the half-open connections are timed out [23]. The purpose of this attack is to reject any new connection from an authorized TCP client. Figure 2 shows the details of the SYN flood attack mechanism [24].

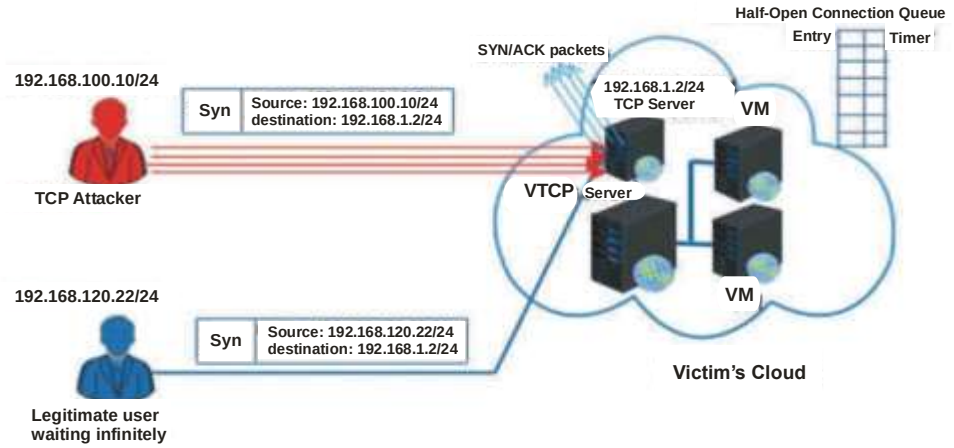


Figure 2: Neptune (SYN Flood) Attack
Source: http://www.riorey.com/types-of-ddos-attacks. Retrieved February 18, 2023

Smurf Attack

A smurf attack is a kind of amplifier attack. If broadcasting is enabled in a network device, then an attacker can exploit this to use the network as an amplifier (also called a 'smurf amplifier') and perform a DoS attack on a target. To perform a smurf attack, the attacker continuously sends ICMP PING requests to the broadcast address of the smurf amplifier network containing as their source IP address the IP address of the target. All of the hosts in the amplifier network reply to the PING requests and as a consequence the target starts receiving a potentially enormous number of ICMP PING response packets. These packets very quickly consume

Open Access
ONLINE ISSN: 2992-5819
PRINT ISSN: 2992-6149

the target's network bandwidth, preventing legitimate users from accessing that target's resources [25].

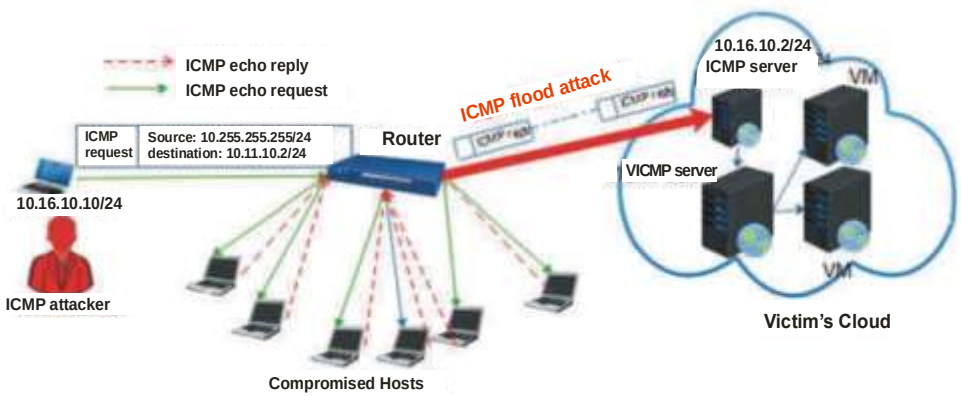


Figure 3: Smurf (ICMP Flood) Attack
Source: http://www.riorey.com/types-of-ddos-attacks. Retrieved February 19, 2023

Mail Bomb Attack

In this form of attack, the attacker continuously sends or urges others (zombies) to send a large number of successive e-mails to a target e-mail address in an attempt to crash the victim's mailbox or slow down the mail server. Every e-mail is sent with a different message to pass the spam filters. Figure 4 shows the architecture of the mail bomb attack mechanism [26].

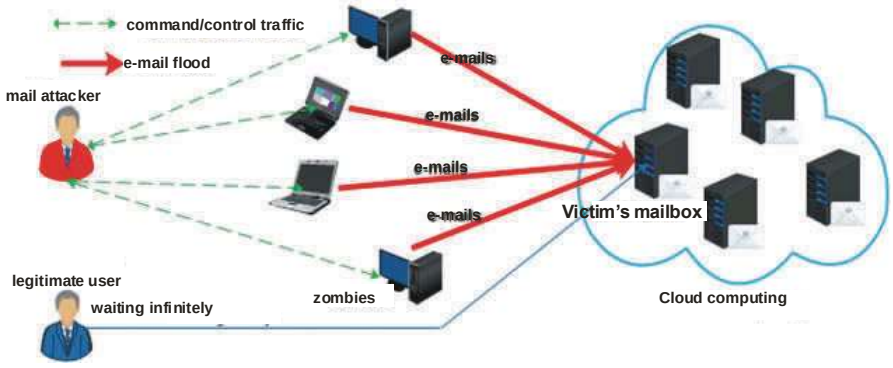


Figure 4: Mail Bomb Attack
Source: http://www.riorey.com/types-of-ddos-attacks. Retrieved February 20, 2023

Ping of Death

The default size of a PING packet is 32 bytes, but can be adjusted to be larger. However, many operating systems cannot handle a PING packet larger than 65535 bytes. Attackers exploit this by performing a "Ping of Death" attack by sending PING packets larger than 65535 bytes, through fragmentation, to a target. Since the operating system of the target cannot handle such a large packet, it will experience buffer overflow and could even crash. Preventing this attack can done by using a firewall to check what the PING packet size would be after reassembling the fragmented PING packets. Another method is to increase the size of the memory buffer to larger than 65535 bytes in order to avoid buffer overflow (DDoSProtection.Net.).

Open Access
ONLINE ISSN: 2992-5819
PRINT ISSN: 2992-6149

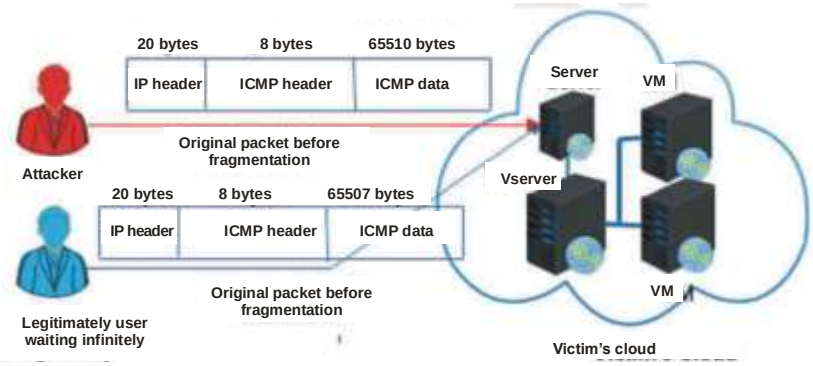


Figure 5: Ping of Death Attack
Source: http://www.riorey.com/types-of-ddos-attacks. Retrieved February 18, 2023

Teardrop

A teardrop is an old type of DoS attack. It exploits a weakness in early TCP implementations. Every network device fragments packets larger than the output link's maximum transmission unit (MTU). The receiver of these packets reassembles the fragmented packets. To perform a teardrop attack, the attacker sends fragmented IP packets with overlapping data in order to exploit the fact that the TCP/IP stack in operating systems (e.g. Windows 95, Windows 98) did not know how to handle such packets and the operating system would crash. However, today most operating system can correctly reassemble these fragments (DDoSProtection.Net.)

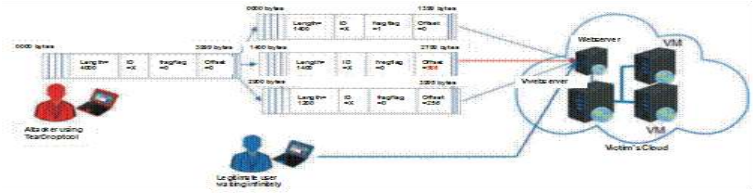
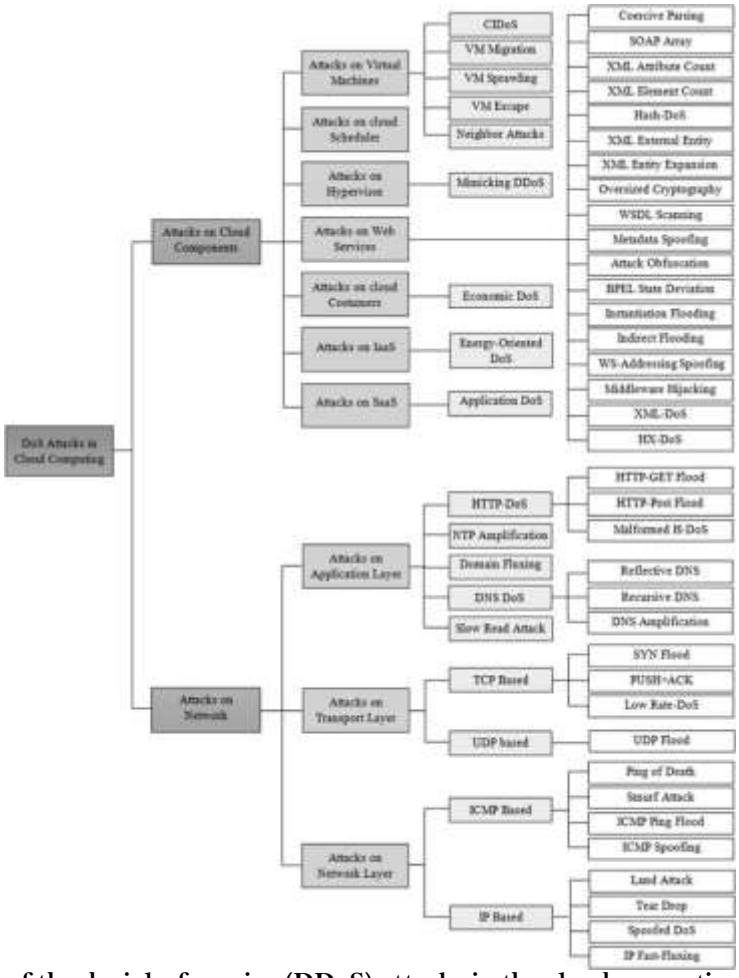


Figure 6: Teardrop Attack
Source: http://www.riorey.com/types-of-ddos-attacks. Retrieved February 22, 2023
Classification of the Denial-of-Service (DoS) Attacks in the Cloud Computing Environment.

Open Access
ONLINE ISSN: 2992-5819
PRINT ISSN: 2992-6149



Classification of the denial-of-service (DDoS) attacks in the cloud computing environment. Retrieved July 19, 2023, from https://onlinelibrary.wiley.com/doi/epdf/10.1002 /sec.1539

Different ways to mitigate DDoS security attacks in cloud computing

Today, cloud computing is growing even more popular than it was in the past. However, along with this growth in popularity come a growing number of security risks. As these grow more common, it is important that you know what to watch for so you can protect organization from DDoS attacks. The key concern in mitigating a DDoS attack is differentiating between attack traffic and normal traffic. In the modern Internet, DDoS traffic comes in many forms. The traffic can vary in design from un-spoofed single source attacks to complex and adaptive multi-vector attacks. A multi-vector DDoS attack uses multiple attack pathways in order to overwhelm a target in different ways, potentially distracting mitigation efforts on any one trajectory. An attack that targets multiple layers of the protocol stack at the same time, such as a DNS amplification (targeting layers 3/4) coupled with an HTTP flood (targeting layer 7) is an example of multi-vector DDoS. Mitigating a multi-vector DDoS attack requires a variety of strategies in order to counter different trajectories. The more complex the attack, the more likely it is that the attack traffic will be difficult to separate from normal traffic. The goal of the attacker is to blend in as much as possible, making mitigation efforts as inefficient as possible. Mitigation attempts that involve dropping or limiting traffic indiscriminately may throw good traffic out with the bad, and the attack may also modify and adapt to circumvent countermeasures. In order to overcome a complex attempt at disruption, a layered solution will give the greatest benefit.

Blackhole routing

Blackhole filtering is implemented without specific restriction criteria, both legitimate and malicious network traffic is routed to a null route, or blackhole, and dropped from the network. If an Internet property is

Open Access
ONLINE ISSN: 2992-5819
PRINT ISSN: 2992-6149

experiencing a DDoS attack, the property's Internet service provider (ISP) may send the entire site's traffic into a blackhole as a defense.

Rate limiting

Limiting the number of requests, a server will accept over a certain time window is also a way of mitigating denial-of-service attacks. While rate limiting is useful in slowing web scrapers from stealing content and for mitigating brute force login attempts, it alone will likely be insufficient to handle a complex DDoS attack effectively. Nevertheless, rate limiting is a useful component in an effective DDoS mitigation strategy.

Web application firewall

A Web Application Firewall (WAF) is a tool that can assist in mitigating a layer 7 DDoS attack. By putting a WAF between the Internet and an origin server, the WAF may act as a reverse proxy, protecting the targeted server from certain types of malicious traffic. By filtering requests based on a series of rules used to identify DDoS tools, layer 7 attacks can be impeded. One key value of an effective WAF is the ability to quickly implement custom rules in response to an attack.

Anycast network diffusion

This mitigation approach uses an Anycast network to scatter the attack traffic across a network of distributed servers to the point where the traffic is absorbed by the network. This approach spreads the impact of the distributed attack traffic to the point where it becomes manageable, diffusing any disruptive capability. The reliability of an Anycast network to mitigate a DDoS attack is dependent on the size of the attack and the size and efficiency of the network. An important part of the DDoS mitigation implemented by Cloudflare is the use of an Anycast distributed network. Cloudflare has a 100 Tbps network, which is an order of magnitude greater than the largest DDoS attack recorded.

Combine DDoS Protection Standard with Application Gateway Web Application Firewall for comprehensive protection

When combined with DDoS Protection Standard, Application Gateway web application firewall (WAF), or a third-party web application firewall deployed in a virtual network with a public IP, provides comprehensive protection for L3-L7 attacks on web and API assets.

Contribution of DDoS to understanding and mitigating cloud computing security attacks

The limited aim of DDoS attacks is killing a service availability and impair customer experience. Without cloud DDoS mitigation, which can distinguish valid traffic from malicious, it is unusual for cloud DDoS attacks go unnoticed.

DDOS PROTECTION TECHNIQUES

Reduce Attack Surface Area

One of the first techniques to mitigate DDoS attacks is to minimize the surface area that can be attacked thereby limiting the options for attackers and allowing you to build protections in a single place. We want to ensure that we do not expose our application or resources to ports, protocols or applications from where they do not expect any communication. Thus, minimizing the possible points of attack and letting us concentrate our mitigation efforts. In some cases, you can do this by placing your computation resources behind Content Distribution Networks (CDNs) or Load Balancers and restricting direct Internet traffic to certain parts of your infrastructure like your database servers. In other cases, you can use firewalls or Access Control Lists (ACLs) to control what traffic reaches your applications.

Plan for Scale

The two key considerations for mitigating large scale volumetric DDoS attacks are bandwidth (or transit) capacity and server capacity to absorb and mitigate attacks.

i) Transit capacity

When architecting your applications, make sure your hosting provider provides ample redundant Internet connectivity that allows you to handle large volumes of traffic. Since the ultimate objective of DDoS attacks is to affect the availability of your resources/applications, you should locate them, not only close to your end users but also to large Internet exchanges which will give your users easy access to your application even during high volumes of traffic. Additionally, web applications can go a step further by employing Content Distribution Networks (CDNs) and smart DNS resolution services which provide an additional layer of network infrastructure for serving content and resolving DNS queries from locations that are often closer to your end users.

Open Access
ONLINE ISSN: 2992-5819
PRINT ISSN: 2992-6149

ii) Server capacity

Most DDoS attacks are volumetric attacks that use up a lot of resources; it is, therefore, important that you can quickly scale up or down on your computation resources. You can either do this by running on larger computation resources or those with features like more extensive network interfaces or enhanced networking that support larger volumes. Additionally, it is also common to use load balancers to continually monitor and shift loads between resources to prevent overloading any one resource.

Know what normal and abnormal traffic is

Whenever we detect elevated levels of traffic hitting a host, the very baseline is to be able only to accept as much traffic as our host can handle without affecting availability. This concept is called rate limiting. More advanced protection techniques can go one step further and intelligently only accept traffic that is legitimate by analyzing the individual packets themselves. To do this, you need to understand the characteristics of good traffic that the target usually receives and be able to compare each packet against this baseline.

Deploy Firewalls for Sophisticated Application attacks

A good practice is to use a Web Application Firewall (WAF) against attacks, such as SQL injection or cross-site request forgery, that attempt to exploit vulnerability in your application itself. Additionally, due to the unique nature of these attacks, you should be able to easily create customized mitigations against illegitimate requests which could have characteristics like disguising as good traffic or coming from bad IPs, unexpected geographies, etc. At times it might also be helpful in mitigating attacks as they happen to get experienced support to study traffic patterns and create customized protections.

CONCLUSION

Though cloud computing has its pros and cons, on the whole, it is more beneficial than the harm it causes. Investment in cloud computing should be for the long term and the cloud computing domain is expected to evolve further in the future. Cloud computing has brought about a huge change in the way organizations operate. They have improved the entire process in a number of ways. We have seen a few of the major benefits that cloud computing has to offer.

WAYS FORWARD

Both outside attackers and insider threats (malicious or accidental) are substantial cloud security threats. It is essential to develop a comprehensive cloud security model to tackle the threat. With the appropriate tools and practices, you can significantly reduce your security risks.

REFERENCES

1. Niraj Suresh Katkamwar, Atharva Girish Puranik, and Purva Deshpande, "Securing Cloud Servers against Flooding Based DDoS Attacks," International Journal of Application or Innovation in Engineering & Management (IJ AI E M), vol. 1, pp. 50 – 55, Nov. 2012.
2. Varghese, B., & Buyya, R. (2017). "Next Generation Cloud Computing: New Trends and Research Directions," pp. 1–22
3. Qumer, S. M., & Ikrama, S. (2022). Poppy Gustafsson: redefining cybersecurity through AI. *The Case for Women*, 1-38.
4. Eze, V. H. U., Ugwu, C. N., & Ugwuanyi, I. C. (2023). A Study of Cyber Security Threats, Challenges in Different Fields and its Prospective Solutions : A Review. *INOSR Journal of Scientific Research*, *9*(1), 13–24.
5. Ogbonna, C. C., Eze, V. H. U., Ikechuwu, E. S., Okafor, O., Anichebe, O. C., & Oparaku, O. U. (2023). A Comprehensive Review of Artificial Neural Network Techniques Used for Smart Meter-Embedded forecasting System. *IDOSR Journal of Applied Science*, *8*(1), 13–24.
6. Gupta, B. B., & Misra, M. (2008). Combined Statistical Approach for Degrading and High Bandwidth Disruptive DDoS Attacks Detection. Proceedings of 16th IEEE International Conference on Networks, 10.1109/ICON.2008.4772654, Delhi, India.
7. Okafor, K. C., Okoye, J. A. & Ononiwu, G. (2016). "Vulnerability Bandwidth Distributed Cloud Computing Network: A QoS Perspective," *International Journal of Computer Applications*, vol. 138, no. 7, pp. 18–30, 2016.
8. Amber Jackson (2023). Cyber Magazine - The Digital Community for Global Cybersecurity Executives. Available on https://cybermagazine.com/cyber-security/zayo-group-confirms-ddos-attacks-in-2023-are-up-200 Retrieved 10th September, 2023
9. Andreja Velimirovic (2021). How to Prevent DDoS Attacks: 7 Tried-and-Tested Methods. Available on https://phoenixnap.com/blog/prevent-ddos-attacks Retrieved 10 August 2023

Open Access
ONLINE ISSN: 2992-5819
PRINT ISSN: 2992-6149

10. Eze, V. H. U., Iloanusi, O. N., Eze, M. C., & Osuagwu, C. C. (2017). Maximum power point tracking technique based on optimized adaptive differential conductance. *Cogent Engineering*, *4*(1). https://doi.org/10.1080/23311916.2017.1339336
11. Ogbonna, C. C., Eze, V. H. U., Ikechuwu, E. S., Okafor, O., Anichebe, O. C., & Oparaku, O. U. (2023). A Comprehensive Review of Artificial Neural Network Techniques Used for Smart Meter-Embedded forecasting System. *IDOSR Journal of Applied Science*, *8*(1), 13–24.
12. Roopak, M., Tian, G. Y. & Chambers, J. (2020) ``An intrusion detection system against DDoS attacks in IoT networks," in Proc. 10th Annu. Comput. Commun. Workshop Conf. (CCWC), Las Vegas, NV, USA, Jan. 2020, pp. 0562_0567, doi: 10.1109/CCWC47524.2020.9031206.
13. Gumaste, S. & Shinde, S. (2020). Detection of DDoS attacks in OpenStack-based private clouds using Apache spark. Journal of Telecommunications and Information Technology.
14. Shen, Y., Zheng, K., Wu, C. & Yang, Y. (2020). A Nature-inspired Multiple Kernel Extreme Learning Machine Model for Intrusion Detection. KSII Transactions on Internet and Information Systems (TIIS), 14(2), pp.702-723.
15. Priya, S.S., Sivaram, M., Yuvaraj, D., & Jayanthiladevi, A. (2020). "Machine learning based DDoS detection". In Proceedings of the 2020 International Conference on Emerging Smart Computing and Informatics (ESCI), Pune, India, 12–14; pp. 234–237.
16. Bojović, P.D., Bašičević, I., Ocovaj, S. & Popović, M. (2019). "A practical approach to detection of distributed denial-of-service attacks using a hybrid detection method". Computers & Electrical Engineering, 73, pp.84-96.
17. Wani, A.R., Rana, Q.P., Saxena, U., & Pandey, N. (2019). "Analysis and Detection of DDoS Attacks on Cloud Computing Environment using Machine Learning Techniques". In Proceedings of the Amity International Conference on Artificial Intelligence (AICAI), Dubai, United Arab Emirates, pp.4–6.
18. Zhang, N., Jaafar, F. &Malik, Y. (2019). ``Low-rate DoS attack detection using PSD based entropy and machine learning," in Proc. 6th IEEE Int.Conf. Cyber Secur. Cloud Comput. (CSCloud), 5th IEEE Int. Conf. Edge Comput. Scalable Cloud (EdgeCom), Paris, France, pp. 59_62, doi: 10.1109/CSCloud/EdgeCom.2019.00020.
19. Ogbomo-Odikayor. I. F., Anigbogu. S.O., Edebeatu Dom & Anigbogu, G.N. (2018). "A hybrid model of intrusion detection system in a cloud computing environment," International Research Journal of Advanced Engineering and Science, Volume 3, Issue 3, pp. 194-200.
20. Khalid, A. F. (2016). "An Overview of DDOS Attacks Detection and Prevention in the Cloud". International Journal of Applied Information Systems (IJAIS) – ISSN: 2249-0868 Foundation of Computer Science FCS, New York, USA Volume, pp.11 – No. 7 – www.ijais.org
21. Darwish, M., Ouda, A., & Capretz, L.F. (2013). Cloud-based DDoS attacks and defenses. In: Proceedings of the international conference on information society (i-Soci-ety), Toronto, ON, Canada, 24–26, pp.67–71. New York: IEEE.
22. Eddy, W. "TCP SYN Flooding Attacks and Common Mitigations,". Available on http://tools.ietf.org/html/rfc4987. Retrieved 17th September, 2023
23. Katkamwar, Niraj et al., 2012, Securing Cloud Servers against Flooding Based DDoS Attacks. International. Journal of Application or Innovation in Engineering & Management, Vol. 1, Issue 3, p. 51.
24. Chang, R. K. (2002). Defending against flooding-based distributed denial-of-service attacks: A tutorial. IEEE Communications Magazine, 40(10), 42–51. Available on doi:10.1109/MCOM.2002.1039856. Retrieved 20th September, 2019
25. National Institute of Standards and Technology (NIST). (2004). "Computer Security Incident Handling Guide".
26. Kim, W., Jeong, O. R., Chulyun, K. I. M. (2011). The dark side of the Internet: Attacks, costs and responses. Information Systems, 36(3), pp. 675–705. Available on doi:10.1016/j.is.2010.11.003. Retrieved 17th September, 2023.

©NIJSES
Publications

Open Access
ONLINE ISSN: 2992-5819
PRINT ISSN: 2992-6149

CITE AS: Joshua John, Okonkwo Obikwelu, Godspower Akawuku and Chika Lilian Onyagu (2023). Understanding and Mitigating Cloud Computing Security Attacks: A Case of DDoS. NEWPORT INTERNATIONAL JOURNAL OF SCIENTIFIC AND EXPERIMENTAL SCIENCES (NIJSES) 4(1) 25-35.
https://doi.org/10.59298/NIJSES/2023/10.4.1000