International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

Security Mechanisms of Distributed Denial-Of-Service (DDOS) Attack in Everything-as-a-Service (XaaS) - Survey

[1]Almerri Mubarak H M M J, [2]Lokman Mohd Fadzil
[1]National Advanced IPv6 Centre (NAv6)
University Sains Malaysia (USM)
Penang, Malaysia
e-mail: mubarakalmerri@student.usm.my
[2]National Advanced IPv6 Centre (NAv6)
University Sains Malaysia (USM)
Penang, Malaysia
e-mail: lokman.mohd.fadzil@usm.my

Abstract— This paper illustrates research on DDoS attack which overload targeted servers with traffic to render hosted resources inaccessible and unavailable. The attacks are increasingly being launched from multiple locations, gradually spreading over larger networks, consequently to obscure the attack origin. The precipitous cloud computing as the new 'anywhere anytime' paradigm, in the form of Everything-as-a-Service (XaaS), transforms these attack mechanisms to become progressively destructive, affecting Quality Of Service (QoS) performance. The attack vectors examination ranges from volumetric attack that flood network links, to application layer attack that target specific services, to protocol attack that exhaust network's resources, with evolving consequences. DDoS attacks mitigation in XaaS environments poses unique challenges. Current literature explores the limitations of traditional on-premise and XaaS-based mitigation techniques to instantaneously detect and mitigate malicious traffic. The role of intelligent analytics in distinguishing legitimate and malicious traffic are also being investigated by application of machine learning algorithms to safeguard against prospective interruptions to XaaS-based services' availability and reliability.

Keywords - Anomaly mitigation, attack vectors, cloud security, DDoS attacks, network monitoring, threat detection, XaaS

I. INTRODUCTION

A distributed denial-of-service attack or DDoS attack, is a form of a cyber-attack, where a number of distinct traffic, originating from many different sources, floods a target victim's server. The primary objective of DDoS attacks are to overload the target computer resources so that its services are inaccessible to normal users (Figure 1), thus enabling them to steal sensitive information. The second purpose is to conceal their identity by imitating legal online activities by engaging multiple agents to conduct such attack. A number of sophisticated strategies are required to mitigate this type of attack, as an attempt to block multiple attacks at the same time is logically insufficient.

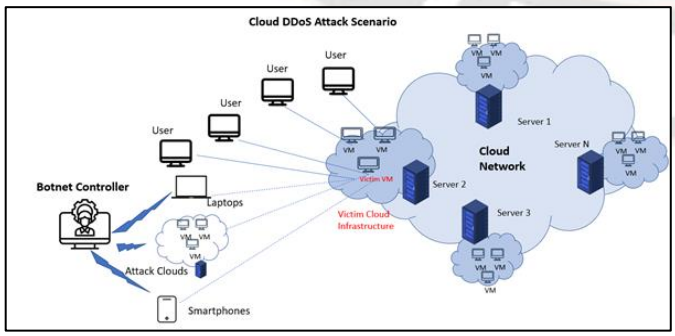

Figure 1. DDoS Attack In A Cloud Environment

II. LITERATURE REVIEW

A number of cloud-based DDoS attacks has been documented in literature. João et al.'s work demonstrated a method for detecting User Datagram Protocol (UDP) Flood DDoS assaults in a Software-Defined Networking (SDN)/Network Functions Virtualization (NFV) attack environment, similar to the cloud ecosystem. Their work uses two distinct unsupervised machine learning techniques with purpose to determine the stated algorithms' effectiveness in terms of DDoS attacks detection accuracy and efficiency. The two proposed algorithms had a 99% accuracy rate, with the k-means method 33% quicker than the fuzzy c-means, demonstrating its efficacy and scalability (de Almeida Neto et al., 2020).

AI Islam et al. proposed a detection technique to deal with two particular types of DDoS attacks: software exploits and flooding attacks. These types are classified based on packets volume and number of DDoS attackers. The detection is based on Recurrent Neural Network (RNN) classifier that differentiates between real and false data associated with the attack, including the Synchronize (SYN) Flood Attack covered in this research. This study focuses primarily on pure theoretical rather than practical basis due to dearth of analytical tests or findings (Al Islam & Sabrina, 2009).

A. Consequences Of A DDoS Attack

These attacks are considered highly significant based on DDoS historical attacks and impact on victim organizations' financial position and reputation (Table 1). The surveyed parameters vary significantly according to the victim's business nature, degree of disturbance, and the disruption duration. For each minute of downtime, prominent or heavily-visited Internet

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

sites, such as e-commerce, gambling, and web hosting portals stand to lose significantly in monetary value. Average cost of a single DDoS attack in the United States is approximately USD218,000 excluding ransomware, as reported by Corero's The Importance of Always-On DDoS Protection whitepaper (Newman, n.d.).

Panix, one of the world's earliest Internet service providers portal was taken down for several days in 1996 due to SYN flood attack, a method that eventually evolved into a standard DDoS attack mechanism, making it the first documented DDoS attack in literature. The ISP compiled the junk bulk emailers list and developed a tool that enables users to direct company's mail servers to reject all incoming messages, irrespective of sender, which blocking tool usage is optional per Schwinn-Clanton. In this regard, Panix customers are able to change their personal list to ban other bothersome email sources, or to reinstate sources from which they wish to receive emails. The actual loss was not recorded in literature, but anecdotally described as extremely huge (Nicholson, 2021).

One of the largest DDoS attacks in history took place in 2000, attributed to a 16-year-old Canadian miscreant nicknamed Mafiaboy, which forced countless large commercial websites to become offline (Long, 2012). As part of the attack, the attackers took control of dozens, if not hundreds of Internet sites, and reprogrammed them to broadcast voluminous data to target sites (Long, 2012). The attacks, dubbed as 'Rivolta' or 'riot' in Italian language, shut down major websites like Yahoo, eBay, CNN, Amazon, among others, and inflicted an estimated $1.7 billion losses ('MafiaBoy' Michael Calce Discusses the Mindset of a Hacker | Insight, n.d.).

Other reported cases to the Central Bank and relevant law enforcement includes November 2016 DDoS attacks on a number of Russian major banks. Sberbank successfully repelled a series of intense DDoS attacks orchestrated from a number of countries. In similar cases, identical attacks were also launched against Alf Bank, Moscow Bank (a subsidiary of VTB), Rosbank, and the Moscow Exchange, as reported by Vedomosti.

Attackers utilized multi-vector SYN flood attacks by sending a large number of SYN requests to the target's system. The HTTP flood attacks exploit HTTP GET or POST requests, masked as legitimate requests, to exhaust the server resources. Eventually the systems become unresponsive and unavailable (Russian Central Bank Reports DDoS-Attack on Major Banks - Business & Economy - TASS, 2016).

In October 2016, several world's leading websites, such as PayPal, Reddit, Twitter, Pinterest, Etsy, Spotify, Netflix, Comcast, and even Bluefin's PayConex came to a grinding halt for hours due to widespread Internet outage. Dyn, a New Hampshire-based company, one of the internet's major switchboards was down due to DDoS attacks. Hackers use botnets to overwhelm and shut down DNS servers with sheer volume of requests that apparently originated from a single infected device, such as a router or PC. The mechanism is similar to a phone operator struggling to answer simultaneous 100 phones calls, estimated to cost between $60 ~ $100 million [7]. Similarly, hackers launched a targeted DDOS attack on Lloyds Banking Group in 2017, forcing them to cease service for two days resulting in affected customers, as reported by Financial Times. TSB, a separate entity from Lloyds, was also affected [8].

According to a Kaspersky 2017 study, average cost of a DDoS assault for each small to medium-sized organization is approximately USD120,000. In this respect, major entities may need to spend more than $2 million per a single assault. Over time, lower estimates were obtained last year, with $100,000 for Small and Medium Sized Business (SMB) and $1.6 million for major businesses (The High Price Businesses Pay In Case of a DDoS Attack, 2021).

It is difficult to quantify the losses generated by a negative brand's reputation. As an example, 14,500 domains opted to migrate to another DNS provider after the catastrophic attack on Dyn in October of that fateful year. Approximately 8% of their entire income comes from this source [9].

Cisco anticipates that the overall number of DDoS attacks, including PCs, embedded systems, and Internet of Things (IoT) devices, to be more than double from 7.9 million in 2018 to more than 15 million by 2023 [10], demonstrating an increasing trend.

To address this, there is a need to find an optimal algorithm capable of accurately detecting major types of DDoS attacks to protect the systems from impending attacks. Accuracy in identifying this attack is critical. For example, a system with 95% detection rate represents a 5% infection rate. One infection may incur huge financial and customer loss, and potentially results in decline of the stock prices and customer confidence.

A number of algorithms have been investigated in numerous studies to detect 12 known types of DDoS attacks with its own features, clues, and context. The purpose of this study is to conduct a comparative analysis of the best algorithms for detecting DDoS attacks and modified algorithms in order to achieve the highest possible accuracy.

TABLE I. SSD PERFORMANCE

No	Year	Attack Name	Type of DDoS	Average Losses	Duration
1	1996	Panix	SYN Flood	Very Huge	Many Days
2	2000	Mafiaboy	DNS Flood	$1.7 Billion	Two Days
3	Nov 2016	Russia's Top 10 Financial Institutions	SYN Flood	$100K ~ $1.6 Million	
4	Oct 2016	Dyn	DNS Flood	$60 ~ $100 Million	~12 Hours
5	2017	Lloyds	DNS Flood	$100K ~ $1.6 Million	Two Days

B. DDoS Attack Mechanisms

DDoS attacks tactics are evolving rapidly in reaction to the ever-expanding Internet networks (Figure 2). Today's connected world enables people to communicate with one another easily, which, in turn, becoming more reliant on Internet technologies

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

for their day-to-day business. The human dependence on technology provides individuals and groups with ulterior motives to illegally generate enormous amounts of money by knocking down networks, services, and other appealing targets.

On the other hand, with the emergence of new technologies, the black market is able to quickly iterate their assault plans in response to changing efforts to counter their malicious attacks. When Internet's infrastructure was originally built, security was not given priority, hence its vulnerability to security risks. As the Internet has grown in popularity, these vulnerabilities are being exploited by organized threat actors motivated by financial gain.

Three distinct levels can be detected in DDoS attacks history. In July 22, 1999, University of Minnesota's system was attacked by a network of 114 compromised PCs executing the malicious Trin00 script. The infected machines sent huge quantities of data packets and overburdened the university's network, making this incident as the first documented DDoS attack in history. The technique, however, swiftly gained favor. Within months, Yahoo, Amazon, and CNN, all of which were already well-known, were all victims of the onslaught. Consider the fact that one of these assaults was carried out by a 15-year-old Canadian man. Following the aforementioned instances, blackhole or sinkhole approaches ceased to be successful at neutralizing such large-scale attacks [13].

The first half of the 2010s saw regular updates to records for DDoS assault power: 300 Gbps, 500 Gbps, and 620 Gbps, to mention a few. Hardware-assisted protection alone proved inadequate to reduce incoming threats from several botnets. Alternatives have to be considered. And then they appeared. The majority of the main network security vendors are nearing completion of their distributed filtering network architecture. Additionally, at the same time, the era of global cloud-based DDoS protection services started [13].

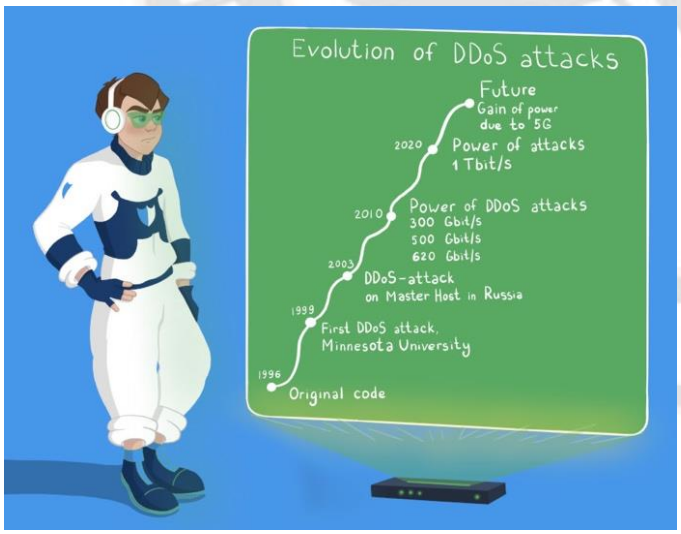

Figure 2. Evolution of DDoS attacks

C. Technology Used In The Attack

Since 2011, tremendous progress has been made in deep learning approaches, with the concept of artificial intelligence gaining center stage. Naturally, hacking groups are eager to capitalize on a good opportunity and quickly begin using these new techniques to enhance the efficacy of current distributed DDoS attacks. The technological barrier and expense of attacks continue to decrease as new technologies such as deep learning are introduced. Artificial intelligence-based malware automation and attack automation solutions are gaining popularity among hackers. In the cybersecurity world, more distributed DOS (DDoS) attacks driven by machine intelligence are on the horizon [14].

A Botnet is a group of computers linked to the Internet that have been wrangled and remotely controlled by an intruder, sometimes referred to as a Bot-master, for the purpose of running malicious applications. Additionally, it has a fair risk of leaking communications between the server and specific clients, providing additional security concerns. IRC-based bots are unsuccessful in the sense that the Botnet as a whole may be harmful if not maintained properly. As a consequence, it is conceivable that the whole IRC server will be shut down [15].

D. Technology Used For Defense

In the case of DDoS attacks against the Internet of Things, it is envisaged that a mature edge computing architecture would bridge the security gap in the IoT device landscape by providing consistent authentication and authorization, as well as standard network access for hardware devices. One advantage of edge computing is that it may be used to strengthen the security perimeters of Internet of Things devices. Another advantage is that it can be used to provide central governance at network edges, therefore strengthening the protection of edge devices. Additionally, blockchain technologies may be used to mitigate the impact of botnets, such as the Mirai botnet, which consists of tens of thousands of hacked Internet of Things devices. Certain malware obtains remote access to computers by using weak login credentials that are easily guessable or wrongly guessable. Our public keys have been encrypted and may be used in place of default login credentials as a consequence of the blockchain's storage of identity/public key pairs. As a result, public keys are difficult to decipher, allowing only device makers to use this method to install firmware on their devices. Finally, deep learning has been used to a number of tasks to boost the level of automation and the accuracy of detections. Also, deep neural network (DNN) was constructed and tested in experimental situations for the purpose of detecting distributed DOS attacks (DDoS) [14].

E. Types of DDoS Attacks

While it's always the intention of a distributed DOS (DDoS) attack to overwhelm the targeted system, how that's accomplished might vary. There are three main categories of distributed DOS attacks (What Is a DDoS Attack?, n.d.):

1) Application layer attacks

The application layer is responsible for data collection and organization. When a hacker uses many bots or devices to make identical requests to the server, they have launched an application layer attack. Most application layer attacks take the form of HTTP flood attacks, in which attackers repeatedly submit a wide variety of HTTP requests to a server from several IP addresses. Repeatedly requesting a server to produce PDF files is an illustration of this. It's impossible for the server to tell if it's under attack because the IP address and other identifiers are always different (Figure 3).

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

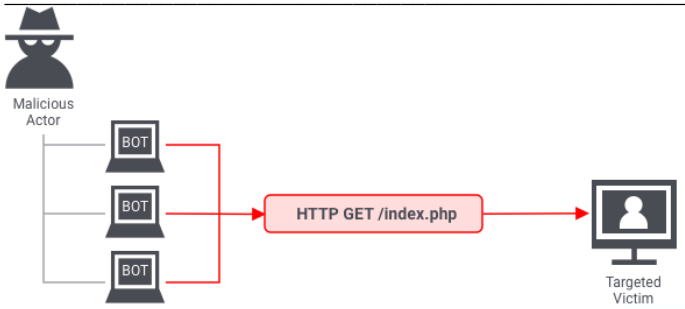

Figure 3. Example of a DNS DDoS application layer attack where a malicous actor mobilizes 3 nodes as 'zombie bots' to target and overwhelm a potential server usng HTTP protocol

2) Protocol attacks

Protocol attacks aim to deplete a server's or a network's resources, such as those of the server's or network's firewalls, routing engines, or load balancers. The SYN flood attack is one kind of protocol attack. There must be a TCP handshake between two computers before they can establish a safe line of communication. Attackers using faked IP addresses flood a server with SYN packets in a SYN flood attack. Each packet is acknowledged by the server (through SYN-ACKs), signaling that the server is ready for the client to finish the handshake. The server keeps waiting, but the client(s) never respond. After waiting for too many answers, it eventually freezes (Figure 4).

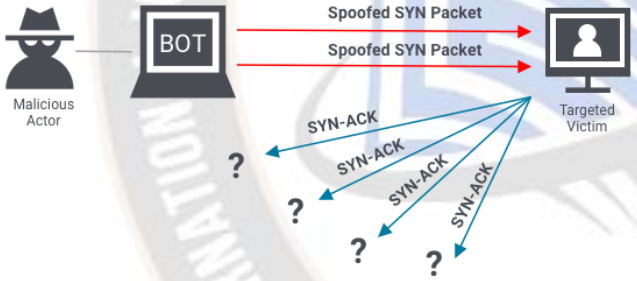

Figure 4. Example of a DNS DDoS protocol attack

3) *Volumetric attacks*

The goal of a volumetric attack is to overwhelm a server with traffic until it crashes. The DNS amplification attack is the most typical kind of volumetric attack. The attacker makes queries to a DNS server from the victim's faked IP address. The answer is subsequently transmitted by the DNS server to the requested server. This might cause chaos on the target server if done in large enough quantities, since the DNS answers would flood it.

4) *DDoS NTP Attack*

Amplification Attacks are attacks against target systems that use publicly accessible Network Time Protocol (NTP) servers, still in use today for computer systems' clocks synchronization, to flood them with UDP traffic (Figure 5) (NTP DDoS Vulnerability, 2014).

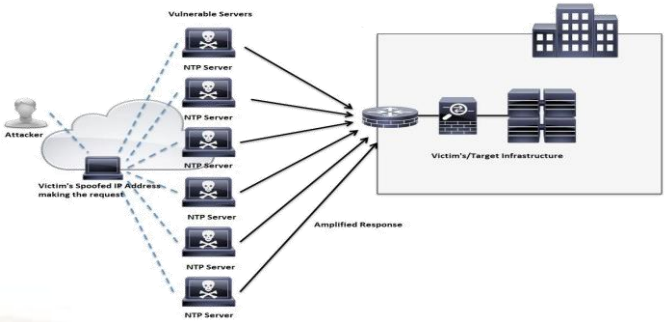

Figure 5. NTP Attack (NTP DDoS Vulnerability, 2014)

5) LDAP *DDoS Attack*

This attack involves three parties: the attacker, the Lightweight Directory Access Protocol (LDAP) server, and the victim. The relationship between the three parties is depicted in Figure 6 (Segal, 2017):

1. To obtain further information, the attacker sends small queries to a publicly accessible "amplifying" server.
2. An LDAP server generates massive (amplified) responses reflected by a destination server.

Figure 6. LDAP DDoS Attack (Segal, 2017)

6) NetBIOS *DDoS Attack*

Network-based operating systems (NetBIOS) are designed to enable programs running on separate computers to establish connections and sessions to share resources and locate one another over a local area network (LAN). Cybercriminals initiate a NetBIOS-based DDoS attack by sending many requests to the victim's host, resulting in a spike in network traffic. These queries have the originating IP substituted with the victim's IP address (spoofing), legitimizing them and mirroring the attack (INCIBE, 2021).

This attack generates between 2.56 and 3.85 times the amount of response traffic supplied to the target due to the initial queries submission (INCIBE, 2021). The protocol was developed by IBM and was integrated into early versions of Windows. It communicates over the 137 ports, and its primary victims were targets in the gaming and Web hosting sector (Cimpanu, 2015).

7) SNMP *DDoS Attack*

Simple Network Management Protocol (SNMP) reflection attacks can generate attack volumes of hundreds of gigabits per second, directed at attack targets from multiple broadband networks. As shown in Figure 7, the attacker device, using a spoofed IP address, is sending a flood of SNMP requests to many other devices. The victim IP is the spoofed IP used in the previous attack. As a result, responses will be sent to the victim's IP address, which may cause the device to become idle for some time (Bay, 2016).

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

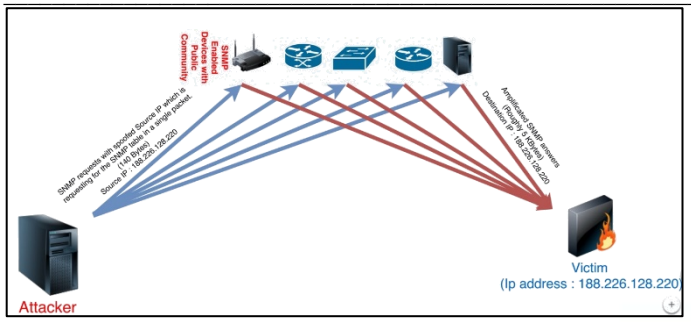

Figure 7. SNMP DDoS Attack (Bay, 2016)

8) SSDP *DDoS Attack*

Simple Service Discovery Protocol (SSDP) attacks are similar to reflection DDoS attacks. They leverage the Universal Plug and Play (UPnP) network protocols to send an amplified data stream to the target site (Figure 8). The following are the six steps involved in a typical SSDP DDoS assault:

1. The attacker begins by scanning plug-and-play devices that might be used as amplification factors.
2. As the attacker detects networked devices, they compile a list of all responding devices.
3. The attacker produces a UDP packet using the intended victim's faked IP address.
4. The attacker then utilizes a botnet to send a faked discovery packet to each plug-and-play device, requesting as much data as possible via the use of particular flags, most notably "ssdp:rootdevice" or "ssdp:all."
5. As a result, each device will respond to the targeted victim with data up to about 30 times the size of the attacker's request.
6. The target then receives a flood of traffic from all the devices and becomes overwhelmed, resulting in denial-of-service attacks against genuine traffic.

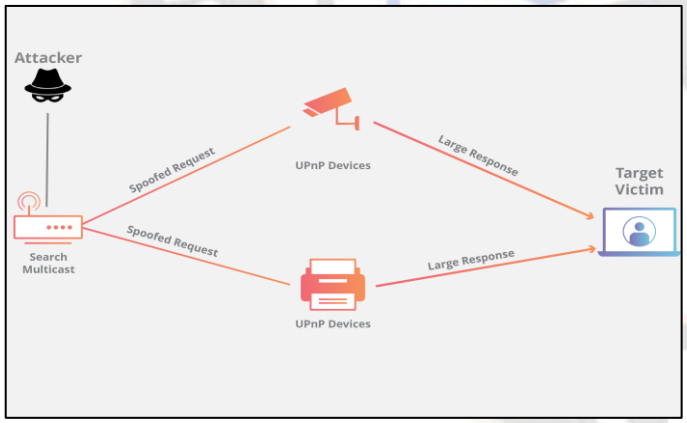

Figure 8. SSDP DDoS Attack (SSDP DDoS Attack, Cloudflare, n.d.)

F. Cloud Computing and Security

Security is the most important part of any kind of computing; therefore, it should come as no surprise that security concerns are also critical in cloud environments. As the cloud computing model may involve the storage of sensitive user data on both client-side and cloud servers, identity management and authentication are vital in cloud computing (Ahmed & Hossain, 2014).

Cloud computing, like any system, contains security flaws that may be exploited. The numerous security issues in a cloud computing system are listed below (Padhy et al., 2011):

Access to Servers & Applications: Administrative access must be handled via the Internet, which increases the risk and exposure. Frequently, user credentials are kept in the databases of cloud application providers and not as part of the enterprise IT infrastructure.

Data Transmission: In cloud environment most of the data is not encrypted in the processing time. Therefore, access controls are required to ensure the confidentiality and integrity of a system. Consequently, this leaves it vulnerable to Man-in-the-middle attacks.

Virtual Machine Security: It is challenging to create and maintain consistent security due to the dynamic nature and tendency for VM sprawl. Unknowingly, vulnerabilities or configuration problems may be transmitted.

Network Security: Shared, non-shared, public, private, local area, and wide area networks are all susceptible to security risks. Network security issues include DNS attacks, Sniffer attacks, reused IP addresses, and others.

Data Security: Hypertext Transfer Protocol is the most popularly used communication protocol for achieving cloud computing services (HTTP). Hypertext Transfer Protocol Secure (HTTPS) and Secure Shell (SSH) are widely used to protect sensitive information and maintain data integrity. In particular when business information is stored on the service provider's side.

Data Privacy: There should also be a privacy steering committee set up to help make decisions about data privacy. Organizations risk not following government rules, while cloud vendors who expose sensitive information risk legal trouble.

Data Integrity: Cloud storage is crucial for any data center, and integrity monitoring is necessary there because data corruption can occur at any storage level and with any type of media.

Data Location: Users of the cloud do not have knowledge of the datacenter's precise location, nor do they have authority over the data's physical access mechanisms.

Data Availability: It's a major issue for businesses that must operate without compromise to their missions and employees' safety. In the event of a service provider system failure, data owners whose data is stored on remote systems may experience data loss.

Data Segregation: When storing information on the cloud, users oftentimes do so in a communal setting where data from other customers is also stored. There is no guarantee that encryption will solve all issues with data isolation.

Security Policy and Compliance: Standard service providers go through regular external audits and must hold various security certifications. There will be an obvious loss of

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

trust in a cloud service provider if they fail to pass these security checks.

Patch management: The cloud's user-driven model could complicate patch management efforts. If a business sets up a Web server in the cloud using the vendor's provided templates, for instance, the vendor is no longer responsible for the server's patch management; instead, it falls under the purview of the subscriber.

Since we are only interested in DDoS attacks in this paper, we will attempt to focus solely on the security issues associated with them. The Distributed DOS (DDoS) attack is a severe danger to the availability of cloud-based infrastructure, which is one of the three primary difficulties in cloud security along with confidentiality and integrity. While DDoS attacks on single-tenant designs can be devastating, their potential impact is magnified with cloud computing, where infrastructure is shared by possibly millions of users.

G. DDoS Attacks in Cloud Computing Environment

All the three types of DDoS attack that were previously presented in Section 1.3 are applicable in cloud computing environment. In (Wani et al., 2019) HTTP DDoS attacks are detected among other DDoS attack types. HTTP DDoS attacks conducted at both high and low rates, with each scenario having a major effect on the victim.

The high-rate attacks bombards the victim with numerous requests, whereas in the low rate scenario, the victim's resources are depleted due to sluggish and compromised queries. The Intrusion Detection System SNORT was used to detect malicious network packets that matched specific rules. Several machine learning algorithms are used in this work: Overall accuracy was 99.7% for Support Vector Machine, 97.6% for Naive Bayes, and 98.0% for Random Forest when it came to classification.

Another type of DDoS attacks has been discussed in (Al-Hawawreh, 2017) were the statistical properties of TCP/IP headers used to assess and detect a SYN flood attacks in a virtual cloud environment. It is better to detect SYN flood attacks based on the TCP/IP header due to its low calculation costs and fast detection speed. the author has been used testbed environment which was conducted in (al Hawawreh et al., 2018).

For comparison among the classification algorithms, the accuracy and error rate of correct predictions were 99.98 percent and 0.020 for MLP-NN,99.16 percent and 0.840 for NB, and 98.205 percent and 1.795 for K-Means, 99.995 percent and 0.005 for J48.

In this research (He et al., 2017), the authors suggest a cloud-based machine learning-based DOS attack detection system on the source side. Using data collected from the cloud server's hypervisor and the virtual machines, this system blocks packets from leaving the server. We do a comprehensive analysis of the nine most popular machine learning algorithms available today. Through experimentation, they found that more than 99.7 percent of four distinct DOS attacks may be identified. One of these attacked was DNS Attack.

According to (Agrawal & Tapaswi, 2019), DDoS attacks may be divided into two categories in terms of frequency: brute-force and semantic. Brute-force attacks, also known as flooding or high-rate Distributed Denial-of-Service attacks, involve the sending of a large number of malicious requests with the intent of overloading the network capacity of the targeted cloud server. The enormous volume of attack traffic makes these kinds of attacks easy for defensive measures to spot.

Semantic attacks, also known as vulnerability attacks, target the flaws in the protocols themselves rather than the underlying infrastructure, such as a network or cloud storage. The adversary creates a little amount of malicious traffic directed towards a certain protocol or program. Low-rate distributed DDoS attacks are one type of DDoS attack. The slow-moving attack traffic blends in with the normal flow. For this reason, low-rate DDoS attacks are more difficult to detect than high-rate ones.

In this paper (X. Wang et al., 2009), a fast deterministic packet marking method (FDPM) is described for IP traceback in the face of distributed DOS attacks. This scheme employs a unique marking algorithm and vastly enhances IP traceback in two key respects: (1) FDPM may scale to massive, dispersed attacks with thousands of attackers because (2) the victim doesn't need to accommodate fragments for recovery; thus, it takes many packets to identify an ingress router with reduced false positives. FDPM is used in (Joshi et al., 2012) as a cloud protector and detected around 91% of with a miss rating of 9% on its training sets. As an additional note, there was a 3% decrease in variance when comparing the results to the test dataset (88% of attack traffic).

Most distributed DOS (DDoS) attacks against the cloud occur at the application level. The work presented by (Wani et al., 2019) was conducted in-house utilizing Tor Hammer to target the cloud infrastructure. In order to detect intrusions, the SNORT intrusion detection system was fed data that had been downloaded from the server. All of these assaults are detected using a freely available rule-based tool, however the default rules were modified to specifically recognize DDoS attacks. By specifying the necessary tuples, the output from the SNORT may be controlled. Weka's Support Vector Machine, Random Forest, and Naive Bayes were used to categorize the Snort database. Support Vector Machine, Random Forest, and Naive Bayes all had an accuracy of 99.7 percent in classification, but Naive Bayes was the least accurate at 98.0 percent.

III. Future Work

This study exclusively focuses on the theoretical aspect. Consequently, future research may involve the partial or complete implementation of this work in practical settings. This can be accomplished by simulating the 12 types of DDoS attacks, subsequently evaluating the performance of the three algorithms on these attack types, and comparing their efficacy in terms of speed and error rate.

IV. Conclusions

As a result, our analysis of security measures for Distributed Denial-of-Service (DDoS) attacks in the context of XaaS (Everything-as-a-Service) attacks highlights how crucial it is to handle the changing threat landscape in cloud services. Our research has shown that although XaaS has many advantages,

there are additional security risks associated with it, especially when dealing with DDoS attacks.

We have found that a diversified strategy is necessary after analyzing the many security tools available for XaaS setups to mitigate DDoS attacks. Proactive monitoring and response tactics, application-level security, and network-level defenses are all incorporated into this strategy. Moreover, in order to keep XaaS solutions secure and accessible, service providers, customers, and regulatory agencies must all be involved, which will be addressed in a future paper.

Advanced security mechanism research and development are becoming more and more necessary as XaaS adoption rises. It is apparent that the threat landscape will continue to change over time, and security protocols must change with it. The use of state-of-the-art technology, frequent training and awareness campaigns, and stakeholder collaboration are all essential elements of a comprehensive security plan to ward off DDoS attacks in cross-cloud infrastructure.

In conclusion, this survey emphasizes how difficult and important it is to handle security issues in XaaS, particularly when DDoS attacks are involved. In order to protect the XaaS ecosystem from DDoS attacks, we hope that the insights presented in this article will act as a basis for further investigation and the creation of strong security mechanisms for uninterrupted success and growth of XaaS-based services.

ACKNOWLEDGMENT

This paper is a partial outcome of the Intelligent Connected Streetlights research project work supported by the Renesas-USM industry matching grant as per MoA#A2021098 agreement with grant account no 7304.PNAV.6501256.R128.

REFERENCES

[1] Newman, S. (2021, October 17). The True Cost of DDoS Attacks. Retrieved from Infosecurity-Magazine: https://www.infosecurity-magazine.com/opinions/the-true-cost-of-ddos-attacks/

[2] Nicholson, P. (2021, 07 21). Five Most Famous DDoS Attacks and Then Some. Retrieved from A10: https://www.a10networks.com/blog/5-most-famous-ddos-attacks/

[3] Long, T. (2012, Feb 07). Feb. 7, 2000: Mafiaboy's Moment. Retrieved from Wired: https://www.wired.com/2012/02/feb-7-2000-mafiaboys-moment/

[4] Insight. (2018, Feb 28). Retrieved from 'MafiaBoy' Michael Calce Discusses the Mindset of a Hacker: https://www.insight.com/en_US/content-and-resources/2018/02282018-mafiaboy-michael-calce-discusses-the-mindset-of-a-hacker.html

[5] Russian Central Bank reports DDoS-attack on major banks. (2016, November 10). Retrieved 12 11, 2021, from TASS: https://tass.com/economy/911426

[6] The High Price Businesses Pay In Case of a DDoS Attack. (2021, February 04). Retrieved from The European Business Review : https://www.europeanbusinessreview.com/the-high-price-businesses-pay-in-case-of-a-ddos-attack/

[7] The Attack that Almost Took Down the Internet. (2016, 10 27). Retrieved from Bluefin: https://www.bluefin.com/bluefin-news/attack-almost-took-down-internet/

[8] Lloyds Bank suffered 2-day-long DDoS attack. (2017). Retrieved from Information Age: https://www.information-age.com/lloyds-bank-suffered-2-day-long-ddos-attack-123464123/

[9] Felter, B. (2017, 02 10). Larger more frequent attacks increase business risk requiring 'Smarter' Solutions. Retrieved from VXchnge: https://www.vxchnge.com/blog/ddos-attacks-set-increase-2017

[10] Cisco Annual Internet Report (2018–2023) White Paper. (2020, 03 09). Retrieved from Cisco: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html

[11] Neto, J. d., Souza, L. S., & Lima Ribeiro, A. d. (2020). Comparative Analysis between the k-means and Fuzzy c-means Algorithms to Detect UDP Flood DDoS Attack on a SDN/NFV Environment. 16th International Conference on Web Information Systems and Technologies (pp. 105-112). WEBIST 2020.

[12] AI Islam, A. A., & Sabrina, T. (2009). Detection of various DOS and Distributed DOS Attacks using RNN Ensemble. 12th International Conference on Computer and Information Technology (pp. 603-608). Dhaka, Bangladesh: IEEE.

[13] Evolution of DDoS Attacks. (2021, July 16). Retrieved from Storm Wall: https://stormwall.network/blog-analytics-evolution-of-DDoS-Attacks

[14] Hao, M. (2019, July 01). Nsfocusglobal. Retrieved from DDoS in the Past Decade: https://nsfocusglobal.com/ddos-in-the-past-decade/

[15] Tuan, T. A., Long, H. V., Son , L. H., Kumar , R., Priyadarshini , I., Thi , N., & Son, K. (2019, 11 20). Performance evaluation of Botnet DDoS attack detection using machine learning. Evolutionary Intelligence. Germany: Springer-Verlag GmbH Germany, part of Springer Nature 2019.