A Review on Defense Mechanisms Against Distributed Denial of Service (DDoS) Attacks on Cloud Computing

Dhefaf Radain
Faculty of Computer and Information Technology
King Abdulaziz University
Jeddah, Saudi Arabia
https://orcid.org/0000-0002-1769-9167

Saliha Almalki
Faculty of Computer and Information Technology
King Abdulaziz University
Jeddah, Saudi Arabia
https://orcid.org/0000-0002-8042-1563

Hana Alsaadi
Faculty of Computer and Information Technology
King Abdulaziz University
Jeddah, Saudi Arabia
https://orcid.org/0000-0001-5096-3655

Shaimaa Salama
Faculty of Computer and Information Technology
King Abdulaziz University
Jeddah, Saudi Arabia
ssalama@kau.edu.sa

2021 International Conference of Women in Data Science at Taif University (WiDSTaif) | 978-1-6654-4948-9/21/$31.00 ©2021 IEEE | DOI: 10.1109/WIDSTAIF52235.2021.9430220

***Abstract*—Recently, businesses and organizations are depending on the cloud to provide their services. The important aspects that need to be taken into consideration when it comes to the cloud are availability, confidentiality, accessibility, and integrity. The severity of the consequences of any attack on the cloud could lead to downtime which as a result will cause financial and reputational loss. An important security matter that targets cloud computing is the Denial of Service (DoS) attack. The Distributed Denial of Service (DDoS) attack is an improved version of the DoS attack which has targeted the cloud infrastructures heavily in recent years. This paper discusses the cloud computing infrastructure and the DDoS attack scenario and its effect on cloud computing. Cloud features that enable the DDoS attacks to be launched are highlighted along with the description of the different types of DDoS attacks. Moreover, several defense mechanisms are stated including prevention, detection, and mitigation techniques. This study shows that some DDoS attacks cannot be prevented, detected, or mitigated. These are the ones launched from a legitimate IP address or have a signature not stored in the signature database. Moreover, the defense mechanism may not be able to distinguish the high traffic caused by an attack from the ones caused by an actual heavy legitimate traffic to know when to add extra resources. Additionally, some techniques work remotely which may slow the defense mechanism, and others are provided by third parties and the service owners may have problems sharing the control with them. Keywords— Distributed Denial of Service (DDoS) attack; Cloud Computing; DDoS attacks Defense mechanisms.**

I. INTRODUCTION

Cloud computing is a promising technology that provides the users with many great services [1] as well as scalability and effectiveness of the cost [2]. As a result, it has become a trend [3] Mainly it runs a suitable platform for the users to access the cloud recourses and services over the internet [1]. Due to its advantages which include on-demand services, pay-as-you-go, and low-cost, it became a strong competitor with the traditional IT implementations[4]. On-demand service providing is the main goal of cloud computing [5]. However, there are lots of security issues, threats, and challenges connected to the use of cloud computing [1].

One of these threats is DDoS attack which is not new, but they are an important security issue that must considered [2, 6].

The number of reported DDoS attacks is very high and continues to rise, which makes this type of attack the most important threat among others[4, 7]. The Internet came across major incidents of DDoS attacks, these attacks are continuing to grow every year and become more sophisticated [8]. More than 20% of worldwide enterprises had at least one DDoS attack in their infrastructure [4].

Highlighting the DDoS attacks is the aim of this paper particularly on the cloud environment. It shows the most known DDoS attacks and discusses the different defense mechanisms against them.

This paper is organized as follows. An overview of cloud computing and DDoS attacks and the main reason behind the massive use of cloud computing is provided in section II. Section III describes the scenario of the DDoS attack on cloud computing starting from choosing the agents , the victim to describe the actual attack while highlighting the cloud features that enable the DDoS attacks to take place. Additionally, some types of DDoS attacks are discussed in this section as well. In Section IV the well-known and most used defense mechanisms against DDoS attacks are discussed. Some prevention, detection, and mitigation techniques are explained in detail. Section V is dedicated to the different proposed solutions against DDoS attacks that took place in other research papers but are not well known to be applied. A comparison between the different proposed approaches of defense mechanisms is provided at the end of the section. Section VII and Section VIII present the discussion and the conclusion, respectively.

II. OVERVIEW OF CLOUD COMPUTING AND DDOS ATTACK

DDoS attacks are major threats that attack traditional network architectures as well as future architectures such as Software Defines Networks (SDN), Vehicular Networking, Cloud Computing, Edge/Fog Computing, Named Data Networks (NDN), and Smart Grid Systems [8].

This section includes an overview of cloud computing. The main reasons and the major concerns behind using it. An overview of DDoS attacks is also provided in this section.

A. Overview of Cloud computing

Cloud computing services are provided to users in different forms: platforms, software, or infrastructure[5, 9]. Its main objective is to utilize the hardware in the best possible way and take off the maintenance burden from the user. As a result, governments and industries transferred most of their infrastructure into cloud computing if not the whole of it [4, 9].

Security concerns while using the cloud infrastructure are different from those when using non-cloud infrastructure

978-1-6654-4948-9/21/$31.00 ©2021 IEEE

because the data is located in a cloud server in a remote location with no control on it [4].

B. *Overview on DDoS Attacks*

The DDoS attack is a special type of DoS attack where several controlled systems target the victim[10, 11]. These systems are called Bots [12] or Agents [13]. They are chosen based on some vulnerabilities they have in their networks and a malicious program called Trojan Horse is installed on them. They can be used for executing a DDoS attack as well as stealing data, spam delivery, and give access to attackers to link to a victim [2]. The attackers' goal is to overload the victim with fake requests to become unavailable [1].

The attacks could be classified as Low-Rate (LDDoS) and High-Rate (HDDoS) [11] which are also called brute-force and semantic attacks [2]. The volume of the high-rate attack is more than 500 Gbps and aims to either interrupt the connectivity of the legitimate users which is called the Bandwidth Depletion Attack or make the services of the cloud unavailable and this is called Recourse Depletion Attack [5]. While the volume of the low rate is in Mbps and the aim is not to stop the cloud services from doing their normal operations but to decrease the Quality-of-Service (QoS) for the legitimate clients of the cloud [1].

The impact of these attacks could be direct or indirect [4]. The direct effect may be business and revenue loss [10] while the indirect effects could be the extra consumption of energy, components damage, the cost of mitigation, and the reputational loss [4]. Another major impact is the confidentiality of the victim's server and the use of its data to perform malicious actions by the attacker [5].

III. The Scenario of DDoS Attack on Cloud Computing

In this section, the scenario of the DDoS attack on the cloud will be described. Moreover, the cloud features that help the attacker to launch an attack will be highlighted as well in detail while briefly explaining some of the most common DDoS attacks.

In the beginning, the attacker starts by choosing the Botnets that will be used to start the DDoS attack and the target machine which is called the victim. These Botnets are controlled remotely by the attacker who is called the Bot-master by sending the command to the group of compromised systems[13] [12], also known as Zombies [13], to start sending useless packets to the victim. The victim will be overwhelmed with the huge coming traffic which will result in the inaccessibility of the services to the authentic users [12].

A DDoS attack is launched through a virtual machine (VM) from the same cloud infrastructure [13]. The attacker reaches the VM through the node, which is a machine under the control of the attacker through the Command and Control (C&C) server [1, 2]. Bots and trojans are established over the internet to start the DDoS attack by targeting the VM and directing a large amount of false requests to the infrastructure of the cloud, as shown in Fig. 1, which cause the web services to be down. Multiple attacks may be launched simultaneously and affect more than one cloud infrastructure at the same time [13].

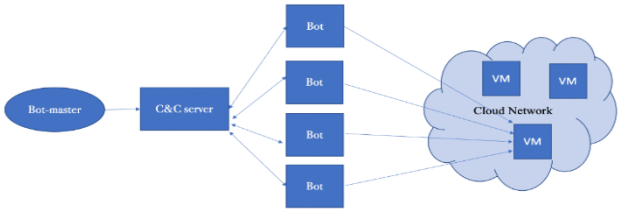

Fig 1. DDoS attack on the cloud infrastructure

Cloud computing technology became a success because of three main features. They are auto-scaling, on-demand resource billing (pay-as-you-go), and multi-tenancy. However, these are the same features that made the DDoS attacks successful in the cloud environment [4].

The feature of auto-scaling of the cloud would take the fake requests being sent to the victim as an overload, because of the massive utilization of the hardware in the server of the victim and starts to add more recourses to the server. It will keep adding resources as long as there no mitigation system available to stop the attack [4]. Moreover, since the cloud infrastructure works in a multi-tenant environment, any damage posed to any of the shared resources will cause the whole tenant to be under attack [10]. This situation will last until all the resources are totally consumed or the cloud service provider pays to provide extra resources for the users. In the end, the cloud server will reach the point of "Service Denial" and all the cloud services provided for the users will be lost. The situation will lead to on-demand resource billing which will cause an economic loss because of the over-budget the cloud service provider (CSP) face [4].

The different types of DDoS attacks could be launches using different packets such as TCP, ICMP, and UDP [2].

In the SYN flooding attack, the victim replies with SYN-ACK to the flood of SYN requests coming from the attacker. The attacker never responds to the ACK causing it to overload the victim and lead to denial of service[14, 15]. In the Ping of death, the attacker sends large size packets of malicious pings to the victim which appear to be irrelevant when they are reformed at the destination. The packets are dropped in the end, but the bandwidth was already consumed denying the legitimate users from accessing the server [14]. The LAND attack is launched by directing a larger number of TCP packets with the same IP of the source and the destination. This causes the victim to reply to itself repeatedly to the point the server is down [16].

Ping flood attack is launched using an ICMP packet [8] by sending a large number of echo requests continuously without waiting for a reply. This consumes the bandwidth and leads to server shutdown [6, 14, 15] The Smurf attack is achieved by broadcasting an ICMP echo to all the computers on the internet via a spoofed IP address which is the victim's address. The responses of the requests start the attack by targeting the victim with their ping response. This results in flooding the victim and causes a denial of service [6].

In a UDP flood attack, the attacker launches a huge number of UDP packets towards the victim's infrastructure. The victim finds the destination unreachable when it looks

for the application. The process will continue until the server becomes unavailable to legitimate users[6, 14, 15].

DDoS attacks took place against the cloud for different businesses. In June 1998 Flash crowd attacked the FIFA website [6] and that made the website services unreachable to legitimate users during the World Cup. While In March 2014, a DDoS attack affected the DNS setup of the RackSpace Domain Name System [2, 4, 17]. In addition, in March 2013, at Microsoft Datacenters [10], a DNS flood attack was launched against the Spamhaus cause to prevent the services with 300 Gbps of traffic. Amazon EC2 server was also affected by a DDoS attack in December 2014, causing a heavy downtime that led to business loss [2, 4, 17]. Additionally, in March 2015 Greatfire.org based on Amazon EC2 was blocked users from accessong to the site [18]. In December 2015 [4, 17], Microsoft and Sony gaming servers were attacked by Lizard Squad. Dyn was the target in October 2016 [8], thousands of Internet of Things (IoT) devices controlled by the Mirai botnet originated the attack. The traffic rate was around 1.2 Tbps. Even GitHub was hit by a DDoS attack in March 2018, with total traffic exceeding 1.7 Tbps [8].

IV. Taxonomy of DDoS Attacks Defense Mechanisms

Since the DDoS attacks have the highest probability of making the resources unavailable from all other types of threats [10], the defense mechanisms against them must be robust enough to match the sophistication of the attacks [8].

In this section, we provide a taxonomy of the well-known and most used defense mechanisms of DDoS attacks, including prevention, detection, and mitigation. Fig. 2 presents a summarization of these methods.

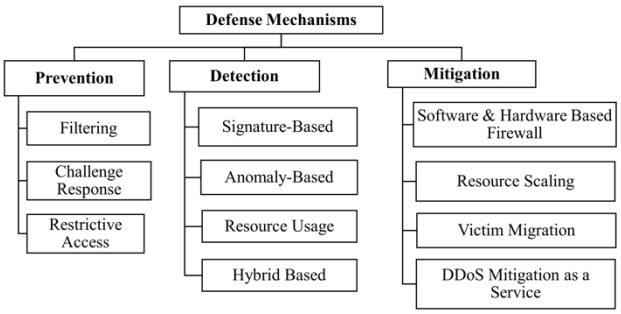

Fig 1. DDoS attack defense mechanisms

A. Prevention of DDoS Attack on Cloud Computing

The meaning of Prevention is to protect the cloud resources and services from the DDoS attack proactively. DDoS attack prevention is built on the management of the network traffic, rescheduling, and hidden proxy/server [1]. Some of these prevention techniques are presented as follow:

1. Filtering: There are six types of filtering methods that are used to prevent the attacks before they occur [13]. These types are:
   - Ingress filtering: Uses the routers for stopping the incoming packets from a spoofed IP address [13].
   - Egress filtering: Enables the packets with a legitimate IP address in a specific network range to leave the network using an outbound filter [13].
   - Route-based distributed packet filtering: Used for capturing and filtering the IP addresses of the spoofed packets and stop the attack using the router's information and the IP traceback [13].
   - Secure Overlay Services (SOS): If the incoming packets are from a legitimate server, they will be considered valid packets. The Overlay is used to filter the other packets. Access to the overlay network requires the clients to authenticate their identity by using replicated access points viz. SOAP [13].
   - History-based IP filtering: Creates an IP address database (IAD) during normal traffic to store the history of IP addresses that are frequently used by the destination. This approach is used to prevent DDoS attacks by ignoring any IP address that does not exist in IAD. Hash and bloom techniques are used to search for the source IP address in IAD. This method is not useful when the attackers use a legitimate IP to lunch the DDoS attacks [19, 20].
   - Source Address Validity Enforcement Protocol (SAVE): An improvement protocol of the Route based distributed packet filtering method. This technique aims to prevent the attack by making all the source routers send updated information about expected/unexpected IP addresses for each destination router. This information is used to filter spoofed IP addresses [19, 20].
2. Challenge Response Protocols (CRPs): aims to identify if the requests are from real users, bots, or attackers' machines to determine if the request is from a real user. It uses the Turing test in the form of CAPTCHA or Crypto puzzles [4].
3. Restrictive Access: This technique is considered a method of permitting the defensive action against the service. Its goal is to delay the responses or access for the assumed attackers or even the extra clients. The delay of responses is done via ordering the legitimate clients or choosing those who have good previous behaviors [4].

B. Detection of DDoS Attack on Cloud Computing

Detection means examining the network to classify the legitimate traffic from the malicious one [1]. In cloud computing, the detection mechanisms are very important, but they are not easy to design and they need great effort [4].

1. Signature-Based Detection: It is known as a misuse technique [21]. It has been used to identify the known attacks on cloud computing by monitoring the performance of the network traffic and compare any incoming packets with a set of attack signatures that are related to some known attacks and stored in a database. Any other attack with a signature that is not stored in the database cannot be detected. Thus, the database of the attack's signature has to be updated regularly with the new signatures to be able to detect the attacks in the future. However, this process is not an easy thing to do, plus it consumes time and resources [10]. The undetectable of zero-day attacks via using this technique is considered the main obstacle of this technique [22].
2. Anomaly-Based Detection: This technique is performed by using the past historic traffic behavior for a period

known as the user profile. This profile is created before the attack takes place by matching the current traffic performance with the normal performance. This approach is used to detect any changes in the system activities to determine the anomalies patterns against the normal traffic [1, 4, 22].

3. Resource Usage: A visualized server known as the hypervisor is used to run the infrastructure as a service cloud. Once the VMs start to use the resources abnormally, an attack is suspected [4]. The real challenge is to be able to distinguish between the high traffic due to an attack and the one due to real traffic. The drawback of this technique is that it only issues a warning about the risk of an attack [10].
4. Hybrid-Based Detection: It is a detection method that uses the benefits of signature-based and anomaly-based mechanisms in detecting the DDoS attack. The advantage of this method is in the improvement of the detection rate. However, collective detection techniques are used to determine the performance and computational cost of the hybrid detection mechanism [22, 23].

C. Mitigation of DDoS Attack in Cloud Computing

Mitigation means taking action based on the impact of the attack at the right time. The results of this phase are used to update the measurements of the prevention phase regularly [1].

In this section, some of the mitigation techniques against DDoS attacks are discussed.

1. Software-based and Hardware-based Firewall Against the DoS and DDoS Attacks: firewalls usage for mitigating DDoS attacks can be very useful and reduce the effect of the attacks. By utilizing the basic standards of the firewall, such attacks would not be very effective. To gain better security, detect and prevent DDoS attacks in the cloud computing, the software-based and hardware-based intrusion prevention systems (IPS) and intrusion detection systems (IDS) can be used. Any IPS or IDS can detect any attack by using stateful protocol analysis detection or signature-based, statistical anomaly-based [3].
2. Resource Scaling: The dynamic auto-scaling of the cloud's resources feature is considered one of the best methods for DDOS mitigation. It helps the server to be available during the attack with the ability to scale the resources. The challenge in this method is to know when to add extra resources and if the decision to add the resources was correct. Unfortunately, the attacker could gain an advantage from this method by increase the strength of the DDoS attack and deplete the newly added resources [4].
3. Victim Migration (VM): The idea of VM migration is to shift the entire running server, during a DDoS attack, to another physical server with unnoticeable downtime. The new server that was shifted to is isolated from the DDoS attack. After detecting and mitigating the attack, the work shifts back to the old "main" server [4].
4. DDoS Mitigation as a Service (DMaaS): There are multiple third parties who provide cloud-based services for protection from DDoS attacks. This solution is presented in the cloud for providing DDoS mitigation as a service. It is mostly useful for companies that need specialized help. It helps the actual firewall to quickly do the mitigation. This solution is based on the threshold/count or intervention of humans. While the major limitation of it is the remote mitigation that makes the mitigation process slow. Moreover, the owner of the service may have some issues with sharing the control with the third party due to security and privacy reasons [4].

V. PROPOSED SOLUTIONS TO DEFEND AGAINST DDOS ATTACKS

There are a large number of researchers who proposed defense techniques against DDoS attacks. Most of them are detection techniques. They include machine-based learning, anomaly-based detection, and signature-based detection. However, the ones based on machine learning are mostly detection and prevention techniques at the same time [2].

In this section, the paper lists some of the proposed defense mechanisms against DDoS attacks on cloud computing in several research papers including prevention, detection, and mitigation techniques. The mechanisms are listed in Table I below with a brief description of each.

TABLE I. ANALYSIS OF PROPOSED DEFENSE MECHANISMS

No.	Authors	Topic	Defense Mechanism			Description
			Prevention	*Detection*	*Mitigation*	
1	B. Al-Duwairia, Ö. Özkasap, A. Uysal, C. Kŭllar and K. Yildirim [8] (2020)	LogDoS: A Novel logging-based DDoS prevention mechanism in path identifier-Based information centric networks	√			-A system based on a novel mechanism that executes GET messages logging-based filtering to make an inter-domain routing. - GET messages are places at the ICN routers in the path of the sender of the content to filter the packets that are not a reply for a previous request. -It is a hybrid approach that uniquely merges between the NDN network and PID-based ICNs -It very effective in responding to data flooding attacks through filtering the packets at the LogDos-enabled routers.
2	H. S.Mondal, M. T. Hasan, M. B.Hossain, M. E. Rahaman, and R. Hasan [24] (2017)	Enhancing Secure Cloud Computing Environment by Detecting DDoS Attack Using Fuzzy Logic		√		- Fuzzy-based detection mechanism designed for detecting the DDoS attacks in cloud environments by filtering the incoming packets before arriving at the cloud. -The packet's behavior is analyzed, and a report is sent to the cloud administrator.

						- Ensures that the cloud system will be secure, reliable, and user-friendly.
3	Mudit Rathore and Abhishek Vaish [15] (2020)	A system design for multi-phase, hybrid DDoS detection		√		-Self-developed framework for detecting DDoS attacks based on ML algorithms that classify and validate the packets by examining the source of the incoming requests and identify the suspicious ones to determine and validate the possible attacks. - Relies on the attributes of the packets on the network for detecting DDoS attacks. packets using a machine learning algorithm -High accuracy of classification and detection.
4	R. Saxena and S. Dey [5] (2019)	DDoS attack prevention using collaborative approach for cloud computing	√	√		- Works by filtering the traffic to distinct the genuine traffic from the malicious ones to find the origin of the DDoS attack. - It provides the interface between the cloud service provider (CSP) and the user of the cloud through the packet trace-back method based on a third-party auditor (TPA). - The testing model is built on a hybrid test model of IRC, AH, and web-based model to detect the Botnet and Dark-net of the IP addresses in the cloud. -Helps to detect the source of the attack and block the system that is on the path of this source.
5	M. Idhammad, K. Afdel, and M. Belouch [25] (2018)	Detection System of HTTP DDoS Attacks in a Cloud Environment Based on Information Theoretic Entropy and Random Forest		√		- Used machine learning, Entropy techniques, and Random Forest classifier to provide a detection technique against HTTP DDoS attacks on the cloud by using a time-based sliding window algorithm that provides an estimation of the entropy for the network traffic. - Based on the average entropy the technique can differentiate the normal traffic from the HTTP DDoS traffic. - A high accuracy is achieved from this approach.
6	M. Zekri, S. El Kafhali, N. Aboutabit, and Y. Saadi [26] (2017)	DDoS Attack Detection using Machine Learning Techniques in Cloud Computing Environments.		√		- It is a hybrid detection mechanism that uses machine learning combined combined with signature-based detection to use its features to increase the detection rate against DDoS attacks. - This mechanism employs a decision tree based on C.4.5 algorithm, which is used to categorize the incoming traffic to detect the DDoS flooding attacks. - Need to be applied in real-time traffic to test its efficiency. -Monitors the DDoS attack in layers 3 and 4 of the OSI model.
7	M. P. NOVAES, L.F.CARVALO, J. LLORET and M. LEMES PROENÇA, Jr. [27] (2020)	Long Short-Term Memory and Fuzzy Logic for Anomaly Detection and Mitigation in Software-Defined Network Environment		√	√	-Applied on SDN environment for anomaly-based detection and DDoS attacks mitigation. - It is made of multiple modules, one of them is for detecting anomalous events using Bienaymé-Chebyshev inequality to detect the normality threshold dynamically, and the Fuzzy logic to detect the presence of an anomaly in a certain time. -Another element of the suggested system is accountable for minimizing the damages by mitigating the detected anomalies. - The mitigation mechanism is applied based on some policies that work automatically to ensure network resilience. -Uses the switch routing table to determine the origin of the attack.
8	A. M. Lonea, D. E. Popescu, and H. Tianfield [28] (2013)	Detecting DDoS Attacks in Cloud Computing Environment		√		-The technique aims to detect and investigate the DDoS attacks on the cloud using the Dempster- Shafer Theory (DST) operations in 3-valued logic and Fault-Tree Analysis (FTA) for each VM-based IDS. - it resolves the problems raised by combining the data from various sensors and improve the work for cloud administrators.

VI. Discussion and Results

Based on the literature, much research has been conducted to find defense mechanisms against all types of attacks targeting the networks in general.

Most of the research are about studying the external DDoS attacks on cloud computing. However, internal cloud DDoS attacks must be taken into consideration as well, since it is a big threat just as much as the external attacks. Experts in the security field expect that the expansion of 5G will escalate the occurrence of DDoS attacks [29].

There is a lack in the diversity of research dedicated to defense mechanisms. As discussed in the previous section, there is a lot of work devoted to the mitigation and prevention of DDoS attacks but there is still a gap between the quantity of this type of attacks that are affecting the cloud environment and the number of proposed systems. A lot of research have focused on proposing a defense system as a detection method against DDoS attacks while there aren't enough proposed methods for prevention and mitigation. Moreover, some papers claim that their system is a prevention and detection system or detection and mitigation system, but when we analyzed the method most of the time it is a detection mechanism more than any of the other mechanisms, which needs to be taken into consideration as well.

One way to increase the number of prevention and mitigation techniques is to model some attacks on a testing cloud environment, to come up with some prevention and mitigation techniques that could help to defend the cloud's services in the real environment to provide their intended purpose to the users.

VII. Conclusion and Future Work

Recently, DDoS attacks have greatly affected cloud infrastructure for a lot of businesses. This paper reviewed research between the years (2013) and (2021) about DDoS attacks and how they affect the cloud. The infrastructure of the cloud, the scenario, and the effect of DDoS attacks are explained in the paper. Additionally, the several kinds of

DDoS attacks with the cloud features that open the door for the attackers to launch the DDoS attack are highlighted as well.

Although many well-known defense mechanisms are there and have been used frequently as stated in the paper, some DDoS attacks cannot be prevented, detected, or mitigated. This is due to many reasons either an unrecognizable signature within the signatures database or the attack is launched from a legitimate IP address. Another reason is the difficulties faced by some mechanisms in distinguishing the DDoS attack high traffic from other massive legitimate traffics.

There are many security issues related to the cloud that must be taken into consideration, and DDoS attack is not the only significant one. So, as an extension to this work, new taxonomies of DDoS attacks can be discovered. Also, the effectiveness of the existing DDoS attacks defense mechanisms could be measured against other kinds of attacks that target the cloud environments. The researchers should work on discovering more effective techniques to make the clouds a safe environment as much as possible.

REFERENCES

[1] N. Agrawal and S. Tapaswi, "Defense mechanisms against DDoS attacks in a cloud computing environment: State-of-the-art and research challenges," *IEEE Communications Surveys & Tutorials,* vol. 21, no. 4, pp. 3769-3795, 2019.

[2] A. Moqeet, "A Machine Learning Based Classification Technique to Detect DDoS Attack in Cloud Computing Environment," CAPITAL UNIVERSITY, 2021.

[3] A. Balobaid, W. Alawad, and H. Aljasim, "A study on the impacts of DoS and DDoS attacks on cloud and mitigation techniques," in *2016 International Conference on Computing, Analytics and Security Trends (CAST)*, 2016, pp. 416-421: IEEE.

[4] G. Somani, M. S. Gaur, D. Sanghi, M. Conti, and R. Buyya, "DDoS attacks in cloud computing: Issues, taxonomy, and future directions," *Computer Communications,* vol. 107, pp. 30-48, 2017.

[5] R. Saxena and S. Dey, "DDoS attack prevention using collaborative approach for cloud computing," *Cluster Computing,* pp. 1-16, 2019.

[6] O. Osanaiye, K.-K. R. Choo, and M. Dlodlo, "Distributed denial of service (DDoS) resilience in cloud: review and conceptual cloud DDoS mitigation framework," *Journal of Network and Computer Applications,* vol. 67, pp. 147-165, 2016.

[7] N. Bandi, H. Tajbakhsh, and M. Analoui, "FastMove: Fast IP switching Moving Target Defense to mitigate DDOS Attacks," in *2021 IEEE Conference on Dependable and Secure Computing (DSC)*, pp. 1-7: IEEE.

[8] B. Al-Duwairi, O. OOzkasap, A. Uysal, C. Kocaoggullar, and K. Yildrim, "LogDos: A Novel Logging-based DDoS Prevention Mechanism in Path Identifier-Based Information Centric Networks," *arXiv preprint arXiv:2006.01540,* 2020.

[9] B. Soewito, F. L. Gaol, and E. Abdurachman, "A Systematic Literature Review: Risk Analysis in Cloud Migration," *Journal of King Saud University-Computer and Information Sciences,* 2021.

[10] J. N. Ahamed and N. Iyengar, "A Review on Distributed Denial of Service (DDoS) Mitigation Techniques in Cloud Computing Environment," *International Journal of Security and Its Applications,* vol. 10, no. 8, pp. 277-294, 2016.

[11] X. Liu, J. Ren, H. He, Q. Wang, and C. Song, "Low-rate DDoS attacks detection method using data compression and behavior divergence measurement," *Computers & Security,* vol. 100, p. 102107, 2021.

[12] J. Singh and S. Behal, "Detection and mitigation of DDoS attacks in SDN: A comprehensive review, research challenges and future directions," *Computer Science Review,* vol. 37, p. 100279, 2020.

[13] R. V. Deshmukh and K. K. Devadkar, "Understanding DDoS attack & its effect in cloud environment," *Procedia Computer Science,* vol. 49, pp. 202-210, 2015.

[14] G. Somani, M. S. Gaur, D. Sanghi, M. Conti, and M. Rajarajan, "DDoS victim service containment to minimize the internal collateral damages in cloud computing," *Computers & Electrical Engineering,* vol. 59, pp. 165-179, 2017.

[15] M. Rathore and A. Vaish, "A system design for multi-phase, hybrid DDoS detection," *Computer Fraud & Security,* vol. 2020, no. 11, pp. 10-19, 2020.

[16] M. Masdari and M. Jalali, "A survey and taxonomy of DoS attacks in cloud computing," *Security and Communication Networks,* vol. 9, no. 16, pp. 3724-3751, 2016.

[17] P. Nelson. (2015, 8 Dec 2020). *Cybercriminals moving into cloud big time, report says*. Available: https://www.networkworld.com/article/2900125/criminals-moving-into-cloud-big-time-says-report.html

[18] T. Robinson. (2015, 8 Dec 2020). *Series of DDoS attacks plague Linode data centers, infrastructure*. Available: https://www.scmagazine.com/?s=Series+of+DDoS+attacks+plague+linode+data+centers

[19] T. Mahjabin, Y. Xiao, G. Sun, and W. Jiang, "A survey of distributed denial-of-service attack, prevention, and mitigation techniques," *International Journal of Distributed Sensor Networks,* vol. 13, no. 12, p. 1550147717741463, 2017.

[20] K. S. Bhosale, M. Nenova, and G. Iliev, "The distributed denial of service attacks (DDoS) prevention mechanisms on application layer," in *2017 13th International Conference on Advanced Technologies, Systems and Services in Telecommunications (TELSIKS)*, 2017, pp. 136-139: IEEE.

[21] S. Alzahrani and L. Hong, "A survey of cloud computing detection techniques against DDoS attacks," *Journal of Information Security,* vol. 9, no. 01, p. 45, 2017.

[22] S. Q. A. Shah, F. Z. Khan, and M. Ahmad, "The impact and mitigation of ICMP based economic denial of sustainability attack in cloud computing environment using software defined network," *Computer Networks,* vol. 187, p. 107825, 2021.

[23] M. A. Alarqan, Z. F. Zaaba, and A. Almomani, "Detection Mechanisms of DDoS Attack in Cloud Computing Environment: A Survey," in *International Conference on Advances in Cyber Security*, 2019, pp. 138-152: Springer.

[24] H. S. Mondal, M. T. Hasan, M. B. Hossain, M. E. Rahaman, and R. Hasan, "Enhancing secure cloud computing environment by Detecting DDoS attack using fuzzy logic," in *2017 3rd International Conference on Electrical Information and Communication Technology (EICT)*, 2017, pp. 1-4: IEEE.

[25] M. Idhammad, K. Afdel, and M. Belouch, "Detection System of HTTP DDoS Attacks in a Cloud Environment Based on Information Theoretic Entropy and Random Forest," *Secur. Commun. Networks,* vol. 2018, pp. 1263123:1-1263123:13, 2018.

[26] M. Zekri, S. El Kafhali, N. Aboutabit, and Y. Saadi, "DDoS attack detection using machine learning techniques in cloud computing environments," in *2017 3rd International Conference of Cloud Computing Technologies and Applications (CloudTech)*, 2017, pp. 1-7: IEEE.

[27] M. P. Novaes, L. F. Carvalho, J. Lloret, and M. L. Proença, "Long Short-Term Memory and Fuzzy Logic for Anomaly Detection and Mitigation in Software-Defined Network Environment," *IEEE Access,* vol. 8, pp. 83765-83781, 2020.

[28] A. M. Lonea, D. E. Popescu, and H. Tianfield, "Detecting DDoS attacks in cloud computing environment," *International Journal of Computers Communications & Control,* vol. 8, no. 1, pp. 70-78, 2013.

[29] I. Ko, D. Chambers, and E. Barrett, "Adaptable feature-selecting and threshold-moving complete autoencoder for DDoS flood attack mitigation," *Journal of Information Security and Applications,* vol. 55, p. 102647, 2020.