Journal of Theoretical and Applied Information Technology
15th July 2022. Vol.100. No 13

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

DDOS ATTACKS DEFENSE APPROACHES AND MECHANISM IN CLOUD ENVIROMENT

[1]SARAH NAIEM, [2]AMIRA M. IDREES, [1]MOHAMED MARIE, [2]AYMAN E. KHEDR

[1]Faculty of Computers and Artificial Intelligence, Helwan University, Cairo, Egypt

[2]Faculty of Computers and Information Technology, Future University in Egypt, Cairo, Egypt

Email: SarahNaiem@fci.helwan.edu.eg, amira.mohamed@fue.edu.eg, dr.mmariem@fci.helwan.edu.eg, ayman.khedr@fue.edu.eg

ABSTRACT

Cloud computing is becoming a very vital part of any business nowadays and the business sector's main concern is the security in terms of availability, authenticity, and confidentiality. Distributed denial of services (DDOS) is becoming the main security threat in cloud where DDOS targets the cloud services and structure to obstruct the access of the rightful users. The protection of cloud from this attack is becoming very challenging, throughout this paper we first discussed the different prevention, detection, and mitigation approaches along with the techniques used for each approach. The prevention approaches include hidden servers, restrictive access, resource limitation, and challenge response, while the detection approached include signature and anomaly-based detection, data mining, resource usage and filtering techniques. Moreover, we discussed the recent defense mechanisms in the different approaches, and it was obvious that most of the defense mechanisms are only based on detection of the DDOS and there is a huge gap in terms of the prevention and mitigation approaches.

Keywords: *DDOS Attacks, DDOS Defense in Cloud, Prevention, Detection, Mitigation.*

1. INTRODUCTION

Cloud computing based environment is being adopted by almost every business now day due to the huge amount of services this technology offers including scalability, availability, efficiency, and adequate cost adaptation [1]. [2] Cloud technology provides its users with different services including Platform as a Service (Paas), Software as a Service (SaaS), and Infrastructure as a service (Iaas) offering Virtual Machines (VMs) to its clients whenever required [3]. Cloud also offers features to its users including auto-scaling, multi-tenancy, and pay as you go for ease of use and availability with that in mind the idea is to remove the liability of handling and maintaining the hardware from the user [4]. We can't deny that the security issue is a concern for most users on the cloud, where the services provided should always be available to the rightful users, the data should be authenticated from unauthorized access and confidential. One of the main problems with cloud security is Distributed Denial of services (DDOS) attacks in which the attacker's purpose is to obstruct the flow of the service and prevent the rightful user of accessing their services and data. [5] The problem with this specific type of attack is that it works by exploiting the features that original attracted the user to shift to cloud technology. In order to counteract this attack, we need to understand several aspects including the motive of the attacker, the target of the attacker and how exactly could a DDOS exploit the in the cloud environment. [5]. The motive of the attacker could be for anything from just an intellectual challenge or for the fun of it and it could also be done for the benefit of a competitor. DDOS attacks targets the features of a cloud where for instance a DDOS could manipulate the victim into adding more resources through multi-tenancy feature of the cloud and auto-scaling feature leading them to pay extra for these features which also exploits the pay as you go feature. [6] [7]

A DDOS attack could have several forms and different strategies, but it is generally branded into either Semantic or brute-force attacks [8]. Where Semantic DDOS attacks which is also known as Low-rate DDOS works on abusing the boundaries of the cloud serves as they generate malicious traffic with a low rate targeting the protocol or service of the user and it's very difficult to trace or capture as this type of traffic is very similar to the normal traffic of a legit user over the cloud. Low-rate DDOS attacks encompasses several attacks like shrew attacks, reduction of quality attacks, economic denial of sustainability attacks, and low rate DDOS attack against application server affecting the quality of the service being provided to the legitimate user. On the other brute-force attacks work through sending a

significantly large number of requests to the targeted user to overwhelm the victim which is known as high-rate DDOS or flooding attacks. The basic idea of flooding is exhausting either the networks or resource's bandwidth capacity through either the application or the network level. [9] [10] [11]

2. LITERATURE REVIEW

To defend the cloud against the DDOS we need to understand the defense ideologies including prevention, detection, and mitigation. The prevention of an attack is a protection upbeat step to reduce the chances of the occurrence of it and in case an attack successfully happened its detection is very vital to handle it and mitigate it to prevent the service from being denied to the rightful users [4]. Each one of these ideologies has different approaches that have been extensively studied and categorized according to its technique. Throughout the rest of this paper, we will first discuss the different approaches used for each of them following that the different techniques are discussed.

2.1 Prevention of DDOS Attacks in Cloud

Prevention of a DDOS means trying to secure the user from the possibility of the attack happening, the approaches of prevention include, hidden server/ports, restrictive access, Challenge response, and resource limitation.

2.1.1 Hidden Server/Ports

Helps legit clients to access the services provided without any direct connection with the server at the beginning, it requires an extra layer of security for the redirection and extra server ports. This approach helps connecting the legit user to the service without an actual direct connection to the server and it required to handling and management of the traffic on these ports. This makes it hard for attackers to manipulate the service as they can't get to track the actual connection. The redirection among the ports needs requires traffic monitoring and balancing between the different addition ports to avoid performance issues. Moving Target Defense (MTD) is one of the well-known techniques that are used. [4] [5] [12]

2.1.2 Restrictive Access

Restrictive access approach is based on delaying their response to new connections by prioritizing the clients according to their reputation which helps in preventing DDOS attacks from malicious users. IT is based on "selective access" or "Delayed access" techniques in assembling the requests allowing access to the service only to users with decent history [6]. Resilient Scheduling is one of the commonly used restrictive access techniques where it has a DDOS resilient scheduler and suspicion assignment that gives an unremitting value to the sessions that is then exploited through the scheduler and given access. Using this approach for prevention might affect the scalability feature not only that but sometimes attackers work on creating a good behavior before attacking the service which will lead the prevention technique to believe that they are not harmful and give them access. [5] [7] [10] [12]

2.1.3 Challenge Response

Challenge Response approach is used to make sure that a user is an actual real user not a bot and it could be applied by the concept of puzzles. The idea is the user is presented with an image and he would be requested to answer specific questions or rearrange it or respond to whatever type of question. Prevention through challenge response is very helpful and operative if the overhead resulting from the use of graphics is accounted for. The idea is to try to make it hard enough for bots but still solvable for humans and at the same time handling the image partitioning, buildup of puzzles and parsing attacks. CAPTCHA, turing tests and crypto puzzles, proof or work techniques are the most commonly used techniques. [4] [5] [10]

2.1.4 Resource Limit

This approach is used in the prevention of economical DDOS (EDOS) as it controls the dynamic scaling feature of the cloud to prevent attackers from gaining access to new resources which unfortunately leads the cloud to lose its elasticity features provide to the legit users. This approach is based on limiting the bandwidth of the clusters as a network traffic management technique [10] and it's also known as "using resource quota" [6]approach where a limit to the scalability is set to reduce to prevent extra cost but yet this will also lead to the service being unavailable when the attacker reaches that limit. [4] [5]

2.2 Detection of DDOS attacks in cloud

The detection of an attack means that the attack is already in action and taking place over the network which makes it very important to be able to capture the attack and handle its consequences. This approach has a lot of different techniques that have been studied and reviewed, it includes signature based, anomaly based, hybrid detection, resource usage, Bot cloud, count based filtering, and source and spoof tracing which are discussed next.

2.2.1 Signature Based Detection

Signature based DDOS detection is built on the concept of stopping known attacks from taking place by the using of Intrusion Detection Systems (IDs) that are installed on VMs where the packets with blacklisted IP addresses are immediately dropped after the traffic over this VM is analyzed. Using this approach requires constant and frequent updating of the blacklisted IP or else the detection of these attacks would fail which is still very impracticable. [4] [10] [11] [13]

2.2.2 Anomaly based Detection

This approach is based on machine learning technique in detecting the abnormal behavior in the traffic of the cloud where the behavior of the network's traffic is being studied over time to be able to detect DDOS. The dataset setting and its selection criteria along with the testing to profile the traffic are the main functions followed when using anomaly detection approach. Anomaly based detection is very efficient against unknown attacks but might lead to extra overhead cost due to training of data and the need high statistical analysis for matching of the traffic features and might not be effective with low-rate DDOS. This approach includes Machine learning (ML), artificial intelligence (AI), statistical, and data-mining based anomaly-based detection. [4] [5]

2.2.2.1 Machine Learning based detection approach

The use of ML depends on the type of data set being used making it either supervised or unsupervised where it studies the performance of the patterns in the dataset. Supervised ML works by trained and labeled datasets and its algorithms include Neural network, decision tree, fuzzy logic, deep learning, support vector machine (SVM) and Naïve Bayes. While Unsupervised ML dataset doesn't need to be the dataset to be labeled as its analysis them to figure out the attack's behavior through algorithms like K-Means and hieratical clustering. [4] [13] [14]

2.2.2.2 Artificial Intelligence based detection approach

It's also known as deep learning which is considered a comparably new approach where using AI based detection has been proven to be an effective detection approach as large data set is being used with very low training time and the results have high accuracy. This technique includes different models like Self-taught learning (STL), restrictive Boltzmann Machine (RBM), and non-symmetric deep autoencoder (NDAE). [4] [5] [13] [15]

2.2.2.3 Statistical anomaly Based Detection Models

This approach has the advantage of the use of statistical feature s in the capturing of malicious traffic which is based on either information entropy, distance entropy, or correlation coefficient entropy. The concept of entropy is based on statistical analysis of the changes in the network for attack detections. Statistical anomaly detection doesn't need much information about its packet headers as it easily identifies the type of traffic not only that but its success rate in detection is high and has high scalability and sensitivity features with low computation cost but setting he optimal threshold could be challenging. [13] [15]

2.2.2.4 Data mining anomaly-based Model

This approach is set to have higher accuracy as in its based on the clustering and knowledge extraction features of the data mining while handling large databases with a low computational cost. On the other hands it doesn't work very well with high incoming traffic rate over the network. [10] [13]

2.2.3 Hybrid Detection approach

This approach is a mixture based on the good qualities of both signature-based and anomaly-based approaches leading to higher classification accuracy. The idea of implementing this detection approach is making sure that the combined approaches won't lead to extra cost or reduction of quality. [4] [7] [13]

2.2.4 Resource Usage Detection approach

This approach is based on the monitoring of the VM by the hypervisor of IaaS in cloud and studying its traffic to help in capturing DDOS attacks. Where the traffic's throughput, auto-scaling of VM and the usage of the CPU and memory are used as a metric for detecting DDOS attacks or even the possibility of its occurrence. The success of this approach relies on differentiation between malicious high traffic and legit high traffic and it only sends a notification that there is an attack [4] [7] [13] [16]

2.2.5 Bot-cloud detection approach

This approach targets the attacks that tack place in the cloud's infrastructure where the attacker tacks advantage and uses the clouds own features to perform the attack in the form of an internal bot. The target of bot-cloud approach, which is considered a CSP, or source-based approach is to work on finding attacks aimed towards the VM's in a cloud. [5] [13]Although this approach is based on the idea of it being deployed on the cloud making it easier to monitor the behavior of the traffic on the network it

doesn't work well with all types of attacks. [4] [5] [13]

2.2.6 Count-based filtering detection approach

It's based on detecting and attack through hop-count, number of requests per time from a particular source, and the number of connections using filtering techniques such as Time-to-live (TTL), Jensen-Shannon, Path identification (Pi), IP flow count, confidence-based filtering (CBF). It's very helpful with DDOS attacks on HTTP, Representational State Transfer (REST), and eXtensible Markup Language (XML). Count-based filtering is very efficient as the administrator of the network can easily take control over the attack situation and the deployment process is considerably easy, but its database need constant updating ,it faces issues with accurateness and integrity due to the IP spoofing, and it also faces problems due to the divergent implementation of heterogeneous hop-count. [5] [7] [17] [18]

2.2.7 Source and Spoof tracing

This approach is very vital for the prevention and detection of DDOS where it could either be reactive or preventive and is based on the tracking back the attack to find its origin and prevent it. However, it's not an easy approach as it needs the CSP and different components of the network and it doesn't function well with large scale DDOS attacks. There are several type of source and spoof tracing including IP traceback, Packet Marking and logging which includes Probabilistic packet marking (PPM) and Deterministic packet marking techniques, and Service Oriented Architecture-Based Tarceback Approach (SBTA). [5] [7] [13]

2.3 Mitigation of DDOS in cloud

Mitigation of an attack is the last step in the defense against DDOS where the idea is to keep providing the services to the legit user and handling the attack at the same time. Mitigation techniques assess the magnitude of the attack and its damage and accordingly acts where it is broadly categorized into collaborative and non-collaborative approaches. Collaborative mitigation is based on firewalls and pushback concept and the non-collaborative which can either by dynamic which provides a solution appropriate for the magnitude of the attack or static which doesn't account for the attack's magnitude. This approach could be done through resource scaling, Software Defined Network based mitigation, victim migration, and DDOS mitigation as a service (DMaaS). [5] [10] [13] [19]

2.3.1 Resource scaling Mitigation approach

Is a non-collaborative dynamic approach for either horizontal or vertical auto-scaling of the resources. Vertical resource scaling works by scaling the resources on the same unit or VM while horizontal scaling works by adding new instant. Even though the addition of new resources helps in providing the services while DDOS is taking place which means that the user is not affected by the attack but sometimes that's the purpose of the attack which is to attack the cloud with the purpose of adding new resources resulting in economic losses. [4] [5] [10]

2.3.2 Software Defined Networking Mitigation approach

SDN mitigation approach is considered comparably new and its very helpful due to the re-configurability on the fly and fast system checking features of SDN and is very helpful with the low-rate DDOS attacks. The only drawbacks so far is that the structure of the SDN could become the attackers target and that it only works well at the ISP level and network boundaries. [5] [19]

2.3.3 Victim mitigation Approach

This approach is based on idea of changing the victim's server to another server without affecting the user or the services provided to him and it's a non-collaborative dynamic approach. When the DDOS is handled on the original server the user is shifted back. This approach is considered a costly one and selecting the candidate host is a challenging process. [4] [5] [10] [19]

2.3.4 DDOS Mitigation as a Service (DMaaS) approach

DMaas is a third-party cloud hybrid-based mitigation approach based on traffic monitoring remotely [5]. Software and Hardware based firewall mitigation is a DMaas collaborative mitigation approach where the fundamental firewall standards are operated to stop the DDOS attempts. This approach works very well when collaborated with intrusion prevention and detections approaches. Unfortunately, this approach sometimes faces issues due to the fact of remote monitoring and it results in extra cost . [4] [5] [10]

3 COMPREHENSIVE STUDY OF THE EXISTING PROPOSED FRAMEWORKS FOR PROTECTION AGAINST DDOS IN CLOUD

Zareapoot and Shamsolmoali conducted a survey on the DDOS detection and mitigation techniques and proposed a model based on the research gaps they found with the purpose of creating an accurate, and simple model with low storage space. The first step in the model is the feature extraction from the packets to generate a silhouette for the network including

both legit and harmful traffic. They extracted the essential attributes for their novelty model including IP source, ports, ipFlags, tcpflages, destination IP, ports, icmpType, udp length. They then offered a formula that would calculate how many hops the packet travelled since the attacker could only spoof the packet's header and can't influence the number of hopes travelled by the packet. After that the model studies the deviation and irregularities of the traffic for clustering through studying the packer headers. The authors based their model on Jensen-shannon entropy divergence concept to calculate the deviation which is an anomaly detection-based technique. The model is based on a cloud lab with an HP ProLiant DL server and a VM-manager based on VMware ESXI 5.0.0 Hypervisor. The DDOS attack was generated by NeTwag tool form two VMs and three client VMs with legit traffic and the packets were captured via JPCap tool. The model was tested using the netwag tool and "CAIDA" for the generation of DDOS attacks and compared the algorithm used against Naïve Bayes (NB), Part, ripper, and random forester (RF) classifiers. The results show that the proposed model accuracy as 97% like the part classifier and 2% less than ripper, 1% less than RF, and its false alarm rate and processing time were the lower than the lab data and the other classifiers exept for the NB [20].

Another anomaly-based detection model was proposed by Hezavehi and Rahmani based on TPANG detector and ND protocol named TPANGND framework and they applied it in cloud environment as a third-party editor. Where it's based on measuring the response time of the SLA (RTSLA) and by the TPANG for DDOS attack detection and the ND protocol sends periodically timed notification messages to the cloud service provider as alarms to compare the RTSLA with a preset threshold value where the RTSLA is used to identify if this is normal traffic time response or its affected by an attack. This anomaly based third-party editor detection approach doesn't support filtering or trace-back features, but it has been proven by the authors that it overcomes a lot of the shortages available with the currently available proposed detection frameworks, but it does not work well with low-rate DDOS attacks. They tested the TPANGDN framework against another cloud environment with internal detection and called it CIDM and created for different scenarios for the attack where they simulated attacks on the CPU, memory, bandwidth, and hybrid targets. The computational efficiency, ability to detect DDOS attack, and response time of the proposed framework and the results showed that it has better performance than the CIDM in all for scenarios, yet the attacks based on hybrid target had lower detection rate and they highlighted that this area needs further research [21].

An intrusion detection and prevention operating on hybrid classification in cloud has been proposed by Balamurugan and Saravan based on a cloud controller (CC), VM management (VMM), and Trust Authority (TA). The CC monitors the packets collected through routers from the cloudlet and in the instance of high traffic the CC mitigates the traffic to another attack free cloudlet. The header of packets of the malicious traffic are then examined using packet scruntinization (PS) algorithm based on its flow, time of arrival, packet counts, and confidence level after that and the packets are diverted to the the VMM for classification through a hybrid classifier composed of normalized K-means (NK) and recurrent neural network (RNN) clustering algorithms called NK-RNN. The packets that are not malicious are handled via a queuing system in the proposed model called M/M/C:FIFO with a set of criteria for packet handling based on the waiting time and request earnestness which results in a huge increase in the quality of the service provided. After that comes the second part of the proposed framework that's based on the TA where a prevention mechanism for the protection of the legit users of the cloud is produced based on providing secure access to the data through elliptical curve cryptographic concept. The user has a private and public key, and the private key is randomly created for a one-use time by the user and the signature is changed after the its used and new private key is generated. The proposed model was tested, and the results shows that the NK-RNN has the lowest false negative rate and highest false negative rate compared to other algorithms, and the highest F-score [22].

R. Saxena and S Dey in their study proposed a detection and prevention technique using an auditor as a third party for DDOS in cloud. They surveyed a lot of techniques and concluded that there are four different stages for securing a cloud against DDOS starting with monitoring the traffic, detection of the attacks, preventing and then mitigating them. The proposed solution they offered is called "Cloud Warrior" (CW) for both the detection and the prevention of DDOS which uses Weibull distribution probability that would undoubtedly help to detect the different DDOS in the environment of the cloud due to the reliability of its function. The CW is composed of the internet, which is used by the cloud users, front-end server with two connections to the Ethernet

one provides the front end server with CSP services and the other helps in the positioning of a virtual private cloud through a cloud fusion unit (CFU), and finally is a virtual private cloud. The Virtual private cloud used in the architecture of the CW is composed of four virtual machines (nodes) that are linked using a private switch to the front-end server and these nodes are ran with the help of "Citrix Xen Server" to make sure that the progressive virtualization features are achieved. The CW operates by first observing the four nodes that are linked to IDS tools and constituted via Weibell Distribution probability, then the front-end server creates packet floods that are stored in a NoSQl data base with the help of basic probability assessments "BPAs". The second stage of the operation of CW is the detection of Distributed DOS where the TCP, ICMP, and UDP packets are investigated using a 3-valued logic to split the flood attacks of each of the protocols along with the Weibell distribution. Then the attack is evaluated at the CFU and the floods of the three protocols are merged and tested for the occurrence of a DDOS attack. [23]

A sahi et al proposed a detection model composed of two stages a detection one and prevention one called CS_DDOS for prevention of TCP flood attacks. The detection module of the proposed architecture where the traffic packets are tested against a blacklist with harmful spoofed IPs and if the IP is present in the list the attack is stopped through the prevention phase and if it's not its then examined through a classifier. The packets sent to the classifier are tested through an algorithm that checks the number of requests from a that IP to see is its more than the predetermined threshold. The authors decided to examine three different classification algorithms including k-nearest, Naïve bayes, multilayer perceptron, and least square support vector machine (LS-SVM) not only that by they also decided to examine three different scenarios in examining the CS_DDOS including normal traffic, malicious traffic from IPs stored in the blacklist, and malicious traffic that's not in the blacklist and used single source attack and multiple source attack scenarios. After CS_DDOS was tested under all the mention scenarios it has been proven that the LS-SVM classification algorithm has the highest detection and prevention for both attack scenarios where the singe attack had accuracy of 97% with 0.89 kappa coefficient which measures the consistency of the results of the experiment and accuracy of 94% and 0.9 kappa coefficient with the multiple attack scenario. [24]

A. Amjad et al proposed a DDOS detection module where they simulated "ping of death" DDOS attack in cloud based environment using PrrotSec which is command line based interface. After simulating the attack, they first used Nmap scanner to find open ports through scanning the targeted environment for anomalies in the system generating a python-based script with the attack that would be then monitored and captured through sniffing at the server's side using "Wireshark" sniffing. The dataset created from the sniffing phase is then used and analyzed by the classifier where they used "Naïve Bayes" due to its simplicity, success rate and ease of use where the resulted output dataset cross validation could either be true positive, true negative, false positive or negative rate. Unfortunately, the proposed model was not tested [2].

B. Al-Duwairia et al proposed a prevention and detection model based on the idea of filtering logged get messages called LogDoS in information centric founded path identifier networks (PID based ICNs). The framework works on logging the information of the get messages passing through the network at every router and they named this process "Comprehensive logging". The first thing they worked on was reducing the overhead resulting from storing the GET messages and decided to follow three different approaches based on Bloom filtering including Comprehensive logging, Odd/even logging, and Dynamic logging and they compared the results and performance of the three scenarios. Comprehensive logging only logs the digests of the get message reducing the storage space as its part of the message not the whole message. Although bloom filters don't have the option of deletion the authors decided to use two bloom filters at each router so that when one reaches the value set for indication false positive rate the other bloom filter is activated and in action. The even/odd logging algorithm they proposed works through enabling specific routers to log the GET message LogDoS from the same path from the customer to the server making the confirmation of a message performed at the exact same router. As for the dynamic logging the routers dynamically perform the packet logging and authentication process in a time span instead of it being continuously logged like in the case of even/odd and comprehensive logging. The authors of this hybrid framework simulated DDOS on the different proposed algorithms and in all cases the results showed that the detection and prevention rate is better than other PID based ICNs. [25]

Rathore and Vaish proposed a multi-phase hybrid architecture for DDOS detection where the first phase is for packet filtering where the incoming data is screened based on the source's genuineness and the second phase is based on machine learning for classification of the packets that passed the first phase. The Packet filtering is based on the segregation of the incoming traffic for IP examination, the initial server receives the IPs and uses Address Resolution Protocol (ARP) for identification then uses the result in updating the packet details according to its source following that the IP of legit traffic is redirected to the section phase through HTTP redirect request. The machine learning classification phase which is based on ensemble learning concept first starts by cleaning the data from unnecessary columns for the information gaining and feature extraction process. They based the ensemble learning is on four concepts including stacking, bagging, boosting, and blending. The idea of using ensemble learning helps with detecting DDOS of different types and the results of the simulation of the framework showed that all the concepts used in phase two very high accuracy, true positive, and true negative and low false positive when tested against multi- class and binary class classification except for the stacked based ensemble based learning where the performance of the multi-class classification is much lower than the rest of the classification models. [26]

Idhammad et al worked on a HHTP DDOS attacks detection system based on machine learning, random forest classification, and entropy techniques based on a time window algorithm for the entropy estimation to classify the normal and malicious traffic. The first phase of the system is the estimation of the incoming network's traffic entropy, where a window of time is set help in the estimation for the features of the network's header through the help of the connection definition features, and the source/destination ports and IPs. The result of this phase helps in setting the lower and upper bounds of the allowed entropy to help in the following two phases of the system. The network traffic preprocessing starts by cleaning the traffic and dropping empty and null values in the data set then via MinMax approach the data is normalized for the final HTTP DDOS detection stage. The classification of the incoming normalized traffic is then classified through the machine learning classifier, and they used different classifiers including random forest, K-nearest, NB, decision trees and compared the results based on the output's correctness and rates of true positive, true negative, and false positive. According the the results of using these different classifiers the authors stuck to random forest as its accuracy rate was 97% and 3% higher than the highest rate of the other algorithms. IT was also highlighted that selecting and appropriate time window was challenging as it should be enough to capture the required information and not large to mess up the whole algorithm. [27]

Another detection architecture was proposed by Ali and Osman in their work consisting of feature extraction and selection phases followed by the detection and prevention phases. The Feature extraction was done through sequential backward selection for the elimination of the feature's redundancy and the features selected are then classified on two levels the first one is based on type-2 fuzzy logic for the packet classification producing normal, harmful, and suspicious packets based on a blacklist with spoofed IPs where the normal packets are permitted, the harmful ones are disregarded, and the suspicious packets are transferred to the second level. The suspicious traffic is classified via SVM based neural network and the harmful packets from this classifier are then added to the blacklist. The architecture included an authentication layer using hash message (HMAC) based on A-256 algorithm where the user uses when accepting packets. The architecture was simulated on CloudSim toolkit which is a multi-level simulator, with "KDD CUP dataset" and the authors used different SVM bounds and Kernels including "POLY,LINEAR,SIGMOID,RBF" and the results showed that the highest DDOS detection accuracy rate and the lowest false positive rate was reached by using SIGMOID while POLY resulted in the lowest accuracy rate and highest false positive rate [28].

A Prevention framework was proposed by Saravanan et,al where they proposed a new challenge response idea that could be used instead of the CAPTCHA or reCAPTCHA method for identifying legit traffic from harmful floods. The proposed prevention technique features Visual Comprehension "VISUALCOM", Image Completion "IMGCOM", and Image Completion Anomaly detection "AD-IMGCOM". Visual comprehension is founded on the idea of challenging user to respond to a question based on an image that is displayed to them and this approach helps with reduction of the storage space that gets consumed when using other turing test techniques.

Another advantage for using VISUALCOM is that one image can produce multiple questions serving multiple users which also helps with the response

time and performance. While Image Completion is considered more complicated since it works by partitioning a picture into several sections and for the user, he is supposed to drag the image partitions and drop them to create the whole complete image as a challenge, even though this approach uses only one image but is a bit harder for the users which makes it hard for bots. AD-IMGCOM is like IMGCOM but more challenging since it adds some anomalies to the image being identified to the user that he has to ignore. The functioning of the proposed methods has been evaluated in terms of performance time and success rate and it was proven that its better than other challenge response techniques increase the success rate and performance. The problem with this approach as mentioned by the authors is that it could lead to puzzle building up and might also lead to extra image overhead leading to late response or even failure and blockage of the system [29].

Moqeet 2021 proposed a machine learning based framework composed of three subsystems for the detection of TCP, UDP, and ICM flooding DDOS attacks. The system is consisted of preprocessing, adaptive attribute selection, and a detection subsystems using NSL-KDD dataset including both harmful and legit requests and then the attributes are extracted from the log files for normalization which initially included 41 attributes labeled as anomaly attributes and normal ones that were reduced to 9. The author used minmax normalization method splitting the data into training and testing datasets 80%,20% for reaching the highest accuracy possible with the lowest number of features. The Detection and prevention part of the systems is based on Correlation Feature Selection (CFS) for the filtration of the data including probability. Entropy and IG, where the probability of a feature being there is used to get the correlation between different attributes through a dynamically build confidence matrix through the calculation of the entropy. The system was based on different classifiers including SVM, Random Forest (RF), KNN, Decision Tree (DT) and the results of the data showed that the highest accuracy rate and true positive was for the RF against the three different protocols followed by KNN then DT. The results of the FR classifier for the TCP DDOS had the highest accuracy 98.5% followed by ICMP 95.86% then UDP at 93.45%and the true positive rate for the TCP was 99.45% followed by the UDP at 93.7% and the ICMP had a 66.6% [30].

We summarized the discussed frameworks Table 1 which is displayed at the end of the article, where we highlighted the actual defense approach followed in in each proposed framework, with the type of DDOS attack mentioned, and brief comment on each proposed framework. The purpose of the table is to create an overview of the current situation when it comes to recent techniques used in defense mechanism of DDOS in cloud.

4 CONCLUSION AND FUTURE WORK

Throughout our study we briefly highlighted the importance of protecting the cloud technology against DDOS attacks and how they work and what they target. After that we offered an extensive study of the different prevention, detection, and mitigations techniques that are used to protect against DDOS attacks and following that we gathered the state of art frameworks that have been proposed through the years 2017 and 2021. It has been clear throughout our research that different studies only focused on the broad classification of the techniques used in handling the DDOS and most of the time not all of the three approaches have been discussed deeply which lead us to gather as much information about them and discussing them in depth. The protection against DDOS includes approaches like challenge response, hidden/server, recourse limiting, and restrictive access, while detection included a lot of techniques to our findings the main approaches included signature based, anomaly based, hybrid, resource usage, bot-cloud, CBF, and spoofing based detection, while mitigation approaches included SDN, DMaaS, resource scaling, and victim mitigation approaches. Additionally, it has been also clear that most of the work that is done focus on the detection of the attack through different approaches where most of the frameworks were based on machine learning and anomaly detection mechanisms. The problem with the current situation is that even though the authors claim that the frameworks proposed are detection and prevention frameworks or detection and mitigation frameworks they are only detection and none of the approaches of mitigation or preventions were used. Not only that but also most of the frameworks only focus on a flooding and high rate DDOS attacks while the Low-rate attacks are harder to capture due to its different nature and yet it is not getting much attention in research. We propose that more work should be done to handle Low-rate DDOS and also handling more than a single specific type of brute-force attacks, along with the creation of a framework that actually integrates the three different approaches together would result in a better cloud environment.

REFERENCES

[1] A. E. Khedr and A. M. Idrees, "Enhanced e-Learning System for e-Courses Based on Cloud Computing," *Journal of Computers,* vol. 12, no. 1, 2017.

[2] A. A. T. F. U. &. T. M. A. Amjad, "Endorsed Transactions Detection and mitigation of DDoS attack in cloud computing using machine learning algorithm," *EAI ,* vol. 6, no. 23, 2019.

[3] A. E. Khedr and A. M. Idrees, "Adapting Load Balancing Techniques for Improving the Performance of e-Learning Educational Process," *Journal of Computers,* vol. 12, no. 3, pp. 250-257, 2017.

[4] D. Radain, S. Almalki, H. Alsaadi and Shaima Salama, "A Review on Defense Mechanisms Against Distributed Denial of Service (DDoS) Attacks on Cloud Computin," in *BOURNEMOUTH UNIVERSITY*, 2021.

[5] G. G. M. S. S. D. C. M. &. B. R. Somani, "DDoS Attacks in Cloud Computing: Issues, Taxonomy, and Future Directions," *Computer Communications.,* 2017.

[6] H. Abusaimeh, "Distributed denial of service attacks in cloud computing," *International Journal of Advanced Computer Science and Applications,,* vol. 11, no. 6, pp. 163-168, 2020.

[7] A. Bakr, A. A. Abd El-Aziz and H. A. Hefny, "A survey on mitigation techniques against ddos attacks on cloud computing," *International Journal of Advanced Science and Technology,* vol. 28, no. 12, p. 187–200, 2019.

[8] A. Shameli-Sendi, M. Pourzandi, M. Fekih-Ahmed and M. Cheriet, "Taxonomy of distributed denial of service mitigation approaches for cloud computing," *Journal of Network and Computer Applications,* vol. 58, pp. 165-179, Dec 2015.

[9] A. Praseed and P. S. Thilagam, "DDoS Attacks at the Application Layer: Challenges and Research Perspectives for Safeguarding Web Applications," *IEEE Communications Surveys & Tutorials,* vol. 21, no. 1, pp. 661-685, 2019.

[10] 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 and Tutorials,* vol. 21, no. 4, pp. 3769-2795, 2019.

[11] N. Agrawal and S. Tapaswi, "Defense schemes for variants of distributed denial-of-service (DDoS) attacks in cloud computing : A survey," *Information Security Journal: A GlobalPrespective,* pp. 1-13, 2017.

[12] G. Somani, "Combating DDoS Attacks in the Cloud : Requirements , Trends , and Future Directions.," 2015.

[13] Alarqan, M. A, F. Z. Zaaba and A. Almomani, "Detection Mechanisms of DDoS Attack in Cloud Computing Environment: A Survey," *VFAST Transactions on Software Engineering,* 2020.

[14] A. Bhardwaj, V. Mangat, R. Vig, S. Halder and C, "Distributed denial of service attacks in cloud : State-of-the-art of scientific and commercial solutions," vol. 39, 2021.

[15] M. Alyas, "A SURVEY OF DDOS ATTACK DETECTION STRATEGIES IN CLOUD," *VFAST Transactions on Software Engineering,* vol. 8, no. 1, pp. 55-63, 2016.

[16] J. N. Ahamed and N. Lyengar, "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.

[17] R. Divyasree and K. Selvamani, "Defeating the Distributed Denial of Service Attack in Cloud Environment : A Surve," 2017.

[18] "Future Directions. DDoS Attacks in Cloud Computing: Issues, Taxonomy, and Future Directions," 2017.

[19] K. Srinivasan and A. Mubarakali, "A Survey on the Impact of DDoS Attacks in Cloud Computing : Prevention , Detection and Mitigation Techniques," *Springer International Publishing,* vol. 2, 2020.

[20] M. Zareapoor , P. Shamso and M. A. Alam, "Advance DDOS detection and mitigation technique for securing cloud," *Int. J. Computational Science and Engineering,* vol. 16, no. 3, pp. 303-310, 2018.

[21] M. S. Hezavehi and R. Rahmani, "An anomaly-based framework for mitigating effects of DDoS attacks using a third party auditor in cloud computing enviro," *pringer Science+Business Media, LLC, part of Springer Nature 2020,* 2018.

[22] V. Balamurugan and R. Saravanan, "Enhanced intrusion detection and prevention system on cloud environment using hybrid classification and OTS generation," *Cluster Computing,* 2017.

[23] R. Saxena, "DDoS prevention using third party auditor in cloud computing.," *Iran Journal of Computer Science,* 2019.

[24] A. Sahi, D. Lai, Y. A. N. Li and M. Diykh, "An Efficient DDoS TCP Flood Attack Detection and Prevention System in a Cloud Environment," *IEEE Access,* vol. 5, pp. 6036-6048, 2017.

[25] B. Al-Duwairi, O. Özkasap, A. Uysal, C. Kocaogullar and K. Yildirim, "LogDoS : A Novel logging-based DDoS prevention mechanism in path identi fi er-Based information centric networks," *Computer and Security 99,* 2020.

[26] M. Rathore and A. Vaish, "A system design for multi-phase , hybrid DDoS detection," *Computer Fraud & Security Bulletin,,* vol. 11, pp. 10-19, 2020.

[27] M. Idammad, K. Afdel and M. Belouch, "Detection System of HTTP DDoS Attacks in a Cloud Environment Based on Information Theoretic Entropy and Random Forest," *Security and Communication Networks,* june 2018.

[28] A. A. A. ALi and S. A. F. Osman, "Efficient DDoS Attack Detection and Prevention Framework Using Two-Level Classification in Cloud Environment," *International Journal of Computer Science and Mobile Computing,* vol. 7, no. 8, pp. 1-7, 2018.

[29] A. Saravanan, S. SathyaBama, S. Kadry and L. R. Ramasa, "A new framework to alleviate DDoS vulnerabilities in cloud computing," *Journal, I., & Engineering, C,* 2019.

[30] A. Moqeet, A machine Learning Based Classification Technique to Detect DDOS Attack in Cloud Computing enviroment, 2021.

Table 1: DDOS Defense Approaches' analysis

Reference	Year	Defense approach			Type of DDOS attack	Comments
		Preventio	Detection	Mitigatio		
[30]	2021		√		UDP, TCP, ICM	Entropy based system for detecting more than one type of DDOS. The system is introduced as a detection and prevention systems but it's only a detection.
[25]	2020		√		Flooding attack	Detection based on logging get messages and the overhead is handled
[26]	2020		√		High rate and low rate DDOS	Hybrid anomaly 2 phase detection
[21]	2020			√	Not specified	Anomaly based Detection not prevention
[29]	2019	√			Not specified	Challenge response-based prevention proposed only framework
[23]	2019	√			Flooding DDOS	ID based detection not prevention
[2]	2019		√	√	Ping of death	NB anomaly-based detection, no mitigation techniques used
[28]	2018	√	√		Flooding attacks	Fuzzy logic-based detection the prevention is an extra security after the detection
[27]	2018		√		HHTP flooding attack	Entropy anomaly detection based on time window and used 3 classifier algorithms
[20]	2018		√	√	Not specified	Anomaly based detection not mitigation with low storage space
[24]	2017	√	√		TCP flooding DDOS	ML (SVM) based detection only no prevention
[22]	2017	√	√		Not specified	Hybrid based detection and the prevention is an extra security after the detection