A SECURED AND ENHANCED MITIGATION FRAMEWORK FOR DDOS ATTACKS

Mujahid shah¹, ShahbazQadar Khattak², Muhammad Farooq³, Sadeeq Jan², MehtabEjaz Qureshi⁴, Naveed Jan⁵, Sheeraz Ahmed¹,⁴

¹IQRA National University, Peshawar, Pakistan
²National Center for Cyber Security, Uni of Engg& Tech Peshawar, Pakistan
³University of Science and Technology, Bannu, Pakistan
⁴Hajvery University, Lahore, Pakistan
⁵University of Technology, Nowshera, Pakistan

https://doi.org/10.26782/jmcms.2019.12.00075

Abstract

DDoS attacks are initiated from various locations around the world and can be started very easily. This can be achieved by thwarting access to virtually anything: servers, devices, services, networks, applications, and even specific transactions within applications. In a DoS attack, its one system that is sending the malicious data or requests; a DDoS attack comes from multiple systems. Generally, these attacks work by drowning a system with requests for data. This could be sending a web server so many requests to serve a page that it crashes under the demand, or it could be a database being hit with a high volume of queries. The result is available internet bandwidth, CPU and RAM capacity becomes overwhelmed. Distinguishing between attack traffic and normal traffic is difficult, especially in the case of a application layer attack such as a botnet performing a HTTP Flood attack against a victim’s server. Because each bot in a botnet makes seemingly legitimate network requests the traffic is not spoofed and may appear “normal” in origin. In this research propose DDoS attack mitigation framework, the framework composed two parts proactive approach and reactive approach, proactive approach further contain four components Secure software development life cycle, application load test application stress test and ddos incident response plan, while reactive approach contain eighth components bandwidth management, perimeter firewall, intrusion detection and prevention system, web application firewall, load balancer, endpoint security firewall, Dedicated DDoS mitigation device and monitoring, collectively this framework will help as to design such infrastructure which will be stopping DDoS attack enough so that they attacker cannot be easily breakdown and unavailability of the services should accessible.
Keywords: DDoS attack, Application Layer Attack, Attack detection, botnet, DDoS framework

I. Introduction

A distributed denial-of-service (DDoS) attack is one of the most powerful weapons on the internet. When you hear about a website being “brought down by hackers,” it generally means it has become a victim of a DDoS attack. In short, this means that hackers have attempted to make a website or computer unavailable by flooding or crashing the website with too much traffic. Distributed denial-of-service attacks target websites and online services. The aim is to overwhelm them with more traffic than the server or network can accommodate. The goal is to render the website or service inoperable. The traffic can consist of incoming messages, requests for connections, or fake packets. In some cases, the targeted victims are threatened with a DDoS attack or attacked at a low level. This may be combined with an extortion threat of a more devastating attack unless the company pays a crypto currency ransom.

In 2015 and 2016, a criminal group called the Armada Collective repeatedly extorted banks, web host providers, and others in this way. The primary way a DDoS is accomplished is through a network of remotely controlled, hacked computers or bots. These are often referred to as “zombie computers.” They form what is known as a “botnet” or network of bots. These are used to flood targeted websites, servers, and networks with more data than they can accommodate. The botnets may send more connection requests than a server can handle or send overwhelming amounts of data that exceed the bandwidth capabilities of the targeted victim. Botnets can range from thousands to millions of computers controlled by cybercriminals. Cybercriminals use botnets for a variety of purposes, including sending spam and forms of malware such as ransomware. Your computer may be a part of a botnet, without you knowing it. Increasingly, the millions of devices that constitute the ever-expanding Internet of Things (IoT) are being hacked and used to become part of the botnets used to deliver DDoS attacks. The security of devices that make up the Internet of Things is generally not as advanced as the security software found in computers and laptops. That can leave the devices vulnerable for cybercriminals to exploit in creating more expansive botnets.

The 2016 Dyn attack was accomplished through Mirai malware, which created a botnet of IoT devices, including cameras, smart televisions, printers and baby monitors. The Mirai botnet of Internet of Things devices may be even more dangerous than it first appeared. That’s because Mirai was the first open-source code botnet. That means the code used to create the botnet is available to cybercriminals who can mutate it and evolve it for use in future DDoS attacks.
The authors applied an organized flow of feature engineering and machine learning to detect distributed denial-of-service (DDoS) attacks. Feature engineering has a focus to obtain the datasets of different dimensions with significant features, using feature selection methods of backward elimination, chi2, and information gain scores[1]. Different supervised machine learning models are applied on the feature-engineered datasets to demonstrate the adaptability of datasets for machine learning under optimal tuning of parameters within given sets of values. The results show that substantial feature reduction is possible to make DDoS detection faster and optimized with minimal performance hit. The authors proposed a DDoS attack detection and defense mechanism based on cognitive-inspired computing with dual address entropy is proposed. The flow table characteristics of the switch are extracted, and a DDoS attack model is built by incorporating the support vector machine classification algorithm. This mechanism can realize real-time detection and defense at the preliminary stage of the DDoS attack and can restore normal communication in time[II]. The experiment shows that our mechanism not only detects attacks quickly but also has a high detection rate and low false positive rate. More importantly, it can take appropriate defense and recovery measures in the time after the attack has been identifieddetection. The proposed mitigation schema models the rule assignment to defense stages as a Generalized Assignment Problem. Items, i.e. generic mitigation rules, are assigned to bins, i.e. defense stages, based on capacity constraints and reward values guided by operator policies. Our approach considers reducing the GAP input size to enable reasonable execution of the resulting integer programming formulation. During the mid to late 1990s, when Internet Relay Chat (IRC) was first becoming popular, some users fought for control of non-registered chat channels, where an administrative user would lose his or her powers if he or she logged off. This behaviour led hackers to attempt to force users within a channel to all log out, so they could enter the channel alone and gain administrator privileges as the only user.
present. These “king of the hill” battles—in which users would attempt to take control of an IRC channel and hold it in the face of attacks from other hackers—were fought using very simple bandwidth-based DoS attacks and IRC chat floods.

One of the first large-scale DDoS attacks occurred in August 1999, when a hacker used a tool called “Trinoo” to disable the University of Minnesota’s computer network for more than two days. Trinoo consisted of a network of compromised machines called “Masters” and “Daemons,” allowing an attacker to send a DoS instruction to a few Masters, which then forwarded instructions to the hundreds of Daemons to commence a UDP flood against the target IP address. The tool made no effort to hide the Daemons’ IP addresses, so the owners of the attacking systems were contacted and had no idea that their systems had been compromised and were being used in a DDoS attack. Other early tools include “Stacheldraht” (German for barbed wire), which could be remotely updated and support IP spoofing, along with “Shaft” and “Omega”, tools that could collect attack statistics from victims.

Because hackers were able to get information about their DDoS attacks, they could better understand the effect of certain types of attacks, as well as receive notification when a DDoS attack was detected and stopped. Once hackers began to focus on DDoS attacks, DoS attacks attracted public attention. The distributed nature of a DDoS attack makes it significantly more powerful, as well as harder to identify and block its source. With such a formidable weapon in their arsenals, hackers began to take on larger, more prominent targets using improved tools and methods. By the new millennium, DDoS captured the public’s attention. In the year 2000, various businesses, financial institutions and government agencies were all brought down by DDoS attacks. Shortly after, DNS attacks began with all 13 of the Internet’s root domain name service (DNS) servers being attacked in 2002.

DNS is an essential Internet service, as it translates host names in the form of uniform resource locators (URLs) into IP addresses. In effect, DNS is a phonebook maintaining a master list of all Internet addresses and their corresponding URLs. Without DNS, users would not be able to efficiently navigate the Internet, as visiting a website or contacting a specific device would require knowledge of its IP address. Application layer attacks or layer 7 (L7) DDoS attacks refer to a type of malicious behaviour designed to target the “top” layer in the OSI model where common internet requests such as HTTP GET and HTTP POST occur. These layer 7 attacks, in contrast to network layer attacks such as DNS Amplification, are particularly effective due to their consumption of server resources in addition to network resources.
There are three basic categories of attack:

1. Volume-based attacks, which use high traffic to inundate the network bandwidth

2. Protocol attacks, which focus on exploiting server resources
iii. Application attacks, which focus on web applications and are considered the most sophisticated and serious type of attacks

**Figure 5: Application Layer attack**

Different types of attacks fall into categories based on the traffic quantity and the vulnerabilities being targeted.

**II. Literature Review**

The authors proposed many detection and defense techniques to protect cloud computing against DDoS attacks. The authors presented a review of many detection techniques that are useful in spotting DDoS attacks that are cloud-based and make a comparative analysis between them to find a suitable technique for spotting these clouds computing based DDoS attacks [III].

**Figure 7. Cloud computing architecture**
The authors analyzed three major components of DDoS defense mechanisms such as DDoS detection, DDoS mitigation, and IP traceback. In the first step, need to detect all DDoS attacks using any intrusion detection system to pinpoint the exact packet characteristics of the attack. The researchers classify the attack traffic based on packet characteristics[IV]. The authors presented SEAL (SEcure and AgiLe) – a novel Software Defined Networking (SDN) based adaptive framework for protecting smart city applications against DDoS attacks. The SEAL framework leverages key characteristics of SDN such as the global visibility, centralized control, and programmability to enhance the security and resilience. SEAL is capable of effectively detecting and mitigating DDoS attacks not only on application servers but also on network resources. SEAL is also unique in this regard that it provides application specific DDoS attack security solution instead of static threshold mechanism. Moreover, inherently distributed architecture of the SEAL framework ensures fault tolerance, scalability and reliability of the smart city. The SEAL framework comprises three modules, namely D-Defense, A-Defense and C-Defense. These modules collectively provide a mechanism to detect and mitigate DDoS attack on smart city applications and the network infrastructure. Adaptability in SEAL is achieved through implementing customized version of estimated-weighted moving average (EWMA) filters. Three types of filters, Proactive Filter, Active Filter, and Passive Filter are proposed and implemented to compute the dynamic threshold in real time for various types of applications. Experimental evaluation of the SEAL framework has been conducted to establish the efficacy of the framework and its components in detecting and mitigating DDoS attacks. The results prove that SEAL is able to detect and mitigate DDoS attacks effectively. The focus of the SEAL framework is to protect smart city applications; however, the SEAL framework can potentially be utilized in a wide range of systems[V].

The authors focused on Machine Learning techniques to detect DDoS attack in network communication flows using continuous learning algorithm that learns the normal pattern of network traffic, behavior of the network protocols and identify a compromised network flow. Detection of DDoS attack will help the network administrators to take immediate action and mitigate the impact of such attacks. DDoS attacks are costing enterprises anywhere between $50,000 to $2.3 million per year[VI]. The authors proposed DAD-MCNN, a multi-channel CNN(MC-CNN) based DDoS attack detection framework, which can fully utilize information from a huge amount of network packages and set up an earlier warning system. Our contributions can be summarized as follows: (1) the researches proposed a new preprocessing method for the network dataset. (2) MC-CNN is applied to detect DDoS attack and the detection result is decided by data in respective channels. (3) the authors used incremental training method to optimize training procedures and time in MC-CNN. (4) The experiment result shows that MC-CNN has the highest accuracy compared
with conventional machine learning methods. The result also proves that our approach has performed well not only in DDoS attack detection but also in another anomaly attack\[VII\].

The authors provided a clustering-based approach to distinguish the data representing flows of network traffic which include both normal and Distributed Denial of Service (DDoS) traffic. The features are taken for victim-end identification of attacks and the work is demonstrated with three features which can be monitored at the target machine. The clustering methods include agglomerative and K-means with feature extraction under Principal Component Analysis (PCA). A voting method is also proposed to label the data and obtain classes to distinguish attacks from normal traffic. After labeling, supervised machine learning algorithms of k-Nearest Neighbors (kNN), Support Vector Machine (SVM) and Random Forest (RF) are applied to obtain the trained models for future classification\[VIII\]. Focus on internal DoS/DDoS attacks launched against the WAMS devices by exploiting the vulnerabilities. To counter such attacks, the researchers proposed a proactive and robust extension of the Multipath-TCP (MPTCP) transportation protocol, termed as MPTCP-H. The proposed extension mitigates the internal attacks by using a novel stream hopping mechanism, which periodically renews the sub flows to hide the open port numbers of the connection. By doing so, MPTCP-H significantly increases the attacker’s cost for a successful attack without perturbing the WAMS data trace. The experimental results show that the proposed MPTCP-H provides a significant DoS/DDoS attack mitigation for WAMS at the expense of reasonable overheads, i.e., additional latency and message \[IX\]. This article explores the 5G security by combining the physical layer and the logical layer from the perspective of automated attack and defense, and dedicate to provide automated solution framework for 5G security \[X\].

The authors presented the state of art of the DDoS attacks in SDN and cloud computing scenarios. Especially, focus on the analysis of SDN and cloud computing architecture. Besides, the researchers also overviewed the research works and open problems in identifying and tackling the DDoS attacks\[XI\]. The schoolers provided a comprehensive overview of different mitigation approaches and categorizes them into three different classes on the basis of their methodology to handle the malicious traffic. In addition to that, the researchers found out some possible limitations in these mitigation approaches and propose the possible features of an optimal solution against DoS attacks. To the best of researchers’ knowledge, this work is the first attempt toward the classification of DoS mitigation strategies and to find out their limitations in the SDN environment\[XII\].

The authors proposed a method and system for controlling multi-tiered mitigation of cyber-attacks. The method comprises monitoring at least availability.
and load of each protection resource in a multi-tiered communication network, wherein each tier in the multi-tiered communication network includes a plurality of protection resources having capacity and security capabilities set according to the respective tier; for each protection resource, computing a current aggregated load metric (ALM); determining based on at least one of the computed ALM and security capabilities of a respective protection resource, if the respective protection resource assigned to a protected entity can efficiently handle a detected cyber-attack against the protected entity; and selecting at least one new protection resource to secure the protected entity upon determining the protection resource cannot efficiently handle the detected cyber-attack, wherein the selection is based on at least one of the computed ALM and a security capabilities of the at least one protection resource.[XIII]. The authors incorporated various machine learning algorithms: Support Vector Machine, Naïve Bayes, and Random Forest for classification and overall accuracy was 99.7%, 97.6% and 98.0% of Support Vector Machine, Random Forest and Naïve Bayes respectively.[XIV].

Figure 6. Depicts the DDoS Attack on Owncloud

The authors presented the recent detection methods of DDoS attack at the application layer and highlights several recommendations for future research[XV].

Figure 9. Web server architecture
The authors designed a novel Chinese Remainder Theorem based Reversible Sketch (CRT-RS). CRT-RS is not only capable of compressing and fusing big-volume network traffic but also has the ability of reversely discovering the anomalous keys (e.g., the sources of malicious or unwanted traffic). Then, based on traffic records generated by CRT-RS, the researchers proposed a Modified Multi-chart Cumulative Sum (MM-CUSUM) algorithm that supports self-adaptive and protocol independent detection to detect DDoS flooding attacks. The performance of the proposed detection method is experimentally examined by two open source datasets [XVI].

The authors Disclosed systems and methods for detecting distributed denial of-service (DDoS) attack. An exemplary method includes receiving one or more requests from a first user for a service executing on a server, and generating a first vector associated with the first user comprised of a plurality of characteristics indicative of the first user accessing the service; calculating a comparison between the first vector and a reference vector [XVII]. The authors proposed a stacked self-organizing map, which is a feature dynamic deep learning approach that utilizes NetFlow data collected by the ISP to combat the dynamic nature of novel DDoS attacks [XVIII].

The authors evaluated a few machine learning techniques, i.e., J48, Random Forest (RF), Support Vector Machine (SVM), and K-Nearest Neighbors (K-NN), to detect and block the DDoS attack in an SDN network. The evaluation process involved training and selecting the best model for the proposed network and applying it in a mitigation and prevention script to detect and mitigate attacks. The results showed that J48 performs better than the other evaluated algorithms, especially in terms of training and testing time [XIX].
The authors one embodiment, a distributed denial of service attack on a network is identified. In response to the distributed denial of service attack, a script to request a short-term certificate is executed. The short-term certificate is generated by a certificate server and received either directly or indirectly from the certificate server. An instruction to redirect traffic using the short-term certificate and private key is sent to a distributed denial of service attack protection service that is operable to filter or otherwise mitigate malicious traffic involved in the distributed denial of service attack[XX]. The authors proposed intended to make underlying network intelligent enough so as to prevent DNS based DDoS attacks[XXI].

The authors proposed several machine learning algorithms have been adopted to predict and classify malicious user or Denial of Service (DDoS) attack from a user, using private network data in SDN based environment. The purpose of using ML in SDN environment is to leverage the ML approach so that security rules on SDN controller can be defined to block the potential attackers as well as their entire subnet. To accomplish the goal Mininet (an open-source emulation software) had been used for creating and simulating an SDN-based testbed and WEKA (an open-source machine learning software) had been used to build, test, and compare different machine learning models[XXII].

![Figure 10. Overview of intrusion detection system](image)

The authors a detailed study on DDoS threats prevalent in SDN is presented. First, SDN features are examined from the perspective of security, and then a discussion on SDN security features is done. Further, two viewpoints on protecting networks against DDoS attacks are presented. In the first view, SDN utilizes its abilities to secure conventional networks. In the second view, SDN may become a victim of the threat itself because of the centralized control mechanism. The main focus of this research work is on discovering critical security implications in SDN while reviewing the current ongoing research studies. By emphasizing the available state-of-the-art
techniques, an extensive review of the advancement of SDN security is provided to the research and IT communities[XXIII].

Figure 11. Link discovery with LLDP

The authors proposed method includes receiving, by a detector, a plurality of data feeds from a plurality of data sources, wherein the detector is communicatively connected to the plurality of data sources; processing, by the detector, the plurality of received data feeds to generate enriched Flow data sets; analyzing the enriched Flow data sets to detect a potential cyber-attack; and upon detection of a potential cyber-attack, providing indication to each network entity of the network entities that is under attack[XXIV].

Proposed DDoS Attack Mitigation Framework

This framework composes two major parts proactive approach and reactive approach.
II.i Proactive approach contains four elements.

a) Secure Software Development Lifecycle

A Secure SDLC process ensures that security assurance activities such as penetration testing, code review, and architecture analysis are an integral part of the development effort. The primary advantages of pursuing a Secure SDLC approach are: The criminals or novice hackers can break into an organization's network through various routes and one such route is the application host. If applications are hosted by an organization are vulnerable, it can lead to serious consequences. Adopting a secure SDLC will help the organization to secure their application from cyber threats proactively.

b) Application Load and Stress Test:

Extreme load conditions are rarely seen in production. Therefore, stress testing benefits organizations by revealing application issues that only become apparent...
under these extreme conditions. Proper stress tests can also help organizations uncover the following:

- DDoS attack situation
- Synchronization and timing bugs
- Interlock problems
- Priority problems
- Resource loss bugs
- Memory leaks
- Data loss & corruption
- Utilizing stress testing tools

When approaching stress testing, want first identify test objectives, key scenarios, the workload you want to apply, and the metrics you’ll be tracking. After you’ve created your test cases, work with a stress testing tool to simulate the required load for each test case and capture performance metrics. Reaching the Breaking Point Stress testing is an essential and beneficial process that provides otherwise unattainable insight into the performance of your web and mobile applications under extreme load. Identifying the potential breaking points in your application will allow you to correct them before they become expensive issues in production.

Figure 14: Stress and Load Test

c) Incident Response Plan.

One of the biggest assets of an effective proactive incident response plan is a better ability to prevent crime. Cyber threats are, unfortunately, exceedingly common, especially when your company has something valuable to offer, like healthcare information or personal financial records. Rather than living in fear, a proactive plan...
makes it easier to see when these kinds of threats are forthcoming. Thinking proactively offers numerous advantages to your crime prevention strategies, allowing you to better detect malicious activity and abnormalities. The more you know about your environment in a normal state, the quicker you will be able to identify an incident in the early stages. Rather than striking back after an assault has been initiated, you can do your best to stop an attack in its tracks when appropriate proactive measures are in place. Reduced Investigative Costs Facing a cyber-attack comes with many necessary tasks, from investigating the source of a breach to implementing additional security measures to prevent current weaknesses from leading to further complications. Companies who do not prepare for the enduring possibility of attack are often shell shocked when something happens, making the investigation process longer and harder than ultimately necessary, but those who do are much more likely to be ready to take action.

A proactive incident response plan assumes that incidents are always possible, which makes acting on an issue much easier. Engaging with or, at the very least, identifying reputable outside resources can help reduce the price and turnaround time of negotiating during an incident. In addition, you won't lose any time looking, vetting, and contacting investigative agencies; instead, you'll be ready for anything at the first sign of trouble. No one wants to keep investigative resources on speed dial, but when something happens, you'll be glad the connections are there.

The incident response phases are:

- Preparation
- Identification
- Containment
- Eradication
- Recovery
- Lessons Learned
SIX PRIMARY PHASES

1. Reactive approach
   - DDoS dedicated device or solution
   - Bandwidth Management
   - Perimeter Firewall
   - IPS/IDS
   - WAF
   - Load Balancer
   - End Point Security Firewall
   - Monitoring

Figure 15: Incident Response Plane
Internet. While a proxy server protects a client machine’s identity by using an intermediate layer between the client and the Internet. A shield is placed between the web application and the Internet. This method of attack mitigation is usually part of a suite of tools which together create a holistic defence against a range of attack vectors. By deploying a WAF in front of a web application, a shield is placed between the web application and the Internet. A WAF or Web Application Firewall helps protect web applications by filtering and blocking malicious traffic. It typically conducts inspections of control traffic (network and application headers), not DPI, to determine whether there is a DDoS attack present or not, and instantaneously mitigate the attack at line rates of tens of Gbps. The main purpose is to ensure that good traffic always get through, while making sure the effects of DDoS attacks are minimized. Firewalls provide perimeter access control by monitoring and tracking permitted network traffic flows.

In many ways, a firewall plays the role of a network’s traffic cop. It allows the good packets to proceed unimpeded and blocks bad packets from gaining access to the network. Firewalls can also be helpful in detecting an incoming DDoS attack. An IPS is deployed deeper in the network, typically behind the firewall. It is designed to prevent intrusions such as server exploits, code injections, cross site scripting attempts, etc. and thus performs deep packet inspection (DPI) to prevent these intrusions because they mainly occur at the application layer. A WAF or Web Application Firewall helps protect web applications by filtering and monitoring HTTP traffic between a web application and the Internet. It typically protects web applications from attacks such as cross-site forgery, cross-site-scripting (XSS), file inclusion, and SQL injection, among others. A WAF is a protocol layer 7 defence (in the OSI model), and is not designed to defend against all types of attacks. This method of attack mitigation is usually part of a suite of tools which together create a holistic defence against a range of attack vectors. By deploying a WAF in front of a web application, a shield is placed between the web application and the Internet. While a proxy server protects a client machine’s identity by using an intermediate layer between the client and the Internet.

Figure 16: Reactive DDoS Mitigation Infrastructure

In the figure a DDoS mitigation system deployed in-line and at the edge of the network it is the most effective protection against DDoS. A DDoS mitigation system conducts inspections of control traffic (network and application headers), not DPI, to determine whether there is a DDoS attack present or not, and instantaneously mitigate the attack at line rates of tens of Gbps. The main purpose is to ensure that good traffic always get through, while making sure the effects of DDoS attacks are minimized. Firewalls provide perimeter access control by monitoring and tracking permitted network traffic flows.
intermediary, a WAF is a type of reverse-proxy, protecting the server from exposure by having clients pass through the WAF before reaching the server. Load balancing refers to efficiently distributing incoming network traffic across a group of backend servers. A load balancer acts as the “traffic cop” sitting in front of your servers and routing client requests across all servers capable of fulfilling those requests in a manner that maximizes speed and capacity utilization and ensures that no one server is overworked, which could degrade performance. If a single server goes down, the load balancer redirects traffic to the remaining online servers. When a new server is added to the server group, the load balancer automatically starts to send requests to it. Endpoint security software protects these points of entry from risky activity and/or malicious attack. When companies can ensure endpoint compliance with data security standards, they can maintain greater control over the growing number and type of access points to the network.

III. Conclusion and Future Work

In this research paper proposed a DDoS mitigation framework, the framework comprises of two approaches one proactive approach and second reactive approach, organization adopt this framework will reduce or mitigated DDoS attack, proactive approach address application vulnerability in development stage before the application going online, in the first stage the organization also know the breakpoint of application using stress and load testing, incident response plan help the organization will ready to cope with incident properly. Reactive approach helps the organization to stop the DDoS attack in various layer also generate alert to the administrator about attacks, in this research these two approaches make an effectively DDoS mitigation framework. For future, this research to distinguish an application layer’s DDoS attack from flash event through examining their various behaviors of access.

References

I. Aamir, Muhammad, and Syed Mustafa Ali Zaidi. "Clustering based semi-supervised machine learning for DDoS attack classification." Journal of King Saud University-Computer and Information Sciences (2019).

II. Aamir, Muhammad, and Syed Mustafa Ali Zaidi. "DDoS attack detection with feature engineering and machine learning: the framework and performance evaluation." International Journal of Information Security (2019): 1-25.
III. Alanazi, Sultan T., Mohammed Anbar, Shankar Karuppayah, Ahmed K. Al-Ani, and Yousef K. Sanjalawe. "Detection Techniques for DDoS Attacks in Cloud Environment." In *Intelligent and Interactive Computing*, pp. 337-354. Springer, Singapore, 2019.

IV. Amjad, Aroosh, Tahir Alyas, Umer Farooq, and Muhammad Arslan Tariq. "Detection and mitigation of DDoS attack in cloud computing using machine learning algorithm." (2019).

V. Bawany, Narmeen Zakaria, and Jawwad A. Shamsi. "SEAL: SDN based secure and agile framework for protecting smart city applications from DDoS attacks." *Journal of Network and Computer Applications* 145 (2019): 102381.

VI. Chen, Jinyin, Yi-tao Yang, Ke-ke Hu, Hai-bin Zheng, and Zhen Wang. "DAD-MCNN: DDoS Attack Detection via Multi-channel CNN." In *Proceedings of the 2019 11th International Conference on Machine Learning and Computing*, pp. 484-488. ACM, 2019.

VII. Cui, Jie, Mingjun Wang, Yonglong Luo, and Hong Zhong. "DDoS detection and defense mechanism based on cognitive-inspired computing in SDN." *Future Generation Computer Systems* 97 (2019): 275-283.

VIII. Dayanandam, G., T. V. Rao, D. BujiBabu, and S. Nalini Durga. "DDoS Attacks—Analysis and Prevention." In *Innovations in Computer Science and Engineering*, pp. 1-10. Springer, Singapore, 2019.

IX. Demir, Kubilay, Ferdaus Nayyer, and Neeraj Suri. "MPTCP-H: A DDoS attack resilient transport protocol to secure wide area measurement systems." *International Journal of Critical Infrastructure Protection* 25 (2019): 84-101.

X. Dimolianis, Marinos, Adam Pavlidis, Dimitris Kalogeras, and Vasilis Maglaris. "Mitigation of Multi-vector Network Attacks via Orchestration of Distributed Rule Placement." In *2019 IFIP/IEEE Symposium on Integrated Network and Service Management (IM)*, pp. 162-170. IEEE, 2019.

XI. Dong, Shi, Khushnood Abbas, and Raj Jain. "A Survey on Distributed Denial of Service (DDoS) Attacks in SDN and Cloud Computing Environments." *IEEE Access* 7 (2019): 80813-80828.

XII. DORON, Ehud, B. E. N. Yotam, and David Aviv. "System and method for out of path ddos attack detection." U.S. Patent Application 16/212,042, filed June 13, 2019.

XIII. Doron, Ehud, David Aviv, B. E. N. Yotam, and Lev Medvedovsky. "Multi-tiered network architecture for mitigation of cyber-attacks." U.S. Patent Application 16/164,260, filed February 14, 2019.
XIV. Imran, Muhammad, Muhammad Hanif Durad, Farrukh Aslam Khan, and Abdelouahid Derhab. "Toward an optimal solution against denial of service attacks in software defined networks." *Future Generation Computer Systems* 92 (2019): 444-453.

XV. Jaafar, Ghafar A., Shahidan M. Abdullah, and Saifuladli Ismail. "Review of Recent Detection Methods for HTTP DDoS Attack." *Journal of Computer Networks and Communications* 2019 (2019).

XVI. Jing, Xuyang, Zheng Yan, Xueqin Jiang, and Witold Pedrycz. "Network traffic fusion and analysis against DDoS flooding attacks with a novel reversible sketch." *Information Fusion* 51 (2019): 100-113.

XVII. Khalimonenko, Alexander A., Anton V. Tikhomirov, and Sergey V. Konoplev. "System and method of determining ddos attacks." U.S. Patent Application 15/910,616, filed January 17, 2019.

XVIII. Ko, Ili, Desmond Chambers, and Enda Barrett. "Feature dynamic deep learning approach for DDoS mitigation within the ISP domain." *International Journal of Information Security* (2019): 1-18.

XIX. Lopez, Alma D., Asha P. Mohan, and Sukumaran Nair. "Network Traffic Behavioral Analytics for Detection of DDoS Attacks." *SMU Data Science Review* 2, no. 1 (2019): 14.

XX. Rahman, Obaid, Mohammad Ali Gauhar Quraishi, and Chung-Horng Lung. "DDoS Attacks Detection and Mitigation in SDN Using Machine Learning." In 2019 IEEE World Congress on Services (SERVICES), vol. 2642, pp. 184-189. IEEE, 2019.

XXI. Reddy, Tirumaleswar, Daniel Wing, and Prashanth Patil. "Short term certificate management during distributed denial of service attacks." U.S. Patent Application 10/104,119, filed October 16, 2018.

XXII. Saharan, Shail, and Vishal Gupta. "Prevention and Mitigation of DNS based DDoS attacks in SDN Environment." In 2019 11th International Conference on Communication Systems & Networks (COMSNETS), pp. 571-573. IEEE, 2019.

XXIII. Sen, Sajib, Kishor Datta Gupta, and Md Manjurul Ahsan. "Leveraging Machine Learning Approach to Setup Software-Defined Network (SDN) Controller Rules During DDoS Attack." In *Proceedings of International Joint Conference on Computational Intelligence*, pp. 49-60. Springer, Singapore, 2020.

XXIV. Swami, Rochak, Mayank Dave, and Virender Ranga. "Software-defined Networking-based DDoS Defense Mechanisms." *ACM Computing Surveys (CSUR)* 52, no. 2 (2019): 28.