iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** V **Month of publication:** May 2020

DOI: http://doi.org/10.22214/ijraset.2020.5072

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue V May 2020- Available at www.ijraset.com

Distributed Denial of Service

Kushagra Yadav[1], Akshay Pratap Singh[2], Akash Kumar Raikwar[3], Ayush Sarkari[4], Mr. Madhup Aggarwal[5]
[1, 2, 3, 4]*Fourth Year,* [5]*Assistant Professor, Department of Computer Science and Engineering, RKGIT, Ghaziabad, U.P.*

Abstract: ***With the emergence of new technologies in this technological era the cyber world has also seen an increase in the number of attacks out of which the DDOS attack remains one of the most silent yet dangerous attack. DDOS attacks are carried by professionals who have the motivation of bringing down working systems, websites due to some personal or political agenda. This research paper is intended to highlight some ways in which a DDOS attack is detected and mitigated. We will also see how Machine Learning can be helpful in mitigating the DDOS attacks.***
Keywords: DDoS Attack, Web Server, Malicious user, Bot-net, Route, Machine Learning, IP Address, Network

I. INTRODUCTION

Distributed Denial of Service Attack (DDoS) is a type of Denial of Service (DoS) attack in which a group of malicious users or a botnet tries to bring down the resources of a company which maybe a website, or a system due to their personal or political agenda. In DDoS attack a large number of requests are made simultaneously which in turn increases the bandwidth, other system resources of the target server, and makes the server inaccessible to other legitimate users and thus bringing down a server by these simultaneous requests.

What makes DDoS attacks more dangerous than the DoS (Denial of Service) attack is that unlike DOS attack, the DDoS attack comes from multiple sources simultaneously hence it becomes difficult to block connections from all these multiple sources. A new type of Denial of Service attack is the DDoS Reflector attack in which a legitimate third-party server is used to send the traffic to the victim server. The attackers send packets to the legitimate servers thus making their IP address hidden and thus making it difficult to mitigate.

II. PURPOSE AND HARM BEHIND DDOS ATTACK

DDoS attack does not involve any kind of stealing of valuable information or any kind of unauthorized access to the system. So why would anyone put a tremendous amount of effort in taking down your website? Well the answer to this could be listed below:

A. Many companies are making their way to the digital era, hence there are lot of companies that serve the same purpose. So, to minimise the competition one company might hire someone to DDoS the competitor company and if your competition is down, all the traffic will come to your website. Furthermore, it will enrich your brand value and spoil the competitor's brand value.
B. As you may know that DDoS is not about taking data. It can be used to strongly cast an opinion about any topic for political and public agenda. The web is the new battlefield and DDoS acts as a special weapon.
C. An extremely common motive behind DDoS attack could be to seek revenge upon your enemy.
D. Another motive for DDoS attacks could be for recreational purpose and to create a chaos.
E. The attackers maybe planning to launch even more bigger attack

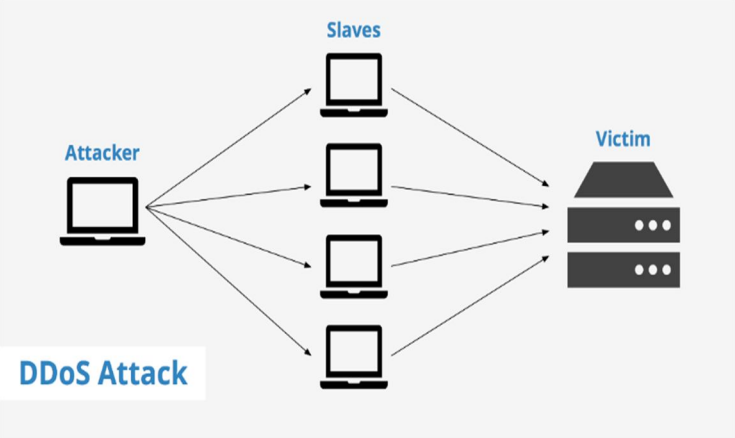


Fig. 1 Simple illustration of DDoS attack

A DDoS attack is far more dangerous than other attacks because of the following reasons:

1) Lost productivity
2) Exhaustion of system resources of the server.
3) They are used as a smokescreen to launch bigger attacks on the company.
4) The reputation of a company falls in the mind of public as long as it remains unserviceable.
5) More downtime means more loss of income.
6) Increased IT expense

III. COMMON TYPES OF DDOS ATTACKS

A network connection can be divided into 7 layers as specified in the OSI model. Different malicious users target different layers of the network connection for a successful DDoS attack. Based on this DDoS attacks can be classified into three categories.

A. *Application Layer Attacks*

This attack involves targeting the application layer of the OSI model. The main purpose of this attack is to crash the web server. This attack involves sending large number of HTTP requests which require less processing from client side but a heavy processing on the server side. This is due to the fact that web page creation requires answering the database queries and then generating a web page of the result. These types of attacks are difficult to detect as it is difficult to filter out the malicious requests from original one. The magnitude of these attacks is measured in Request per second (Rps).

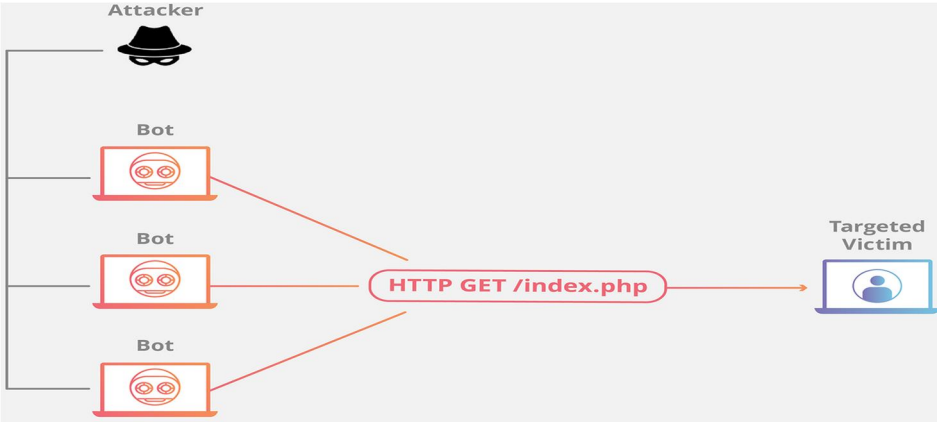


Fig. 2 Application Layer Attack Example

B. *Protocol Attacks*

This attack involves targeting the weakness in Layer 3 and Layer 4 of the OSI protocol stack. Protocol attacks also known as state exhaustion attacks, cause inaccessibility of web servers and also disturb the resources of intermediate systems such as firewalls and load balancers which are used as a measure against these attacks. It includes fragment packet attacks, Ping of Death, SYN floods. The magnitude of these attacks is measured in Packets per second (Pks).

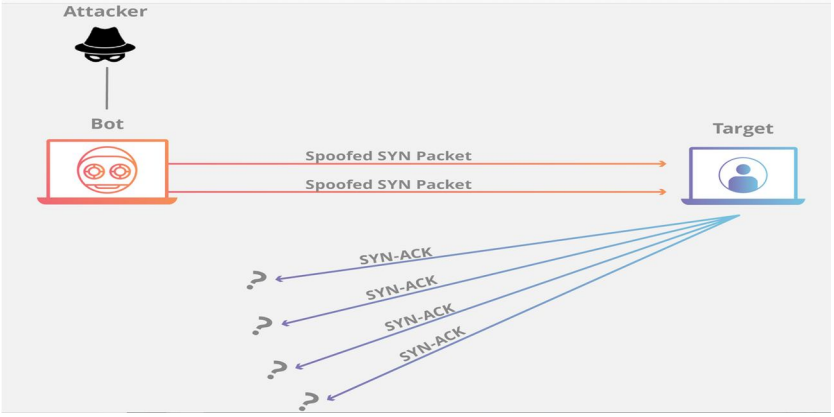


Fig. 3 Protocol Attack Example

C. Volumetric Attacks

The main purpose of this attack is to create congestion by consuming all the bandwidth of the target server so that any legitimate user cannot access the server. Large amount of traffic is sent to the target by creating a botnet. It includes UDP floods, DNS floods, ICMP floods and other type of spoofed-packet floods. The magnitude of this attack is measured in Bits per second (bps).

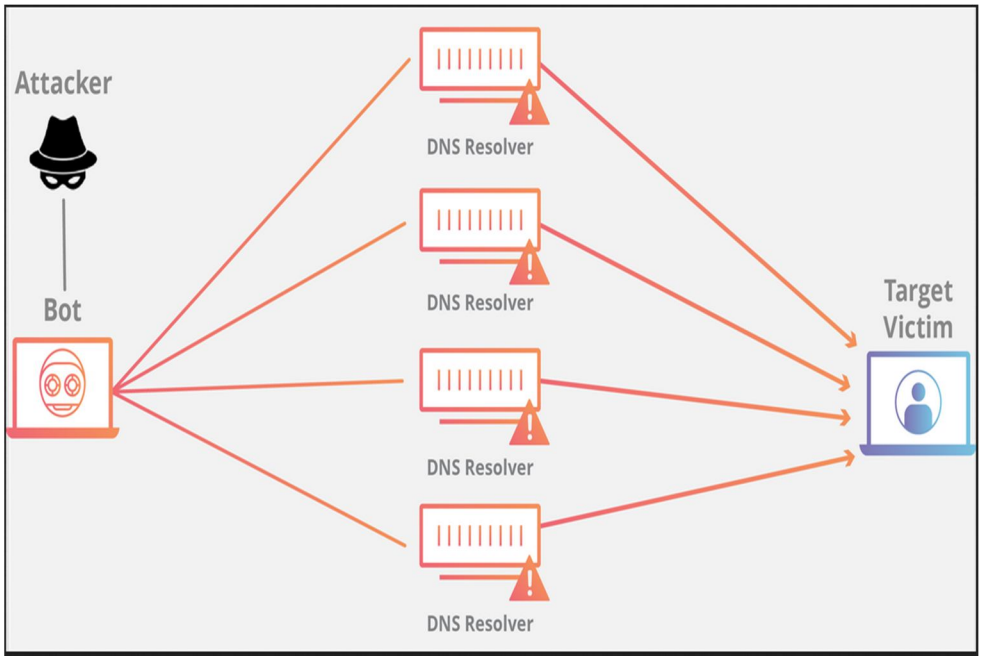


Fig. 4 Volumetric Attack Example

IV. DETECTION TECHNIQUES OF DDOS ATTACKS

The amount of DDoS attack in the last decade has increased at a rapid amount. With automation it has become easy to target organization with application layer attacks. There are numerous applications that will launch DDoS attack and requires little amount of knowledge to operate upon. To defend the organization against such attacks, organizations have various kind of prevention mechanism through which they can tackle the attacker.

A. Behal et al. [1] proposed a method of detection which is called D-Face. D-Face is used to classic traffic reaching to a server into four categories namely low rate, high rate, flash event traffic and legitimate user. Generalized information distance (GID) and generalised entropy (GD) metrics are used for the classification purpose which is proceeded by examining the headers of the packets to classify the network into a unique network flow. However, this detection technique requires more involvement of ISP's so it cannot be used more often.

B. Johnson Singh et al [2] gave a a detection scheme that was based upon computation of number of HTTP GET request, variance and entropy of each connection. Each HTTP GET request were counted after an interval of 20 seconds. The scheme gave approximate calculation for high and low rate of DDoS attacks.

C. Nam and Djuraev [3] propsed a detection technique that used multiple levels to protect a web server by focussing mainly on the workload of server. The first layer accepted or rejected a connection depending upon the whitelist of IP address. If the accepted connection behaved maliciously it was dropped off. However, this detection technique has a flaw that if a legitimate user downloads or streamed a file of very big size then it would drop off the user.

D. Shiaeles and Papadaki [4] introduced a multilayer IP spoofing method called fuzzy hybrid spoofing detection (FHSD) to detect application layer DDoS attacks. It used hop counts, MAC address, operating system (OS), geographical address of IP address. Moreover, it used operative passive fingerprinting and HTTP user agents for cross checking. This results in the detection of botnets also. The only disadvantage of this scheme was that the database required daily updating for effective results.

E. Muhammad Aamir et al. [5] used a semi-supervised machine learning approach to classify DDoS attacks. The features used were processing delay, CPU utilization and traffic rate. Based on this the unlabeled data is clustered using clustering algorithms with a separate cluster class called 'Suspicious'. Then the supervised learning of SVM, KNN are applied on the data. The accuracy of this approach was about 82% which can be improved by using more accurate models of machine learning.

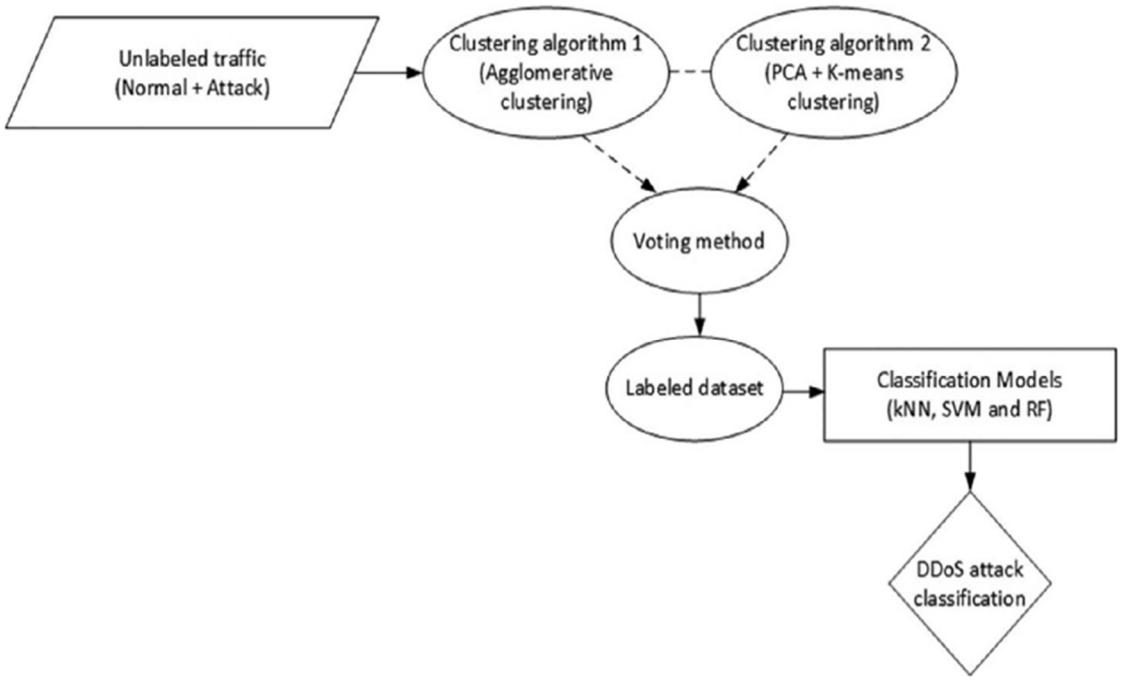


Fig 5 Flow chart of semi-supervised machine learning for DDoS attack classification

V. MITIGATION TECHNIQUES

Whenever a malicious user is successful in bringing down a web server by performing a successful DDoS attack, then a mitigation technique is required so as to bring back the server to its original function and limit the amount of damage caused by the attack. Some of the techniques followed by web administrators are:

A. Black Hole Routing

It is a defense technique used by Internet Service Providers (ISP) which involves network admins to create a virtual blackhole route through which all the traffic gets diverted into. This way all the traffic, the legitimate and the malicious traffic is dumped into the virtual black hole by the ISP. The main drawback of this technique is that the web server will be unavailable to legitimate users also hence the main purpose of the attackers gets fulfilled.

B. Web Application Firewall

A web application firewall is a tool that can help in the process of mitigation of application layer attacks. The firewall acts as a proxy server by managing all the incoming and outgoing connections from the web server. The firewall blocks the unwanted traffic based on some set of rules that can be set in the firewall application. One such example of a firewall that is mostly used by many web servers is Cloudflare.

C. Anycast Network Diffusion

Anycast is a network addressing approach by which incoming request by any user can be dispersed into different servers so that the load on any one server gets less and thus the server does not get overloaded by the malicious traffic. The consistency of this technique depends upon the size of the anycast network and on size of the attack launched against any web server. This mitigation technique is also effective against bot-nets.

D. IP Traceback

IP traceback refers to the tracking down of the original source of the packet. Hong-bin Yim et al. [6] proposed an effective packet marking algorithm in which the router records the route and gets implemented in the IP header. It uses a probabilistic marking scheme and XOR operation to reduce the size of the IP header.

E. Active Packet Filtering

Packet filtering refers to categorisation of traffic coming from different IP into malicious and legitimate traffic. This includes usage of any packet filtering software such as Wireshark. Specific rules and protocols could be specified to have more accurate filtering of packets. Congestion control in IP networks is done at each router through queue management. It can be made more efficient using time-window based filtering mechanism, before queue management policy is applied.

F. Intrusion Detection Systems

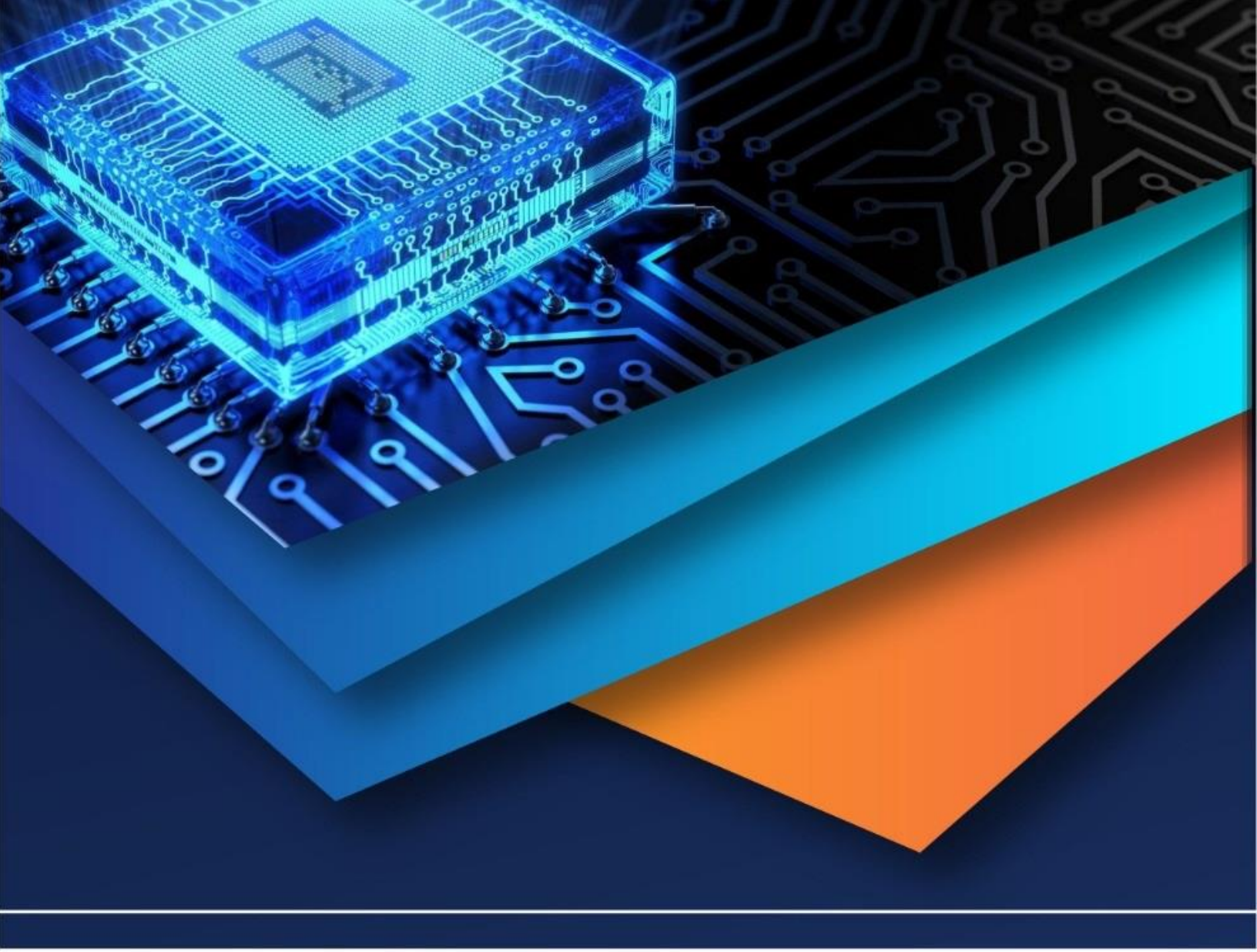
Intrusion Detection Systems such as SNORT keep the signatures of the past DDoS attacks to build a database of pre-defined signatures. With the help of the signature database the SNORT system overviews the proper working of the web server and notifies the admin of the server if any malicious activity is suspected. However, if a very large attack is done then SNORT produces bottleneck to the performance of the system.

VI. CONCLUSION

This paper is to give a detailed description of about the most dangerous and recurring attack that every organisation must have faced once that is Distributed Denial of Service. This paper intends to share more information about DDoS attacks. The paper discusses the possible reasons why a attacker tries to DDoS any web server. This paper also discusses on various detection techniques of DDoS attack and how these attacks could be mitigated. The paper discusses many approaches used by many researchers to make an efficient way to tackle DDoS attacks. The research for detecting DDoS attack makes use of Machine Learning, which suggests that in the future machine learning will provide helpful hand in handling DDoS attacks. At last, this paper helped in understanding DDoS attacks as a whole and how advance technologies like machine learning and artificial intelligence will come handy in making much more efficient algorithms for detection and prevention of DDoS attacks in the upcoming years.

REFERENCES

[1] S. Behal, K. Kumar, and M. Sachdeva, “D-FACE: an anomaly based distributed approach for early detection of DDoS attacks and flash events,” Journal of Network and Computer Applications, vol. 111, pp. 49–63, 2018.
[2] K. Singh, P. Singh, and K. Kumar, “User behavior analytics-based classification of application layer HTTP-GET flood attacks,” Journal of Network and Computer Applications, vol. 112, pp. 97–114, 2018.
[3] S. Y. Nam and S. Djuraev, “Defending HTTP web servers against DDoS attacks through busy period-based attack flow detection,” KSII Transactions on Internet and Information Systems, vol. 8, no. 7, pp. 2512–2531, 2014.
[4] S. N. Shiaeles and M. Papadaki, “FHSD: an improved IP spoof detection method for web DDoS attacks,” Computer Journal, vol. 58, no. 4, pp. 892–903, 2014.
[5] M. Aamir and S. M. A. Zaidi, “Clustering based semi-supervised machine learning for DDoS attack classification,” Journal of King Saud University—Computer and Information Sciences, 2019.
[6] Yim, Hong-bin & Jung, Jae-il. (2010). Probabilistic Route Selection Algorithm for IP Traceback. 122. 94-103. 10.1007/978-3-642-17610-4_11.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY