IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 4, April 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 4, April 2024 ||

| DOI:10.15680/IJIRSET.2024.1304418 |

Mitigating DDOS Attacks in IOT Network Environment

Mr. M. B. Bheema Kumar[1], Ashok Palimiri Pradeep[2], Narpala Nasima[3], Yerikalammagari Omkar[4], Kesamreddy Naveen Kumar Reddy[5], Vanam Naga Jyothi[6]

UG Student, Dept. of E.C.E., GATES Institute of Technology, Gooty, Anantapur, Andhra Pradesh, India[2,3,4,5,6]

Assistant Professor, Dept. of E.C.E., GATES Institute of Technology, Gooty, Anantapur, Andhra Pradesh, India [1]

ABSTRACT: The usage of IOT (Internet of Things) gadgets is said to be innately increasing in people`s daily lives. Such handy devices can particularly benefit the average individual, who does not necessarily have to understand technical knowledge in-depth. The IOT can be found widely in home security and alarm installations, smart fridges, advanced smart televisions, and other essential items. However, these small Internet-connected devices have numerous benefits while still bringing along potential security threats. Malicious actors are often seen attempting to discover new methods to exploit and utilize certain resources, and IOT devices become a perfect candidate for such misuse attributable to the huge volume of active devices involved. Distributed Denial of Service (DDoS) attacks are specifically concerning, involving the exploitation of a massive number of devices, like IOT devices to serve as bots and excessively send fraudulent requests to services, consequently obstructing them.

To identify and detect whether such attacks have occurred in a network, a reliable detection mechanism needs to be properly established based on suitable techniques. The most commonly used technique for this particular purpose is artificial intelligence, implementing Machine Learning (ML) and also Deep Learning (DL) to aid in identifying cyberattacks. ML models incorporate algorithms that require structured data tot learn from, predict outcomes, and detect identifiable patterns.

KEYWORDS: Distributed Denial of Service; TCP SYN flooding; TCP RST attack; Rate detection; HTTP GET flooding; SYN thresholding; port checking.

I. INTRODUCTION

The Internet of Things (IOT) refers to the network of interconnected physical devices that are embedded with sensors, software, and other technologies, enabling them to collect and exchange data. These devices span various domains, including the home automation, healthcare, transportation, and industrial sectors. For instance, smart thermostats, wearable fitness trackers, autonomous vehicles, and industrial sensors are all examples of IoT devices. Recent years have seen a rise in IoT devices, which have expanded to everyday appliances and systems. It is estimated that IoT devices will reach a staggering number of 24.6 billion connected devices by 2025 [1]. With this astonishing number of IoT devices, there is a greater threat of cyberattacks, which can be induced by IoT devices, whether intentionally or by accident. Among the many attacks associated with IoT devices is a type of attack called DDoS attacks. DDoS attacks are growing at a disturbing speed and becoming more sophisticated. IoT devices are an integral part of many DDoS attacks, as they enable and improve the capability of DDoS attacks due to the connectivity of such devices to the Internet and the absence of firewalls and other security components in these devices. Cyberattacks can result in devastating incidents, such as power cuts, military equipment failures, and the leaking of confidential information. It is also possible that these attacks interrupt phone and computer networks, rendering data inaccessible or paralyzing systems. Moreover, IoT devices are more susceptible to being hijacked, as they lack numerous computational resources for adequate security. They can be exploited to conduct large-scale attacks without the knowledge of the device's owner, potentially leading to the creation of botnets.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 4, April 2024 ||

| DOI:10.15680/IJIRSET.2024.1304418 |

II. LITERATURE SURVEY

[1] S. T. Zargar, J. Joshi and D. Tipper, "A Survey Of Defense Mechanisms Against Distributed Denial Of Service (Ddos) Flooding Attacks," In Ieee Communications Surveys & Tutorials, Vol. 15, No. 4, Pp. 2046-2069, Fourth Quarter 2013. Distributed Denial Of Service (Ddos) Flooding Attacks Are One Of The Biggest Concerns For Security Professionals.

[2] S. S. Kolahi, A. A. Alghalbi, A. F. Alotaibi, S. S. Ahmed and D. Lad, "Performance comparison of defense mechanisms against TCP SYN flood DDoS attack," 2014 6th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), St. Petersburg, 2014, pp. 143-147. Distributed Denial of Service (DoS) attacks is one of the major threats and among the hardest security problems in the Internet world. In this paper, we study the impact of a UDP flood attack on TCP throughputs, round trip time, and CPU utilization on the latest version of Windows and Linux platforms, namely, Windows Server 2012 and Linux Ubuntu 13.

[3] B. Nagpal, P. Sharma, N. Chauhan and A. Panesar, "DDoS tools: Classification, analysis and comparison," 2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, 2015, pp. 342-346. Distributed Denial of Service (DDoS) attacks are the major concern for the security experts. DDoS attack presents a serious risk to the internet. In this type of attack a huge number of accommodated targets send a request at the victim's site simultaneously, to exhaust the resources (whether computing or communication resources) within very less time.

[4] Mahadev, V. Kumar and K. Kumar, "Classification of DDoS attack tools and its handling techniques and strategy at application layer," 2016 2nd International Conference on Advances in Computing, Communication, & Automation (ICACCA) (Fall), Bareilly, 2016, pp. 1- 6. Computer networks basically consist of seven layers in all at different levels. The seventh layer i.e. application layer is responsible to ful fill the user's requests. Distributed Denial of Service Attack (DDoS) is a condition in which upper three layers of any computer network generally stop their jobs to ful fill the request of clients.

III. EXISTING SYSTEM

There are many existing techniques used for diabetic retinopathy classification and found many limitaions as well as complexity. Machine learning is a branch of Artificial Intelligence (AI) and computer science which focuses on the use of data and algorithms to imitate the way that humans learn, gradually improving its accuracy. IBM has a rich history with machine learning. One of its own, Arthur Samuel, is credited for coming the term, "Machine learning" with his research around the game of checkers.

IV. PROPOSED SYSTEM

The attack module consists of a packet generator which builds IP headers based on the type of attack used by the attacker. The inputs like the type of attack, source and destination details, speed, spoofing and randomization options are entered in a GUI built using PyQt4 [7].

This attack aims at consuming server CPU memory. In this attack, the attacker floods the target with TCP SYN requests to consume a large part of server resources and thus interrupts the connectivity between the target and genuine clients. When a client wants to establish a TCP connection with a server, a series of messages are exchanged. This process of establishing a connection is called three-way handshaking.

During this time, the server does not close down the connection by sending an RST packet before connection timeout and thus the connection stays open. Before the connection times out, another SYN packet will arrive. This results in a large number of half-open connections. This is the reason SYN flood attacks are also referred to as "half-open" attacks. Eventually, as the server's resources are exhausted, service to legitimate clients will be denied, and the server may even malfunction or crash.

The defence module consists of an IP packet parser to decode each field in an IP header, a DDoS detector program which detects a DDoS attack using various methods that will be explained in this section and finally a mitigation program which employs packet filtering using iptables. Fig. 2 shows the defence module in action. It displays Source IP

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 4, April 2024 ||

| DOI:10.15680/IJIRSET.2024.1304418 |

address, Protocol used by the packet, Size of the packet, Source and Destination Ports if available, Traffic status (Normal or DDoS), Source IP status (Connected or Blocked) and the Rate at which the Source is sending the packets.

BLOCK DIAGRAM

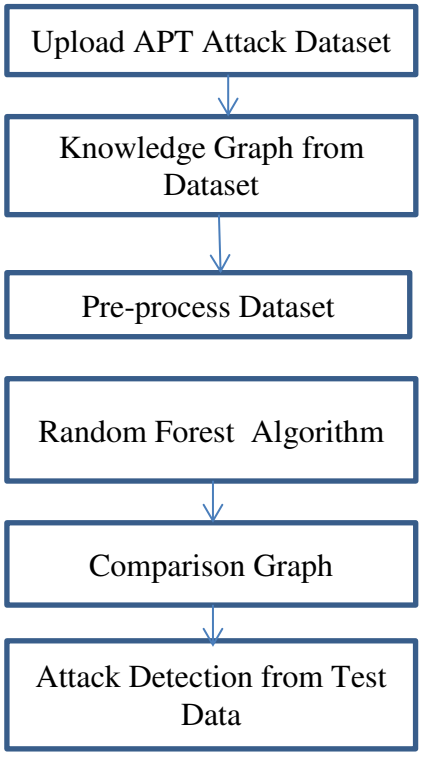

Figure 1: Block Diagram

The defence module gives Trust Score for each IP address. If it is high enough, The IP address is considered to be trusted and it is whitelisted. The process of whitelisting and blacklisting is repeated after every time interval configured in the configuration file. The configuration file has all the information needed to detect any anomalies. The defence module logs all the incidents into a log file and also shows a live log. It also captures all the packets received into a p cap file.

Figure 2: Data set

In above screen we can see all dataset values converted to numeric format and dataset contains more than 70000 records and each record contains 87 features and then we have split dataset into train and test and for training

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 4, April 2024 ||

| DOI:10.15680/IJIRSET.2024.1304418 |

application using 56685 records for training and 14172 for testing. The DDoS (Distributed Denial of Service) attacks generally make use of the characteristic of the three-way handshake process in the course of the TCP (Transmission Control Protocol) connection, and attack the servers through uncountable TCP connections to consume the servers' resources. Therefore the common defense method against DDoS attacks is to buy more servers to increase the service capability to cope with the massive network requests.

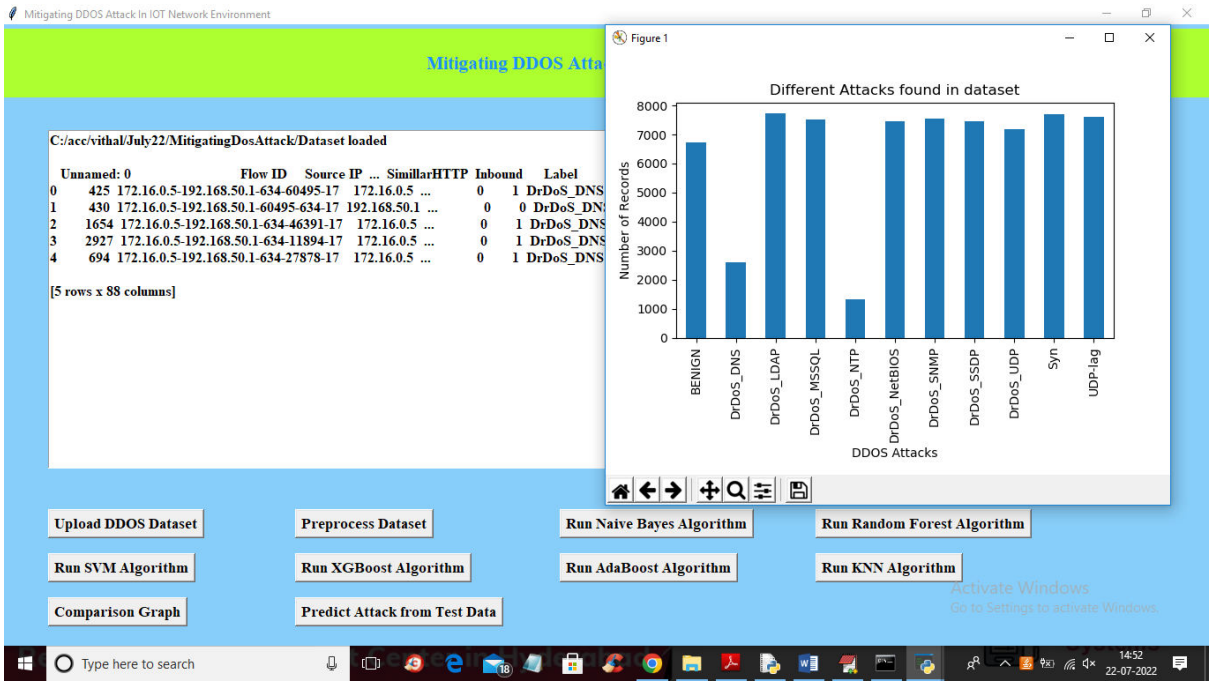

Figure 3: Dataset collection

In above screen dataset loaded and we can see dataset contains both numeric and non-numeric data and in above graph x-axis represents attack names and y-axis represents count of those records.

Whenever a DDoS attack is identified, the solution would be to fix the problem manually by disconnecting the victim from the network. DDoS flooding attacks not only waste a lot of resources (e.g., bandwidth, processing time, etc.) at the target but also on the paths that lead to the target machine; hence, the goal of a DDoS defense mechanism should be to detect them as soon as possible.

A Distributed Denial of Service (DDoS) attack is an attempt to make a target system unavailable for delivering a service by overwhelming it with traffic from multiple sources. Such types of attacks occur when there are multiple systems that have been infected by a malicious user, and flooded the target system with huge amounts of traffic [1]. A crucial problem in the identification of a DDoS attack is the fast detection of malicious hosts trying to drain away the bandwidth of the network and resources of the target system. Log files are generated at a tremendous rate where a server can generate tens of terabytes of log data just in one day based on the traffic it is receiving.

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 4, April 2024 ||

| DOI:10.15680/IJIRSET.2024.1304418 |

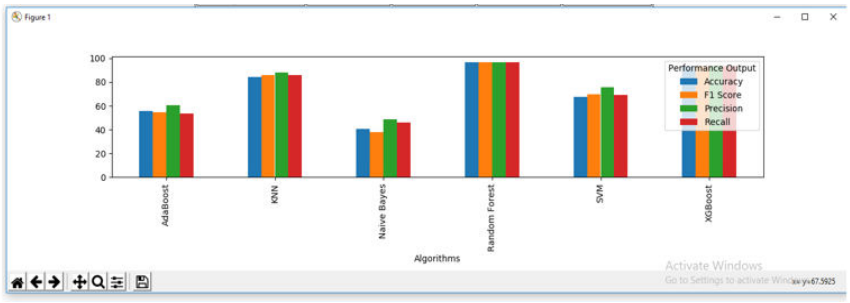

Figure 4: Multi-stage Dia Net

In above graph and comparison table we can see Random Forest got high accuracy and in above graph different colour bar represents different metrics such as accuracy, precision, recall and FSCORE.

The datasets generated by a server are huge and processing them can take a large amount of time. Thus we need a fast parallel processing system with the provision of reliable storage for faster detection and prediction of DDoS attacks. The Hadoop Distributed File System (HDFS) [2] is considered as a primary storage system used by Hadoop applications. It is a distributed file system which is used to provide very fast access to the data among nodes across Hadoop clusters. The HDFS breaks up the input data and sends the chunks of the data to various machines which are the parts of the Hadoop cluster.

V. EXPERIMENTAL RESULT

In this project we are detecting presents of diabetes and its stages and to implement this project we are using Convolution Neural Network (CNN) Algorithm). To train CNN we are using IDRID (Indian diabetes Retinopathy Diabetes) images which consists of 5 different types of diabetes disease images. Those 5 types of diseases are Mild, Moderate, No (not presence of diabetes), Proliferative_DR and Severe

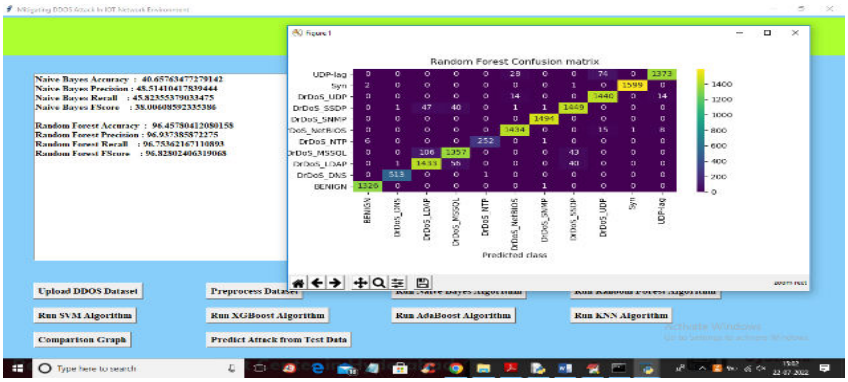

Figure 5: Random Forest Algorithm

VI. ADVANTAGES AND APPLICATIONS

To implement this project we have designed following modules
Step 1. Accept inputs from the GUI of the attack tool.
Step 2. Initialize the IP header fields on the click of 'Lock' button.
Step 3. Depending on the type of attack chosen, jump to the respective attack program.
Step 4. Build the attack packet.
Step 5. Send the attack packet.
Step 6. If 'Stop' button is pressed, go to Step 7 or else go to the Step 4 after a delay or no delay depending on the rate chosen.
Step 7. Stop sending the attack packets and display the Summary.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 4, April 2024 ||

| DOI:10.15680/IJIRSET.2024.1304418 |

VII. CONCLUSION AND FUTURE SCOPE

We conclude that there has been an increased usage of IoT devices in recent years, and this here increase will continue because of the importance of IoT devices in serving the modern technology ecosystems that there surround us, you know. The weakness of security features in such devices may result in huge damage; such as the most common DDoS attack!!! This attack utilizes IoT devices with small computational resources to work under control of the attacker, and launch attacks on the remaining resources in the network. In this paper, we studied and compared different frameworks for detecting DDoS attacks in an IoT environment using these ML models. The future trends in the fields of DDoS attacks by IoT devices present significant challenges!!! and opportunities, I mean. As IoT devices become more ubiquitous, the potential attack surface will continue to expand, thus making it more essential than ever to develop effective strategies for mitigating and detecting DDoS attacks!!! Based on our research gap analysis, we found that creating a new open-source IoT-based dataset would be such a valuable contribution to the research field for detecting IoT DDoS attacks using ML models. Moreover, it is recommended that the number of IoT devices included in the setup be increased to come close to a realistic attack scenario? Additionally, exploring machine learning models that have received limited attention in this context, such as AdaBoost, could yield significant insights for future research in this field.

REFERENCES

[1] S. T. Zargar, J. Joshi and D. Tipper, "A Survey of Defence Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks," in IEEE Communications Surveys & Tutorials, vol. 15, no. 4, pp. 2046- 2069, Fourth Quarter 2013.
[2] S. S. Kolahi, A. A. Alghalbi, A. F. Alotaibi, S. Ahmed and D. Lad, "Performance comparison of defence mechanisms against TCP SYN flood DDoS attack," 2014 6th International Congress on Ultra-Modern Telecommunications and Control Systems and Workshops (ICUMT), St. Petersburg, 2014, pp. 143-147.
[3] B. Nagpal, P. Sharma, N. Chauhan and A. Panesar, "DDoS tools: Classification, analysis and comparison," 2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, 2015, pp. 342-346.
[4] Mahadev, V. Kumar and K. Kumar, "Classification of DDoS attack tools and its handling techniques and strategy at application layer," 2016 2nd International Conference on Advances in Computing, Communication, & Automation (ICACCA) (Fall), Bareilly, 2016, pp. 1- 6.
[5] Kali Linux Operating System - Advanced Penetration Testing Linux distribution used for Penetration Testing, Ethical Hacking and network security assessments. [Online]. Available: https://www.kali.org/
[6] Python programming language. [Online] Available: https://www.python.org/
[7] Python bindings for Qt application framework. [Online]. Available: https://riverbankcomputing.com/software/pyqt/ intro
[8] Hping security testing tool. [Online]. Available: http://hping.org/
[9] Ettercap Man-In-The-Middle-Attack tool. [Online]. Available: http://ettercap.github.io/ettercap
[10] Xbox Live and Sony PlayStation attack. [Online].
[12] V. D. Gligor, "A note on denial-of-service in operating systems," IEEE Transactions on Software Engineering, vol. 10, no. 3, pp. 320– 324, 1984.
[13] P. J. Criscuolo, "Distributed denial of service: Trin00, tribe flood network, tribe flood network 2000, and stacheldraht ciac-2319," DTIC Document, Tech. Rep., 2000.
[14] P. Ferguson and D. Senie, "RFC 2827: Network Ingress Filtering: Defeating Denial of Service attacks which employ IP source Address
[15] K. Park and H. Lee, "On the effectiveness of probabilistic packet making for IP traceback under Denial of Service attack", hoc. IEEE WOCOMM Anchorage, AK, USA, pp. 338- 347, Apr. 2WI.
[16] R. R. Talpade, G. Kim and S. Khurana, 'WOW: Traffic-based Network Monitoring Framework for Anomaly Detection". Prw. 4'h EEE Symposium on Computers and Communications, Ted Sea, EgJpt, pp. 442451,June 1999.
[17] W. Lee and S. J. Stolfo, "'Data mining approaches for intrusion detection", 7' USENIX Security Symposium, San Antonio,TX, pp 79- 93, January 1998.
[18] I. B. D. Cabrera et al., "Proactive Detection of Distributed Denial of Service Attacks using MIB Traflic Variables - A Feasibility SNdy",hoc. 7" IFIPi EEE Int. Symp. On Integrated Network Management, Seattle, WA, May 2001.
[19] Y. Huang, J. M Pullen, "Countefmg Denialuf- Sewice anacks Using Congestion Triggered Packet Sampling and Filtering", Proc. IO' ICCCN, Anzona, USA, Oct. 2001.
[20] T.M. Gil and M Poleto, "MULTOPS: a data- structure for bandwimh attack detection", hoc. lo* USENIX Security Symposium Washington, DC, pp.23-38, Aug. 2001.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details