iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** VI **Month of publication:** June 2022

DOI: https://doi.org/10.22214/ijraset.2022.43723

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: 7.538
Volume 10 Issue VI June 2022- Available at www.ijraset.com

Detection of DDoS Attacks using Concepts of Machine Learning

Prof. Amit Narote[1], Vamika Zutshi[2], Aditi Potdar[3], Radhika Vichare[4]
[1]*Professor, Department of IT, Xavier Institute of Engineering, Mumbai, India*
[2, 3, 4]*Student, Department of IT, Xavier Institute of Engineering, Mumbai, India*

Abstract: ***Distributed Denial-of-Service (DDoS) assaults are the terrorizing preliminaries on the Internet that exhaust the organization transmission capacity. Analysts have presented different safeguard components including assault counteraction, traceback, response, identification, and portrayal against DDoS assaults, however the quantity of these assaults builds consistently, and the ideal answers for this issue have escaped us up to this point. An order of identification approaches against DDoS assaults is given the point of giving profound understanding into the DDoS problem. Although the anticipation of Distributed Denial of Service (DDoS) assaults is preposterous, location of such goes after assumes principal part in forestalling their advancement. In the flooding assaults, particularly new modern DDoS, the assailant floods the organization traffic toward the objective PC by sending pseudo-ordinary parcels. Hence, multi-reason IDSs don't offer a decent execution (and precision) in distinguishing such sorts of assaults.***

Keywords: Denial-of-Service (DoS), Distributed Denial-of-Service (DDoS), Machine Learning, attacks, attackers, system, cyber, bots.

I. INTRODUCTION

A denial of service (DoS) attack is a type of digital attack in which a vengeful entertainer attempts to render a PC or other device inaccessible to its intended clients by interrupting with the device's normal operation. DoS attacks regular work by overloading or flooding a specific computer with requests until normal traffic can't be handled, resulting in expansion client disavowal of administration. A distributed denial-of-service (DDoS) attack is an attempt to damage a particular server's, service's, or network's normal traffic by flooding the victim or its surrounding infrastructure with Internet traffic. DDoS assaults are effective because they use several infiltrated computer systems as attack traffic sources. Computers and other networked resources, such as IoT devices, are examples of manipulated machinery.

II. RESEARCH OBJECTIVES

A. Purpose

Conventional manual methods of risk identification suffer from low precision and long lag issues. Threats can be recorded more rapidly and correctly using ML approaches such as Naive Bayesian, KNN, and Random Forest (Priya.S.et.al). In machine learning, features for classification must be chosen by humans or by specific feature strategically placing. Feature selection, on the other hand, is an essential component of DL. Deep Learning models, such as CNN and RNN, are constructed using a series of nonlinear convolutional filters to learn many levels of data recognition from a large volume of labelled samples. As a result, DL can be an effective tool for DDoS detection (Pouyanfar.et.al). The purpose of this thesis is summarized as follows:

1) To identify the detection of various DDoS attacks.
2) To demonstrate the impact of attacks on system
3) To detect the presence of the unknown attack in a network using the proposed model
4) Evaluating results on the basis of parametric values that can achieve recall, precision and accuracy

B. Severity of the Attack

In the past, it is quite observed that the DDoS attacks have been on a constant rise with no further prevention to be taken. The beginning of these attacks initially took place on a small scale with an attack traffic of 200Mbps. Though with such a small amount of data, it was capable to bring down the entire network for more than a week. Another attack took place in 2007 with an attack of 90Mbps that created major damage to government organizations and they remained shut for 3 weeks. A year later, another attack strike over western Asia and Eastern Europe and crippled the internet infrastructure for a month (Stephen Korns). Thus, it is witnessed that these attacks have resulted in significant financial and economic loss to the entire country.

©IJRASET: All Rights are Reserved

With the rapid growth of the internet, majority of the intruders are exponentially increasing their attacks on servers in order to bring down a vast group of victims. While earlier forms of DDoS attacks mostly aimed to bring down a particular group of organizations, the newer and evolved DDoS attacks possess the capability of bringing down multiple organizations all at once. In the year 2013, the entire infrastructure of the web was put to test, when it was attacked with an attack speed of 300Gbps in Spamhaus (Lucian Constantin).

This attack was a major shook down to the country as it resulted in overall congestion of the network in Europe, delaying user's accessibility to the website. In the following year another attack hit a web hosting company with an attack traffic of 400Gbps (Lucian Constantin). In the year 2016, the highest peak of 1Tbps DDoS attack was launched on some high-profile websites such as Twitter and Airbnb (C. Williams).

Hence it was concluded that such a severity of DDoS attack can highly disrupt the normal functioning of any organization and business taking place on a daily basis. The point of concern here was that these attacks weren't stopping and hence their mitigation was the top most priority. However, detecting them was still being a tedious task. Conventionally observed this attack focused on to directly bringing down their targeted victims.

On the other hand, attacks such as Smurf (Sanjeev Kumar.et.al) had a high rate of attack traffic to victims and resulted into huge traffic congestion taking place on websites leading to denial-of-service. In contrast to this working principle, DDoS would directly send low intensity traffic, resulting in congestion between shared links of victim and third-party devices such as bots (Ahren Studer.et.al).

These low intensity attacks are generally more effective than the high intensity ones as they properly coordinate with the attackers to merge links of individual victims and further create an aggregation point. This generated aggregated traffic has a legitimate IP address and hence can be accessed from any corner of the world, making it indistinguishable from the actual traffic. Additionally, these attackers coordinate with persistent routes that are not stable and hence affect the load balancing mechanisms in sending attack traffic. As a result, these low intensity attacks are more difficult to maintain the security of the internet.

While there are multiple methods to detect the DDoS attack, none of these techniques could balance the systems scalability with the intensity of these attacks. Also, the systems performance was always compromised on in order to match the experimented techniques with attacks. Hence, the ability to recognize such attacks is an essential step towards addressing the problems of attack detection. On the other hand, without the DDoS detection, its anti DDoS measures would be almost impossible to handle. Hence it becomes all the more important to bride this gap and adapt to proper detection approaches.

C. Distributed Denial of Service

A DDoS attack works on the principle of utilizing multiple vehicles to generate high intensity-based attack traffic with the intention to damage the networks integrity. The vehicles used in this attack are not aware that they are being used by the attacker for damage purpose. For this reason, the computer devices used in such attacks are often referred to as "zombies". Therefore, blocking these vehicles could lead to a worst-case scenario of a data loss. On the other hand, these vehicles are difficult to recognize as they take the shape and characteristics of a zombie. This thesis aims to focus on the detection and evaluation of DDoS attacks using Machine Learning techniques.

D. Background

In 2013, the entire Internet infrastructure was put to the test when a DDoS attack with a peak speed of 300Gbps was initiated against Spamhaus, a non-profit anti-spam organisation (Lucian Constantin). This particular attack succeeded in bringing down the Spamhaus servers, causing Internet congestion throughout Europe and postponing users' access to major websites (Lucian Constantin). Since then, it has been observed that the evolution of DoS to DDoS has taken place that is considered to be one of the most destructive kinds of attack. However, due to the destructive nature of the attack it becomes difficult to mitigate as it penetrates through different ports on the firewall that is further responsible to damage the reputation of the company by attacking on the company's firewall leading it to cause damage on the ports. Almost every major technology company has been the victim of a DDoS attack at some point in their history. Because of the significant intensity of such attacks, it is a constant source of concern for those in charge of cybersecurity. However, detecting DDoS attacks is a difficult task. Traditionally, DDoS attacks are carried out by sending high-intensity traffic directly to the victim. While numerous methods to address DDoS attacks have been suggested, the common approaches lack effectiveness, scalability, and information exchange capability for early and accurate identification of high and low-intensity data breaches.

E. Motivation

In a recent study so conducted, it was brought to witness that the DDoS attacks contributed to the majority of the attacks so caused over a secured network. The most vital thing in attacks is its differentiation strategy that needs to be implemented to distinguish between legit and malicious attacks. However, the testing and implementation of such strategies are difficult to deploy due to existing factors such as cost and complexity issues. Hence, a lot of research work has been performed in this domain using machine learning algorithms.

F. Problem Statement

In an ideal situation a DDoS detection system would aim to identify the attack in real time and further mitigate the threat as soon as possible to prevent further damages to the networking system. This in turn, focuses on two primary goals: high precision and early detection. Because. As a result, it is critical to identify DDoS attack traffic as soon as possible in order to reduce the impact of the intrusion on the system. Because many current detection alternatives are primarily focused on the precision and early intervention of DDoS attacks, the primary issues that prevent DDoS attack detection solutions from detecting attacks accurately and early are as follows:

1) *Performance:* Previous DDoS detection systems, such as LADS (Vyas.Sekar), D-WARD (Jelena Markovic), and NetBouncer (Roshan.Thomas.et.al), have primarily been designed to detect high-intensity DDoS attacks. These detection systems detect attacks using volumetric techniques, which are ineffective in detecting newer DDoS attacks such as low-intensity attacks. Because a low-intensity attack has a lower volume, it will not generate any alerts on volumetric-based detectors. To address this issue, non-volumetric approaches, such as entropy-based detection, have been proposed to detect low-intensity DDoS attack traffic (Haiqin Liu).
2) *Scalability:* As networks have grown in size and traffic has increased, it has become difficult to efficiently process the vast amount of network traffic and detect attack traffic that is located close to its respective sources. The ability of a scalable detection system to process traffic seamlessly without ingesting too much computing power or incurring excessive communication overhead is the greatest difficulty.
3) *Information Sharing:* Present interactive approaches for detecting DDoS attack traffic are constrained by information shared among neighbouring nodes or nodes within the same Local Area Network (LAN) (Jer ome Franc¸ois). This not only limits the amount of information that can be gathered for accurate traffic classification, but it also makes early detection difficult because attack traffic can only be identified within each LAN or at nodes close to the victim.

We summarize the problems of DDoS attacks in the following problem statement: The main issue with existing DDoS attack detection strategies is their incapability to efficiently and consistently identify both high and low-intensity DDoS attacks in complex systems.

Due to limitations in their performance, scalability, and information sharing capabilities, conventional means such as spatially dependent traffic classification, centralized computation, and LAN-based correlation no longer effectively support early and precise DDoS attack detection in large-scale networks. As a result, it is critical to develop new methods for accurately and timely detecting both high and low-intensity DDoS attacks.

III.LITERATURE REVIEW

A. Conceptual Framework

Majority if the attacks that are carried out on the internet are witnessed to be done by DoS and DDoS attacks. Hence, using the concepts of machine learning the attacks can be put to ease and can be detected accurately. The most common techniques used by machine learning to detect the same are categorized as signature based and anomaly-based attacks. According to (Dayanandam.et.al) the first kind of attack are used to detect the intrusions caused by signatures whereas on the other hand, a data flow pattern is created and identified using anomaly-based detection technique. The figure also utilizes machine learning approaches to make the system free from attack. The conceptual framework of the study provides the information regarding the necessary point that has to be carried out. The discussion on the malicious downturns, website vulnerability and also server issues are involved. On the other hand, understanding the perspective of theory application as well as the machine learning approach needs to be implemented to get the favourable condition.

B. Cyber-Attacks in a System

A cyber-attack is generally followed by gaining unauthorized access to a computer system with the pure intention to steal private information of the users. It results in a severe damage to the entire system being shut down completely. It might also result in manipulating stored data and deleting all of it on one click. However, these attacks can be initiated from anywhere in the world and by any professional hacker. These hackers follow a specific pattern to unleash such attacks. Generally, cybercriminals are the ones who perform such activities by enhancing their skills in operating such attacks on computers. Such attackers might also be members of a group that perform such attacks on a global scale. These hackers have been accused of even targeting government official sites and non-profit organizations. The most commonly used cyber-attacks are performed for the following reasons:

1) *Financial Gain:* Most of the attacks in recent trends are carried out to gain financial traits. These attacks are launched with the intention of stealing sensitive data from personalized computers. Attackers are able to gain such information by impersonating themselves as legit users and are hence able to gain access to private data. Other financial motive of such attackers is to lock the servers of shareholders and restricting them to perform any regular activity on their systems. Such attackers are also paid in large amounts to perform these activities.
2) *Disruption and Revenge:* These attacks are also caused by attackers with the intention to trigger uncertainty in the normal functioning of a computer system. It is purely performed with the intention to cause harm to the user. Such attacks also include to embarrass corporate entities publicly. At times these hackers also target non-profit organizations.
3) *Cyber Warfare:* Such attacks take place on government levels with cyber attackers planning their cyber-attacks against the nation as a whole. Such attacks are carried out to gain political gains.

The discussion-based on cyber-attack in a system provides the unacceptable situation where the unauthorized activity on the computer system takes place. Damage on the computer is also involved with the help of cyber-attacks. The data related information is also important to be noted whereas the manipulation of the result creates the error (Tran.et.al). The hacking scenario on other systems can be seen as well. Figure 2.3 is indicating the steps that are followed by the attacker to establish a DDoS attack. The unwanted situation based on developmental aspects can't be seen in the case of technological activities and the advanced method is required to be implemented so that the mitigation of the security concern can be achieved (Doynikova). Different types of cyber-attack are also involved with it. Malfunction, Phishing, SQL injection and man the middle attack are types of cyber-attack.

C. DoS Attacks

A Denial-of-Service attack is an attack that targets the victim website with the intent of compromising its availability. It is capable of doing this by sending huge number of unused packets to a particular destination and further preventing its access from legitimate users when in need. Its primary objective is to shut down the network services by exhausting computer resources by using its bandwidth limit.

Examples of a DDoS attack:

- Ping flood.
- SYN flood.
- ICMP flood.

D. Distributed Denial of Service

The most common and widely used implementation of a DoS attack is a DDoS attack. This type of attack happens to be distributed as it coordinates its attack with the availability of a given targeted system that uses the computing power of various machines known as “zombies”. These zombies are responsible to target a victim unknowingly. The implementation of this attack is executed in various stages; wherein the attacker first uses some hosts and further performs a scanning procedure from remote machines. Next, the malicious user installs attacking tools on the host side.

However, the concept of DoS and DDoS attacks are not related with stealing data, modifying or destroying it, but rather it aims to prevent authenticated users from using a particular service. It is nearly impossible to catch a DDoS attacker as they generally make use of spoofed IP address and it becomes all the more difficult to recognize in a distributed environment.

However, if an intruder gets unauthorized access into the system, then it may portray itself as an actively participating node in the system. Through message requests, it makes use of large bandwidth available and further launches its malicious code in the networking system. This results in a massive generation of traffic.

As a secured framework from a DDoS attack, a defense system can be categorized into three steps.

- Attack Prevention
- Attack Detection
- Attack Identification

Distributed Denial of Service (DDoS) is a type of Denial of Service (DoS) attack that seeks to reject network infrastructure by crashing or consuming the resources of the targeted servers, causing these servers to no longer be able to deliver help to legitimate users. In a DoS attack, the intruder launches attacks from a single source; in a DDoS attack, the attacker launches attacks from a wide range of diverse sources. These distributed sources are frequently broadly distributed and can number in the hundreds of thousands (Moheeb Abu Rajab). Typically, these sources come from the attacker's computers or from damaged Internet devices known as bots (Bill McCarty). As a result, DDoS attacks are more powerful (e.g., 600 Gbps) and more complicated to counter than DoS attacks.

E. DDoS Attack Classifications

A DDoS attack can be classified according to its bandwidth classification and resource depletion as shown in the figure below. Bandwidth depletion is designed in order to flood the victim's network with unwanted traffic and discard the legitimate traffic. This attack ties up the resources with that of the victim's system making it unable to process legit users for service. On the other hand, flooding attacks that comes under resource depletion is the most common form of attack used in a network widely.

1) How to Launch an Attack?

Since then, attackers have devised numerous strategies for launching a successful DDoS attack. When an attack breaks security defenses and causes significant disruption, or when it effectively brings down an entire organization's network for several hours, it is found efficient. A significant number of attack hosts (i.e. bots) launching a synchronized DoS attack against a single computer or a large organization connection would be required for this type of attack. As a result, a DDoS attack can be broadly classified into two categories of launching methods, namely direct and indirect flooding.

a) *Direct Flooding:* A direct flooding attack (DFA), as depicted in Figure 2.7.1(a), occurs when the attacker instructs the bot to send the attack traffic directly to its target through a flood of malicious or useless traffic. SYN Flooding: SYN flooding exploits the three-way handshake session in the Transmission Control Protocol (TCP) by opening a large number of half-open links, rendering the target unresponsive. This three-way handshake session consists of three communicating parties between the client and server previous to establishing a connection. The client sends a SYN1 message to the server, and the server responds with a SYN-ACK2 message. After the client responds with the ACK3 message, a link is made.

b) *Indirect Flooding:* An Indirect Flooding Attack (IFA), as depicted in Figure 2.4.1(b), signifies the indirect flooding of a target by transmitting attack traffic to third-party devices, which then route the attack traffic to their respective targets. In some cases, these machines will enhance the attack traffic in order to have a greater influence on their targets. As a result, this strategy intends to boost the attack's stealthiest by concealing the source of the outbreak in order to avoid detection.

Some of the examples are as follows:

- *Crossfire Attack:* A Crossfire attack aims to unnecessarily complicate network links indirectly by sending attack traffic to tripwire servers in the network (Min Suk Kang). While it is related to a Coremelt attack in that bot are used to send out attack traffic, the main goal is not to deluge the servers and make them inaccessible to public users, but to act as bots in flooding the connections that are attached to the targeted system. To be successful, attackers would need to carefully coordinate the attack traffic by congesting all network links surrounding the targeted organization's network in an attempt to block all of their Internet access links.
- *Reflection Attack:* Reflection attacks use network reflectors to direct attack traffic to the target. In this case, the reflector is a wireless router that returns any packets sent to it, which can be web servers, DNS servers, or network routers. Aside from launching a reflection attack by transmitting spoofed requests to the many reflectors on the Internet, which then forwards responses to their destination, the attackers also use the merged transmission power of both the threat machines and the reflectors to orchestrate a powerful flooding attack on the target.

2) What are Attack Intensities:

a) High-Intensity DDoS Attacks: In a traditional DDoS attack, the attacker consumes all network and server resources with high-intensity traffic (Changwang Zhang). High-intensity attacks, such as Smurf (Sanjeev Kumar), would send packets at a high rate, causing a sudden increase in traffic flow and volume. The recent rise can easily activate network sensing devices in the network, allowing mitigation pathways to halt the attack and inhibit further network destruction.

b) Low-Intensity DDoS Attacks: A low-intensity DDoS attack is a covert attack that saturates its target with a large amount of aggregated low-intensity traffic. Although low-intensity attack traffic like Slowloris (Gkberk Yaltirakli) does not rely on quantity to cause denial-of-service, it will keep as many interaction ports open as possible in order to prevent others from accessing the target servers. By enhancing the aggregated attack volume sufficiently, the attack can effectively cripple the target without triggering the detection techniques. There are also low-intensity attacks that do not actively sought to disrupt service completely, but instead choose to deteriorate service over a relatively long period of time in order to cause financial harm (Michael Lesk).

3) What is the Attack Target?

DDoS attacks mostly target hosts and links on the network as a way of disabling their services.

a) Host: With the purpose of bringing down the host, the intruder targets the implementation, CPU, memory, major contribution, or even the equipment of the host, which could be a network component (e.g., router), an edge device (e.g., switch, edge router), or a computer within the system.

b) Link: The intruder attacks network links by crowding network bandwidth and disrupting the targeted organization's network's communication path. This is considered a more serious attack because by crowding the network link, all hosts linked to it will be brought down at the same time.

4) What is used to launch an attack?

A DDos attack can be launched in following ways: -

a) Army of Bots: Bots are infected machines on the Web that are used by attackers to release attack traffic. Bots are auctioned on the dark web because they are not only cheap but also quick to set up, with many offering DDoS attack services at the lowest cost. The intruder only needs to submit the attack command to a Command & Control (C&C) server, where it is distributed to all attached bots. A botnet is a collection of bots attached to the same C&C server, which can have a substantial percentage of bots and is frequently geographically distributed in the launch of high-impact DDoS network attacks. The recent Mirai botnet has demonstrated the peril of bots on the Internet. Bots have been one of the major contributors to the exponential increase in DDoS attack size since 2013.

Some of the bots used in attacks include: -

- Code Red Worm: A worm that continues to spread and has the capacity to integrate bot armies of hundreds of thousands of hosts, each with a predetermined DDoS attack target.
- Internet Chat Relay (IRC): IRC bots were initially introduced to help operators manage busy chat channels, but they are now used by hackers to launch DDoS attacks on IRC clients and applications (Evan Cooke). The bots are typically controlled by the attacker via a centralised command and control server, and some of the most frequently used bots for DDoS attacks are Agobot, Nesebot, Spybot, Rxbot, and Kaiten (Jose Nazario).

b) Attack Software

Because larger materials are needed to accommodate increasing attack sizes, most attackers use a specific type of attack software when launching a DDoS attack. This category of attack software is a computer-assisted tool that assists attackers in managing the launch of a large-scale attack.

Among the well-known attack software are:

- MStream: Mstream (David Dittrich) enables an attacker to rapidly flood and deplete the target's bandwidth by sending TCP ACK packets with masked source addresses.
- Trinoo: Trinoo or Trin00 (Paul J Criscuolo) uses a UDP flood to deny a specific service without spoofing the IP addresses of its sources. This threat tool also allows the attacker to change the size of traffic packets and set the length of time of an attack.

F. Factors influencing DDoS Attacks

This part of the chapter has considered various factors that influence DDoS in a system. In this scenario, a huge amount of collected information creates an influential approach towards the attacker where the application of DDoS can be done to get the data. On the other hand, whenever the number of parties or participants is involved within a website also indicate the factor that can influence the DDoS process for the hacking purpose. The online services are part of the DDoS where the inclusion of strategic approaches needs to be taken up to mitigate the problem (Alluraiah). However, the political influence also plays an important factor where the attack through the help of DDoS can occur rapidly.

It is extremely essential to maintain the competitive nature of business in the market but the occurrence of DDoS attacks will affect it and lead to a downgrading situation. The fall of the value system in the market also involved decreasing the completion level. The vulnerability of the systems allows the attacker to go for the DDoS procedure where the main focus is to get the information regarding the content of the product (Zekri). The presence of the competitors in the case of business perspective also provides the negative impact where the application of DDoS can happen to create a bad impression in the market interest.

While creating the account details on a website the effective way of providing the security basis approach is to put the strong password as well as the personal details. On the other hand, a simple way to sort out the accounting process indicates an essential factor was to face the DDoS attack can occur easily. The presence of the server problem, as well as the hosting issues, is also an important factor in the abscess of DDoS attacks. In this situation, the establishment of a DDoS attack through an untrusted website can create an unacceptable situation. Providing the information in the risky websites exposes all of the important information of the people. However, the process of getting out from the server problem and heavy trafficking also indicates the time consuming where the assurance level is not at the desired range (Kamboj). In this scenario, the better perspective is to the testing process of the advanced level of the software technologies so that a better result can be achieved through it.

The inclusion of huge numbers of people in servers provides a negative impact on the network under which the server operates. The network becomes vulnerable, and the attackers can gain easy access to the sensitive data. In this scenario, the bot networking system also provides the service problem and hacking process to collect all sorts of information. However, the intermediated factor of the work function increases the chances of getting hacked by the attacker. So, the analysis process of the networking system can be done to detect the DDoS attack. The organizations as well as the industrial sectors contain lots of data regarding their work requirement as well as to get the developmental aspect. In this situation, while transferring the data-related information to the second party can face a server problem in a certain moment where the DDoS attack blocks the transfer process and initiates the hacking procedure concerning both of the parties. The requirement of penetration testing can also be done to get the step-by-step information regarding the creation of vulnerabilities during the transferring process of the important information (Bawany). Another benefit is the application perspective of using penetration testing the security basis approach as well. The in-line analysis of all the packets of the information can also be done to detect the DDoS attack. In this scenario, the automation process tracking the hacking perspective as well as the quick mark process is involved with it. Fast detection of the vulnerabilities and also the network traffic issue can be detected easily with the help of an in line examining process. The networking connectivity is also important to be used where the lower level of connection can create a negative impact in case of detection (Bensalah). However, the application of out-of-band detection is required to be implemented to get valuable results to mitigate the networking problem.

G. Available Frameworks for DDoS Attacks

DDoS detection is the process of identification of Distributed Denial-of-service attacks that are initiated from the normal networks. Limitation of access is the primary target of the detection of DDoS attacks. Various methods of DDoS attacks are used by the attackers to complete a successful operation. Unwanted traffic or service requests are sent to the target networks for the completion of an attack. Different kinds of DDoS attacks are used. It is a difficult job to stop the attacks. Blocking a single IP is not a solution for the detection of the attack. Understanding the instance that an attack is happening is crucial. It can be done by gathering sufficient data from the networks. Again, the analysis of the performance is needed. Detection of the traffic is the next step of detection of the DDoS attack (Heiding). Manual process or automation can be imposed to complete the process of malware detection. Detection is an important process in the removal of the process. The success of the detection and removal is dependent upon two factors. The first one is the detection speed and the second one is the accuracy. The two fundamental processes of detection are in-line detection and out-of-band detection. Either of the approaches is used to detect the attacks. In-line detection is a process where the examination of all packers is done. On the other hand, out-of-band detection is done by the traffic flow of a network. Both processes can be implemented in cloud networking or on the premises. Load balancers, firewalls are the acceptable detection of the smaller attacks of DDoS. It is a costly process and its life cycle is small.

Relevancy of the in-line application is still there because ASIC needs a depth investigation (Khalaf.et.al). The network processor is also the reason for the implementation of in-line detection. On the other hand, out-of-band detection receives various data like net flow, j-flow or IPFIX-authorized routers and switches. Elimination of DDoS is completed by the manual method or by routing.

H. Rising trend of machine learning approaches for justifying DDoS detection

DDoS attacks are a threat to the cyber world. The approach of machine learning in the detection of DDoS attacks is trending globally. Machine language is based on two approaches such as supervised and unsupervised. The supervised approach of machine language is dependent upon the labelled network traffic (Alluraiah). On the other hand, an unsupervised approach identifies the attack by the analysis of the incoming traffic of the network. Both types of ML are challenged by the mass traffic of a network. Again, accuracy is a critical part of the detection of DDoS by implementing the ML. Irrelevant traffic can be detected by the unsupervised process of machine learning.

Smart detection of the DDoS attack is used by the modern computer system globally. The collection of the traffic of the network is done automatically. The collection of the samples and the classification is done automatically by the machine learning approach. Signature dataset (SDS) and machine learning algorithm (MLA) are the two key processes of the detection of DDoS. In the process initially, the detection of the DDoS signatures is done. After that, the information is labelled and stored (Alshamrani). Identification of the appropriate MLA is done by this implementation of the sorting. Next, the SDS is created. Different selection techniques are chosen by the selection process. Industrial standard traffic is used as a sample dataset to detect DDoS traffic. On the other hand, the unlabelled traffic is classified into the receiving end buffer. At the point when the data is exceeding the labelled traffic, the detection of DDoS is possible by machine language (Alieyan). When the sample level is lower the detection of the attacks are detected. Performing deep networking is another factor of ML. Infeasibility of the data systems occurs in the application layer.

I. Machine Learning Classification

Machine learning (ML) is an approach in which machines learns and acquires new knowledge based on prior knowledge, thereby improving their overall performance (Tom M Mitchell). As a result, machine learning approaches were developed to counter highly sophisticated attacks that conventional statistical approaches, such as the solitary threshold or moving threshold, have been unable to handle. Because cyberattack sophistication in traffic classification is constantly evolving, ML techniques were first used in 1994 for traffic analysis in the detection of traffic discrepancies (Jeremy Frank). As a result, these ML classifiers learned traffic patterns from both normal and attack traffic via training, but without the need to set and determine the best characteristics or threshold values for identification.

1) Types of Classifiers

There are dozens of machine learning techniques available for characterization; however, different classification problems necessitate the use of various types of classifiers in order to produce quality classification results (Manuel Fernandez-Delgado). According to a frequently referenced survey paper (Manuel Fernandez-Delgado), there are 17 classifier families in machine learning. Neural Networks: Artificial Neural Networks (ANNs) are broadly used in threat detection methods because they use highly interconnected network topologies for classification. This is due to ANNs' superior reliability and high availability in identifying both predictable and unpredictable attack patterns (Jin Li.et.al). ANN is a viable candidate for DDoS detection due to its ability to provide satisfactory results in distinguishing attack from normal traffic (Yuesheng Gu). The Multilayer Perceptron (MLP) (K Giotis) and Recurrent Neural Network (RNN) (Mark JL Orr) are two common examples of ANN classifiers. These ML-based strategies are intended to counter advanced and evolving adversaries due to their ability to deal with large amounts of complex emerging data (Anthony D Joseph). Unlike traditional detection systems, which use fixed threshold values to differentiate attack traffic from normal traffic, ML approaches use classification models built from learned network behavior to distinguish attack traffic from normal traffic.

2) Machine Learning based Detection

(Gu et al) proposed using a multi-ANN classifier with an enhanced genetic algorithm (GA) for systemic optimizing the process parameters and principal component analysis (PCA) to enhance extraction of features for DDoS attack detection. This approach detects both known and unknown DDoS attacks that have similar patterns to the training set by using old and up-to-date datasets (patterns) in the training phase.

(Saied et al.), on the other hand, used ANN to distinguish between known and unknown TCP, UDP, and ICMP threats. The authors evaluated detection performance when training with both old and new datasets, finding that improper training of old patterns resulted in poor performance accuracy. This method outperformed Snort, Probabilistic Neural Network (PNN), and Back-Propagation detection systems in terms of accuracy, sensitivity, specificity, and precision (BP).

J. Trends of Cyber Security to prevent DDoS

The recent strategies or trends of cyber security that have been adopted for fighting against and preventing the distributed denial-of-service attacks have been discussed in this section. A basic level of security should be provided to the organizational network infrastructure. Securing a particular network within an organization may involve the use of a combination of different prevention and treatment systems. Such systems can be firewalls, anti-spam, VPNs, content filtering and balancing load (Kamboj). These applications should be more or less sufficient for identifying any level of inconsistencies present in the data collected or requests served. Some of the basic network security protocols that can be adopted by any organization are the practice to use complex passwords which should be changed occasionally, allowing minimal outside network traffic, the use of secure firewalls and the deployment of anti-phishing applications (Somani). These basic measures can sometimes serve a great purpose. One of the most popular countermeasures that are recently used for the prevention of distributed denial-of-service attacks is the construction of strong network architecture. The security of any organization depends on the basic network architecture used by the company. Delegating work in case of overburdening within a server should be done such that the productivity increases on an overall scale. DDoS-as-a-Service is also a famous application that has been used quite frequently in recent times (Afaqui, N. et.al). The basic objective of this application is to provide flexibility for the environments that are generally associated with third-party resources, cloud-based services and dedicated server hosting. Several monitoring tools have also been used as cyber security to prevent the distributed denial-of-service attacks recently. Early identification can effectively lead to the prevention of data loss and can help the organization bounce back from its vulnerable state.

IV. IMPLEMENTATION & DESIGN

High availability of service delivery is badly required in many ML scenarios. It is a pleasure for attackers to make these systems down. In addition, the rise of ML has significantly benefited attackers to launch DoS attacks since a large number of less secured IoT devices create an ideal place for use of a system as a botnet. This research work provides an IDS system that detects a set of DoS attacks that emanate from adversaries with different kinds of interest. This security work keeps IoT systems safe from certain kinds of DoS attacks directed towards them or the otherwise emanating from them. And it can have a big significance in a move towards realizing ML systems as the vision ahead. The other benefits that this research work can provide to the broader dimensions of the human life can be anticipated by extrapolating what a secure IoT system can bring.

A. Research Philosophy and Approach

The research has followed the positivism theory to gain factual knowledge by observations in an objective way that is considered reliable and trustworthy (Ryan.G). The data that is gathered by observation and experience is genuine as per its definition. This philosophy allows the evaluation of quantitative data in order to identify the issues faced. The issue that has been considered in this study is the occurrence of DDoS attacks over the systems of the target network (Marsonet). However, the philosophy has been beneficial for developing the measure that will prevent the attack and maintain the security of the machines from the attackers.

1) The deductive approach has been followed in the research that has been beneficial to determine the concept from the previous literature or journals. The articles have been evaluated for designing the strategy of the research. However, the possibility to calculate the perceptions quantitatively is possible using the deductive approach (Pearse). The figure below shows the deduction of the concepts that occur from the particular towards the general consideration of a methodological design. The findings of the research about developing a scalable framework for the detection and removal of DDoS attacks can be generalized up to a certain extent. The explanation of the relation between the hypothesis and variables is allowed by the deductive approach in the research.
2) Descriptive research has been considered for the competition of the research. The descriptive design is beneficial to observe the cases of DDoS attacks mentioned in different articles that have been considered for the collection of data. The close observation has provided a detailed understanding of the issues that are faced due to the occurrence of the attack in a systematic way (Atmowardoyo). The design has been effective to answer the questions related to what, where, when, and how related to the detection and removal of DDoS attacks. Therefore, the evaluation of the data is effective by the incorporation of a descriptive research design.

3) Grounded theory has been beneficial to develop the theories from the collected data. The data that is grounded in the secondary data is accessed for obtaining detailed knowledge of the actual situation faced by the DDoS attack. The articles that have been utilized for the data collection method are compared to identify the information grounded in the data (Vollstedt). The utilization of the grounded theory allows the determination of the actual happenings due to the occurrence of DDoS attacks. The real scenario can be understood by the use of grounded theory. The theory is also effective to acknowledge the contradictions in the data collected.

B. Data Collection and Evaluation

The data for the research has been collected from secondary sources and the journals by various authors on the same topic have been considered. The articles with the report on DDoS attacks have also been considered. The secondary data collection method has been effective to maintain ease of access to the data required for the completion of the research (Martins). However, the method is again cost-efficient and also time-saving. The same data can be utilized for the generation of new insights. A large number can be collected from a wide range of sources that have been evaluated to draw the result of the research.

Secondary data that have been collected from different sources is evaluated by a qualitative technique of data analysis. The process by which data evaluation has been done includes identification, evaluation, and finally, interpretation of information gathered. The qualitative data evaluation method is beneficial for understanding the attitude and the techniques used for making the DDoS attack by the attackers (Akinyode). The process is effective to save money and yet reach the desired outcome of the research. The technique is efficient to generate insights specific to DDoS attacks and determine the methods to detect and remove the same from the systems on a specific network.

C. Ethics

Research ethics refers to the practice of codification of morals that is followed in projects. First and foremost, the research has been kept unbiased and the practice of discrimination is not practiced. The secondary data that have been collected for the research have been selected randomly (Dooly). However, the individuals associated with the research have been respected equally. The data that have been used for the research have been kept confidential so that illegal access is not permitted. However, the conflicts in the interest have been attended to maintain the progress of the research work. The research has also been conducted by the maintenance of anonymity of the sources of data.

D. Instrumentation

The methods for the detection of the DDoS attack have been stated clearly. The detection of the attack can also be identified by the installation of various anti-DDoS software. The use of blockchain technology is beneficial for the detection and mitigation of the attack. CRPS approach is one of the best approaches that are used for the detection and mitigation of DDoS attacks within a network. However, Solar Winds SEM Tool is one of the efficient tools that can be used for the prevention of the attack in the network. The software maintains events and logs for conduction of investigation after the occurrence of the attack and provides mitigation of the effects. However, the software at the early stages prevents the attack but if not successful provides efficient measures for resolving the after-effects.

The incorporation of blockchain technology is efficient for the detection of the attack. Blockchain technology allows storage of the encrypted copy of the machine that executes on a different algorithm. This technology is very efficient for the systems that have become inefficient and finally shut down due to the occurrence of DDoS attacks. The technology is beneficial for the maintenance of a centralized cloud flare that provides extra bandwidth as rent to the organizations. The bandwidth can be used by the organization members across the globe and at any point in time. DDoS attacks are often initiated by botnets utilizing infected IoT devices. The incorporation of blockchain technology makes the process of hacking difficult for the attacker. The prime technologies that are used in blockchain technology involve digital signatures, contributed networks, and cryptology or encryption techniques. The method of preventing the attack by the use of these technologies has been found efficient for the detection and removal of DDoS attacks in the network of any organization. Indus face

AppTrana is one such software that provides detection of DDoS attacks by having vulnerability checks on the machines. Therefore, the incorporation of the software and content filtering is efficient to mitigate the issues related to DDoS attacks. The software allows the identification of the inconsistent traffic that might be the result of a DDoS attack. The implementation of SVM in the machines allows the detection of DDoS attacks efficiently. SVM refers to the learning method that is based on the theory of statistical learning. The method that is used in the method uses an algorithm of supervised learning.

Therefore, the implementation of accurate measurements for the detection of DDoS attacks in companies will protect the data from unauthorized access by perpetrators. Successful establishment of the attacks will lead to the theft of confidential data of the company and use them to cause financial damage. Figure 3.4 represents the framework that is effective for the detection of DDoS attacks in real-time scenarios preventing the loss of confidential data. However, protection against DDoS attacks also protects the misuse of data or deletion of sensitive data of the company. The maintenance of security measures in companies is very essential to protect the databases from the perpetrator's activities. The software mentioned here plays an important role in the detection of DDoS attacks and protects the systems from the perpetrators and the unethical aim to store data for illegal practices.

E. Methodological techniques for DDoS attack detection and removal

The detection of DDoS attacks is possible by the implementation of various techniques. Identification of the huge GET request traffic that is illegally imposed on the web server is the prime method for the detection of the DDoS attack. The most commonly used techniques for the detection of DDoS attacks include pattern matching, evaluation of the deviation of network traffic, clustering, the use of the statistical method, correlations, and lastly associations the life cycle of the defence mechanism for a DDoS attack that is beneficial for the detection and removal of the attack from the systems of the targeted network after the successful detection of DDOS or distributed denial-of-service. However, multi-layered IP spoofing has been found effective for the detection of DDoS attacks as well. The method can detect the attack in the application layer. The method is known as fuzzy hybrid spoofing detection.

Therefore, the method is known as HTTP soldier also allows the detection of the attack. The method can distinguish the actual User from the illegal one by the technique of probability of largedeviation (Lysenko). The method relies on web pages to detect HTTP flood attacks. Moreover, the fundamental method of detection includes in-line detection and also out of band detection. The packets are evaluated in the method of in-line detection. Out of band detection refers to the detection of DDoS attacks by monitoring the network traffic. However, the processes are efficient to detect the attack occurring in the network or on cloud services.

Machine learning techniques have a growing trend in order to detect DDoS attacks. Machine learning algorithms are effective for the detection of attacks. The use of decision tree algorithms for the detection of DDOS attacks is efficient and yielded positive results. Early identification of the attack is the most vital step for the removal of the same for the systems (Manso). The monitoring of the packets received by the networks allows identification of the attack.

Increasing the bandwidth of the network is another best practice that is often incorporated by the cybersecurity team in order to detect and remove DDOS attacks from the network. The identification of the malicious traffic on the network should be followed by blocking the traffic to prevent the occurrence of the attack. The development of redundancy in the infrastructure should be implemented in order to make the organization more resilient to such attacks.

F. Cyber Security Enhancement for Detection and Removal of DDoS attack

Cybersecurity refers to the measures that are implemented in order to provide protection to the systems in a network and prevent the leakage of any sensitive data to the perpetrators. The measures that should be practised for improving cybersecurity with any organization to prevent DDoS attacks include the regular updating of passwords. The change of passwords regularly Strong passwords acts as the first-line protection against the security breaches that occur due to DDoS attacks (Fadlil). The change of passwords should be made compulsory for all employees of the organization in order to reduce the chance of attacks on the systems. However, the systems should be updated regularly as the use of outdated versions of operating systems and other software increases the vulnerability of the system and allows the perpetrators to establish access easily. The updated version of software often is inbuilt with firewall services for the protection of the system against various attacks.

The implementation of VPNs for each and every connection is in order to protect the network from DDoS attacks and reduce vulnerability. The concept of work from home has led to the use of various networks by the employees to access the servers which lead to the occurrence of DDoS attacks. VPN creates secure connections between the server and the other systems used. However, VPN allows the maintenance of security against DDoS attacks in a cost-effective manner (Ghorbani). Therefore, the use of VPNs is beneficial for enhancing cybersecurity for the reduction of cyber-attacks. The unused systems should be removed from the network as the lack of monitoring of the unused systems can also lead to the occurrence of various attacks including DDoS attacks. The incorporation of additional firewalls to every system in the network also allows the reduction of DDoS attacks by detecting them fast and stopping them same. The anti-DDoS software is beneficial for the detection and removal of DDoS attacks from the systems and protects the entire network to face the consequences of the attack. Increase awareness about DDoS attacks among the people so that preventive measures are followed sincerely without failure to prevent the attack.

The rise of awareness among the citizens will lead to timely identification of the attack beneficial for prevention of the same (Haider.et.al). The notifications that pop up on the systems due to the presence of a firewall should be attended to carefully. The trial attempts for the attack can give rise to notifications popping up on the screen due to the detection made by the firewalls present. Identification of DDoS attacks can be possible by closely monitoring the activities and other notifications in the system.

The incorporation of additional firewalls to every system in the network also allows the reduction of DDoS attacks by detecting them fast and stopping them same. The anti-DDoS software is beneficial for the detection and removal of DDoS attacks from the systems and protects the entire network to face the consequences of the attack. Increase awareness about DDoS attacks among the people so that preventive measures are followed sincerely without failure to prevent the attack. The rise of awareness among the citizens will lead to timely identification of the attack beneficial for prevention of the same (Haider.et.al). The notifications that pop up on the systems due to the presence of a firewall should be attended to carefully. The trial attempts for the attack can give rise to notifications popping up on the screen due to the detection made by the firewalls present. Identification of DDoS attacks can be possible by closely monitoring the activities and other notifications in the system.

G. Concepts of Machine Learning

The fundamentals of Machine Learning have never ruled out to implement any project, until recently a lot of variations have been observed in medicinal and cyber security fields. These algorithms never fail to solve a complex problem with its easy development concepts. The primary focus of such algorithms has always been to optimize the work and carry out efficiently with achieved accuracy. Therefore, concepts of the same have also been used to detect the presence of DDoS attacks in a server system. And it has been found that it works better than the normal execution of a signature-based algorithm typically used to carry out its execution. It has been observed that all the algorithms of Machine Learning are heavily trained to detect anomalies in any software. These algorithms are typically classified into four types as:

1) Supervised Learning

All the algorithms under this concept are pre-trained with heavy data and evaluation is further carried out to test the data. Further, in order to check the accuracy of the algorithm, a test data is required. In case of supervised learning, the algorithm already consists of a pre-trained dataset and further makes a prediction in the testing phase. Hence, the data is said to perform under supervision of an already existing algorithm. This method usually comprises the usage of labelled data that is used to predict the label further in the training phase. This type of learning is generally used to dictate the machine to what exactly look for when performing such classification activities. The machine further iterates the process until the output becomes satisfactory and a desired accuracy is achieved. Hence this learning involves working with datasets having prior knowledge so as to what needs to be processed. For this purpose, machine learning algorithms makes use of past data and predicts what the output shall be produced. It comprises of training and testing stage wherein the splitting of this data is done in a pre-decided ratio.

2) Unsupervised Learning

This form of learning is implemented without the involvement and the control of the developer. The basic motive behind unsupervised learning is that the developer is aware of the outputs the machine might generate. Hence when the machine sorts out the data, unsupervised algorithms tend to know the output yield of the vector. Another significant difference between supervised and unsupervised learning is the kind of data these algorithms are fed upon. Supervised learning feeds on labelled data, whereas unsupervised learning feeds on unlabelled data. Hence, unsupervised learning mainly involves its training part on unlabelled data and its further procedure is carried out on it. The concept behind using unsupervised learning is to allow the algorithm to self-discover all the related patterns and equations associated with the algorithm. Although the end result happens to be completely unpredictable and cannot be controlled easily, this procedure is generally accompanied with cluster analysis. Unsupervised learning is capable enough to search and locate the hidden patterns that are available in a data. This feature generally allows and increases the overall efficiency of the working system by auto-categorizing the data. Also, it becomes easy for this process to gather unlabelled sources of data from various repositories.

H. Design and Workflow

All the associated agents with respect to the nodes are used as intermediaries between the node systems. In. these attacks the deployed network is further responsible to calculate the algorithm HMM using the nearest likelihood of a specific observation using the new IP address. When the DDoS attack takes place, majority of the IP addresses are unknown at that point of time. The victim is then further used to access his personal credentials from the network traffic that is collected from the IP addresses.

I. Implementation

The concerned research has been developed by following the deductive research approach, and the deductive approach for this research study helps in finding out the reasoning of the collected data. It helps in the analysis of secondary data from every possible angle. In aspects of conclusion, logical arguments can be provided by following this specific approach. According to information from secondary resources, a Denial-of-Service attack can affect business by minimizing its value as it disrupts communication and it can last more than 24 hours also. It generally prevents the websites from working properly and users get harassed for this reason as business operations and other important activities are getting hampered for uncommon behaviours of websites. High profile online servers such as credit or debit card payment gateways, internet banking services often experience DDoS attacks.

The algorithms for different types of DDoS Cyber threat detection are chosen based on the AI and ML algorithms' computational complexity. When the performance of different algorithms is similar, this criterion is important in selecting a low Computational Complexity algorithm.

Machine Learning Algorithms

1) *Naïve Bayes:* The Naive Bayes Classifier is a successful classification method that aids in the development of fast machine learning models capable of making quick predictions. It's a probabilistic classifier, which means it makes estimates based on an object's probability. It is a family of algorithms that share a similar idea, namely that each pair of features being classified is free of the others.
2) *Logistic Regression:* Logistic regression is a statistical tool that is used for developing machine learning models where the dependent variable is binary in nature. Data and the connection between one dependent variable and one or perhaps more independent variables are described using logistic regression. Nominal, ordinal, or interval variables can be used as independent variables. The term "logistic regression" comes from the concept of the logistic function, which it employs. The sigmoid function is another name for the logistic function. This logistic function has a value between zero and one.
3) *Ada Boost:* Ada Boost is an outfit learning technique (otherwise called "meta-realizing") which was initially made to expand the effectiveness of double classifiers. AdaBoost utilizes an iterative route to cater to realize from the slip-ups of powerless classifiers, and transform them into solid ones. AdaBoost was the first truly fruitful supporting calculation produced with the highest goal of twofold grouping.

V. EXPERIMENTAL ANALYSIS

The working of the entire dataset has been taken from Kaggle repository (Kaggle). There are no recent datasets found in the public domain that are solely for DDoS, though IDS data sets are available. As a result, we extracted DDoS flows from the following public IDS datasets: CSE-CIC-IDS2018-AWS, CICIDS2017, and CIC DoS dataset (2016).

A total of 84 columns were present in the dataset, out of which only 13 features were used and the rest of the data was discarded using feature selection technique. The algorithm of random forest was used to discard the extra features from the dataset and the top 13 best features were implemented. Following are the 13 best features along with their values:

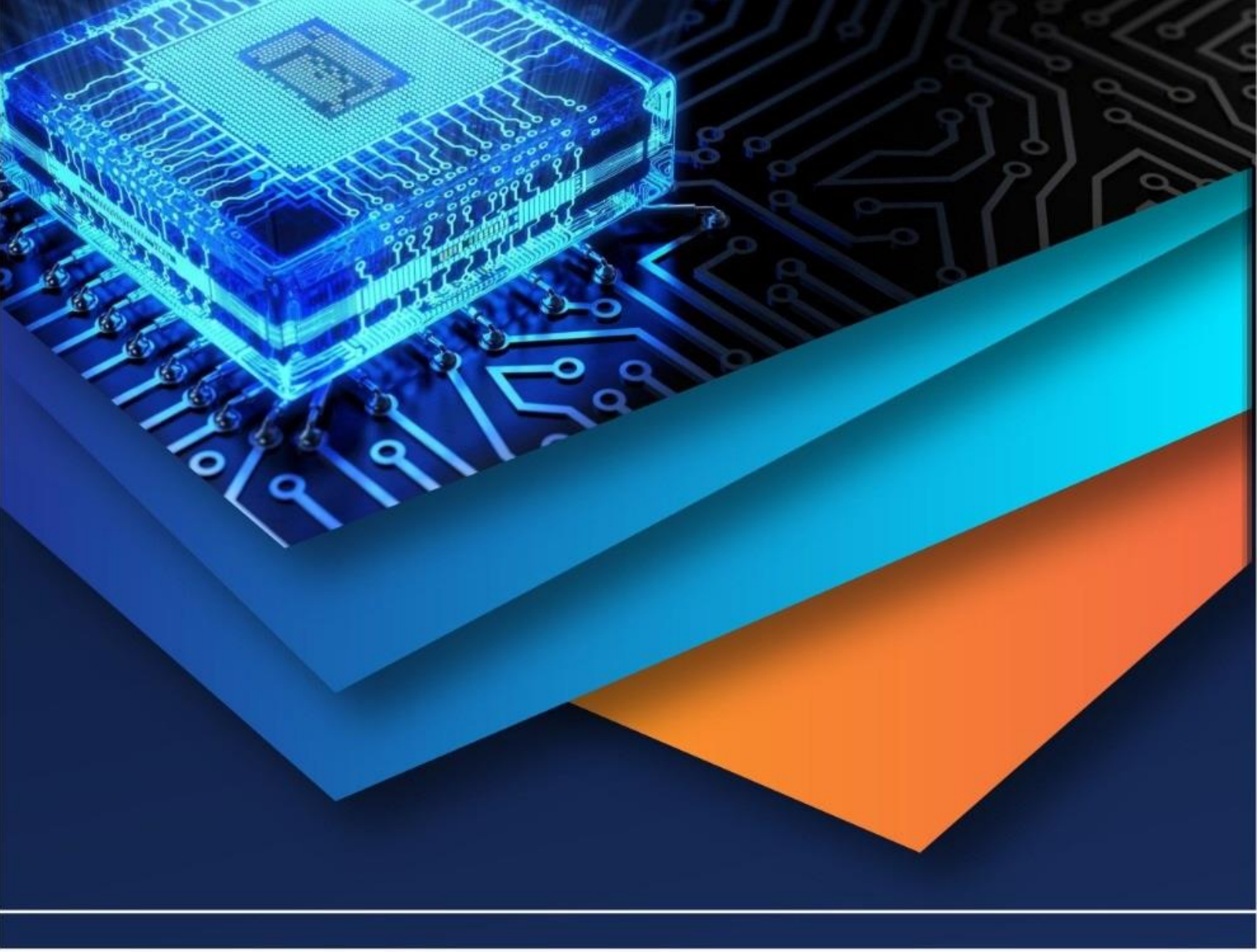
1. feature Init Fwd Win Byts (0.183573)
2. feature Src Port (0.134954)
3. feature Subflow Fwd Byts (0.094038)
4. feature Subflow Bwd Byts (0.081622)
5. feature Fwd URG Flags (0.060384)
6. feature Bwd URG Flags (0.044652)
7. feature Pkt Len Std (0.040275)
8. feature Dst IP (0.03582)
9. feature Src IP (0.031747)
10. feature Fwd Pkt Len Mean (0.022716)
11. feature Bwd Header Len (0.017940)
12. feature Bwd Pkt Len Std (0.016711)
13. feature Dst Port (0.015200)

VI. CONCLUSION

In this thesis, a detailed discussion on detecting DDoS attacks was mentioned. These attacks can be detected using stochastic gradient boosting algorithm. The entire implementation took place on the dataset obtained from the repository. This set of data was developed using a hybrid model and the results were obtained from each model and further compared against each other. It was observed that the hybridized model of SGB outperformed all the machine learning algorithms and produced an accuracy of 100 percent. Also, the hybrid model presented a greater number of features as compared to ML algorithms such as Random Forests and Decision Trees. The proposed work was also aimed to be implemented on an imbalanced set of data that could trigger real time traffic. The proposed hybrid model accomplished a zero-misclassification problem and gave better results in terms of evaluation metrics. On the other hand, other algorithms could not perform much better as they did not yield outputs with desired accuracy. Hence, my work focuses on altering the existing SGB method and develops a model case that could give higher results.

REFERENCES

[1] Doynikova, E. and Kotenko, I., 2018, November. Approach for determination of cyber-attack goals based on the ontology of security metrics. In IOP Conference Series: Materials Science and Engineering (Vol. 450, No. 5, p. 052006). IOP Publishing.
[2] Jaramillo, L.E.S., 2018. Malware detection and mitigation techniques: lessons learned from Mirai DDOS attack. Journal of Information Systems Engineering & Management, 3(3), p.19.
[3] Jonker, M., King, A., Krupp, J., Rossow, C., Sperotto, A. and Dainotti, A., 2017, November. Millions of targets under attack: a macroscopic characterization of the DoS ecosystem. In Proceedings of the 2017 Internet Measurement Conference (pp. 100-113).
[4] Kolias, C., Kambourakis, G., Stavrou, A. and Voas, J., 2017. DDoS in the IoT: Mirai and other botnets. Computer, 50(7), pp.80-84.
[5] Moheeb Abu Rajab, Jay Zafross, Fabian Monrose, and Andreas Terzis. My botnet is Bigger than Yours (Maybe, Better than Yours): why size estimates Remain challenging. In Proceedings of the 1st USENIX Workshop on Hot Topics in Understanding Botnets, Cambridge, USA, 2007.
[6] Bill McCarty. Botnets: Big and Bigger. IEEE Security & Privacy, 99(4):87–90, 2003.
[7] Lee Garber. Denial-of-Service Attacks Rip the Internet. IEEE Computer, 33(4):12–17, 2000.
[8] Min Suk Kang, Soo Bum Lee, and Virgil D Gligor. The Crossfire Attack. In Proceedings of the IEEE Symposium on Security and Privacy (SP), pages 127–141. IEEE, 2013.
[9] Changwang Zhang, Zhiping Cai, Weifeng Chen, Xiapu Luo, and Jianping Yin. Flow Level Detection and Filtering of Low-Rate DDoS. Computer Networks, 56(15):3417–3431, 2012.
[10] Sanjeev Kumar. Smurf-based Distributed Denial of Service (DDoS) Attack Amplification in Internet. In Proceedings of the Second International Conference on Internet Monitoring and Protection (ICIMP), pages 25–25. IEEE, 2007.
[11] Gkberk Yaltirakli. Slowloris. https://github.com/gkbrk/slowloris, 2015
[12] Michael Lesk. The New Front Line: Estonia under Cyberassault. IEEE Security & Privacy, 5(4), 2007.
[13] Evan Cooke, Farnam Jahanian, and Danny McPherson. The Zombie Roundup: Understanding, Detecting, and Disrupting Botnets. SRUTI, 5:6–6, 2005.
[14] Jose Nazario. Ddos Attack Evolution. Network Security, 2008(7):7–10, 2008.
[15] Chao Li, Wei Jiang, and Xin Zou. Botnet: Survey and Case Study. In Proceedings of the Fourth Innovative Computing, Information and Control (ICICIC), pages 1184–1187. IEEE, 2009.
[16] Julian B Grizzard, Vikram Sharma, Chris Nunnery, Brent ByungHoon Kang, and David Dagon. Peer-to-Peer Botnets: Overview and Case Study. HotBots, 7:1–1, 2007.
[17] Jasek Roman, Benda Radek, Vala Radek, and Sarga Libor. Launching Distributed Denial of Service Attacks by Network Protocol Exploitation. In Proceedings of the 2nd International Conference on Applied Informatics and Computing Theory, ser. AICT, volume 11, pages 210– 216, 2011.
[18] David Dittrich, George Weaver, Sven Dietrich, and Neil Long. The Mstream Distributed Denial of Service Attack Tool. http://staff. washington. edu/dittrich/misc/mstream. analysis. txt, 2000.
[19] Paul J Criscuolo. Distributed Denial of Service: Trin00, Tribe Flood Network, Tribe Flood Network 2000, and Stacheldraht ciac-2319. Technical report, DTIC Document, 2000.
[20] Alluraiah, M.K., 2021. A Review on Detection, Defensive and Mitigation of DDoS Attacks with Traceback Methods. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(10), pp.6468-6487.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)