|  |  |  |
| --- | --- | --- |
|  | **MSc Project Report** | |
| Student Name: **Ibrahim Salahudeen** | Matriculation Number: **2113596** | |
| Supervisor: **John Isaac** | Second Marker:  **Mahammad Mekela** | |
| Course: **MSc Cybersecurity** | | |
| Project Title: **Automated detection and prevention of DDOS attacks** | | |
| Start Date: 16/02/2023 | Submission Date: 25/04/2023 | |
| **CONSENT**  I agree  That the University shall be entitled to use any results, materials or other outcomes arising from my project work for the purposes of non-commercial teaching and research, including collaboration.  **DECLARATION**  **I confirm:**   * **That the work contained in this document has been composed solely by myself and that I have not made use of any unauthorised assistance.** * **That the work has not been accepted in any previous application for a degree.** * **All sources of information have been specifically acknowledged and all verbatim extracts are distinguished by quotation marks.** | | |
| Student Signature: **Ibrahim Salahudeen** | | Date Signed: 07/03/2023 |

# TABLE OF CONTENTS

[TABLE OF CONTENTS 2](#_Toc132290909)

[LIST OF FIGURES 3](#_Toc132290910)

[CHAPTER ONE 3](#_Toc132290911)

[BACKGROUND OF THE STUDY 3](#_Toc132290912)

[1.1 Research Motivation 3](#_Toc132290913)

[1.2 Statement of the Problem 4](#_Toc132290914)

[REVIEW OF RELATED LITERATURE 7](#_Toc132290915)

[2.1 Historical background of DDoS attacks 7](#_Toc132290916)

[2.2 Technical background of DDoS attacks 8](#_Toc132290917)

[2.3 Existing Solutions for DDoS Detection and Prevention: 9](#_Toc132290918)

[2.3.1 Network-Based Solutions 9](#_Toc132290919)

[2.3.2 Application-Based Solutions: 10](#_Toc132290920)

[2.3.3 Hybrid Solutions 10](#_Toc132290921)

[2.3.4 Cloud-Based Solutions 10](#_Toc132290922)

[2.3.5 Machine Learning-Based Solutions 11](#_Toc132290923)

[2.3.6 Strengths and Limitations of Existing Solutions 11](#_Toc132290924)

[2.4 Evaluation of Existing Solution 12](#_Toc132290925)

[2.5 Tools to Visualize and Analyze Traffic Incoming to the Server 13](#_Toc132290926)

[2.6 Automated scripting to detect and mitigate DDos attack 14](#_Toc132290927)

[2.7 Tools to Visualize and Analyze Traffic Incoming to the Server 15](#_Toc132290928)

[2.8 Summary 17](#_Toc132290929)

[CHAPTER THREE 18](#_Toc132290930)

[PROJECT SPECIFICATION 18](#_Toc132290931)

[3.1 Aims and objectives of automated detection and prevention of DDOS attack 18](#_Toc132290932)

[3.2 Functional and Non-Functional Requirements 19](#_Toc132290933)

[3.2.1 Functional Requirements 19](#_Toc132290934)

[3.2.2 Non-Functional Requirements 19](#_Toc132290935)

[3.3 Methodology 20](#_Toc132290936)

[3.3.1 Network Traffic Analysis: 20](#_Toc132290937)

[3.3.2 Establishing Baseline Traffic 21](#_Toc132290938)

[3.3.3 Mitigating the Attack 23](#_Toc132290939)

[3.3.4 Post-Incident Analysis: 23](#_Toc132290940)

[3.3.5 Conclusion 23](#_Toc132290941)

[3.4 Brief Explanation of Project’s Plan 24](#_Toc132290942)

[3.4.1 Project Goals 24](#_Toc132290943)

[3.4.2 Project Plan 24](#_Toc132290944)

[3.4.3 Project Deliverables 25](#_Toc132290945)

[3.4.4 Conclusion 25](#_Toc132290946)

[3.5 Legal, ethical, social, professional, and environment review 26](#_Toc132290947)

[3.6 Identification of risks, including security risks and mitigating measures taken 27](#_Toc132290948)

[3.6.1 Identification of Risks: 27](#_Toc132290949)

[3.6.2 Mitigating Measures: 28](#_Toc132290950)

[3.7 Consideration of applicable health and safety, diversity, inclusion, and cultural matters 29](#_Toc132290951)

[3.8 Identification of codes of practice and industry standards related to the work 30](#_Toc132290952)

[CHAPTER FOUR 32](#_Toc132290953)

[DESIGN ALTERNATIVE AND JUSTIFICATION FOR THE CHOSEN DESIGN 32](#_Toc132290954)

[4.1 Design alternative 32](#_Toc132290955)

[4.1.1 Signature-Based Detection 32](#_Toc132290956)

[4.1.2 Anomaly-Based Detection 33](#_Toc132290957)

[4.1.3 Hybrid Detection 33](#_Toc132290958)

[4.1.4 Rate-Based Detection: 34](#_Toc132290959)

[4.1.5 Behavioural Analysis 34](#_Toc132290960)

[4.1.6 Machine learning based 34](#_Toc132290961)

[4.2 Chosen Design and Justification 35](#_Toc132290962)

[4.2.1 Justification for Choosing Machine Learning-Based Detection 35](#_Toc132290963)

[CHAPTER 5 38](#_Toc132290964)

[IMPLEMENTATION AND TESTING 38](#_Toc132290965)

[5.1 Implementation methodology 38](#_Toc132290966)

[5.1.1 DDOS attacks simulation in a virtual environment 39](#_Toc132290967)

[5.1.2 Data Processing 40](#_Toc132290968)

[5.1.3 Machine Learning Models: 41](#_Toc132290969)

[5.2 Testing 47](#_Toc132290970)

[5.2.1 Test Results 48](#_Toc132290971)

[CHAPTER SIX 50](#_Toc132290972)

[EVALUATION OF WORK 50](#_Toc132290973)

[6.1 Results 50](#_Toc132290974)

[6.2 Conclusion 52](#_Toc132290975)

[CHAPTER SEVEN 53](#_Toc132290976)

[CONCLUSION AND FUTURE WORK 53](#_Toc132290977)

[7.1 Current State of Research 53](#_Toc132290978)

[7.2 Future Directions: 54](#_Toc132290979)

[7.3 Conclusion 55](#_Toc132290980)

[REFERENCES 56](#_Toc132290981)

# LIST OF FIGURES

[Fig 3.3.1: Network analysis flow chat 24](#_Toc132290995)

[Fig 4.1.1 Signature-based detection 35](#_Toc132290996)

[Fig 4.1.2 Anomaly-based detection 36](#_Toc132290997)

[Fig 4.1.3 Hybrid-based detection 37](#_Toc132290998)

[Fig 5.1.1 Virtual environment screenshot 42](#_Toc132290999)

[Fig 5.1.2 Network configuration screenshot 43](#_Toc132291000)

[Fig 5.1.3 Data processing 44](#_Toc132291001)

[Fig 5.1.4: Screenshot of R code for importing necessary libraries 46](#_Toc132291002)

[Fig 5.1.5: Screenshot of R code for loading dataset 46](#_Toc132291003)

[Fig 5.1.6: Screenshot of r code for sampled data and variable conversion 46](#_Toc132291004)

[Fig 5.1.7: Screenshot of r code for zero variance and visualization 47](#_Toc132291005)

[Fig 5.1.8: Screenshot of R code for splitting data 47](#_Toc132291006)

[Fig 5.1.9: Screenshot of R code for model performance 48](#_Toc132291007)

[Fig 5.1.10: Screenshot of R code for plotting heat map 49](#_Toc132291008)

[Fig 5.1.11: Screenshot of R code for Roc curve 50](#_Toc132291009)

[Fig 5.1.12: Heat map testing results diagram 52](#_Toc132291010)

[Fig 5.1.13: Model performance metrics plot 52](#_Toc132291011)

[Fig 6.1: ROC curve screenshot 54](#_Toc132291012)

# CHAPTER ONE

# BACKGROUND OF THE STUDY

## Research Motivation

The motivation behind this research is to address the growing threat of Distributed Denial of Service (DDoS) attacks, which have become a significant challenge to network security in recent years. DDoS attacks involve overwhelming a server or network resources with traffic from multiple sources, causing it to become unresponsive and disrupting normal network traffic (Mirkovic et al. 2014). The impact of DDoS attacks can be devastating, causing significant financial losses for organizations, damaging reputation, and compromising critical business operations. According to a report by Netscout (2020), DDoS attacks rose by 22% in the first half of 2020, with the largest attack recorded at 1.17 Tbps. The report also revealed that the average duration of DDoS attacks increased by 5%, while the frequency of shorter-duration attacks increased by 17%. These statistics underscore the need for effective solutions to detect and prevent DDoS attacks.

The motivation for this research is to develop an automated system for detecting and preventing DDoS attacks (Mirkovic et al. 2004). Traditional methods of detecting and preventing DDoS attacks involve manual intervention, which can be time-consuming and ineffective in responding to rapidly evolving threats (Alrawi et al. 2020). Therefore, an automated system is essential for ensuring timely response and mitigating the impact of DDoS attacks. The proposed automated system will be developed based on the following research objectives: the creation of a virtualized network to simulate DDoS attacks (Wang et al. 2020), the development of tools to visualize and analyze incoming network traffic (Bhattacharya et al., 2018), the reproduction of SYN flood attacks (Chaudhary et al. 2018), and the creation of an automated scripting system to detect and mitigate DDoS attacks (Kim et al. 2016). These objectives are designed to enable the development of a comprehensive system that can effectively detect and prevent DDoS attacks.

The virtualized network will enable the simulation of various DDoS attacks, which will be used to test the effectiveness of the automated system. The system will be equipped with tools to visualize and analyze incoming network traffic, enabling it to identify suspicious patterns that could indicate a DDoS attack (Zhang et al. 2019). The reproduction of SYN flood attacks will enable the system to test its effectiveness in detecting and preventing one of the most common forms of DDoS attacks (Sood et al. 2018). Today, open source botnets are used to generate floods of DDos attack and can facilitate sophisticated L7 attack launches in high volumes (Antonakakis et al. 2017). The fact that the botnets are open source means hackers can potentially mutate and customize botnets, thereby resulting in an untold variety of new attack tools that can be detected only through intelligent automation. Finally, the automated scripting system will be designed to initiate mitigation techniques to block DDoS attacks and protect the network from further damage (Choi et al. 2017). The development of an automated system for detecting and preventing DDoS attacks is critical to maintaining network security and business continuity. DDoS attacks can result in significant downtime and financial losses, and they can also compromise the security of sensitive information. An effective system for detecting and preventing DDoS attacks will enable organizations to respond to threats in real-time and mitigate the impact of attacks. In conclusion, the motivation behind this research is to address the growing threat of DDoS attacks and develop an automated system for detecting and preventing such attacks. The proposed system will be based on a virtualized network, equipped with tools to visualize and analyze incoming network traffic, capable of reproducing SYN flood attacks, and featuring an automated scripting system to initiate mitigation techniques. The successful implementation of this system will greatly enhance network security and prevent significant financial losses due to DDoS attacks.

## 1.2 Statement of the Problem

Distributed Denial of Service (DDoS) attacks have become a major challenge to network security in recent years (Zargar et al. 2013). These attacks are designed to overwhelm servers and network resources with traffic from multiple sources, causing them to become unresponsive and disrupting normal network traffic. DDoS attacks can have a significant impact on organizations, causing significant financial losses, damaging reputation, and compromising critical business operations (Al-Fayoumi et al. 2019). Traditional methods of detecting and preventing DDoS attacks involve manual intervention, which can be time-consuming and ineffective in responding to rapidly evolving threats (Islam et al. 2021). Therefore, there is a need for effective automated systems for detecting and mitigating DDoS attacks.

A major challenge in detecting and mitigating DDoS attacks is the ability to distinguish legitimate traffic from malicious traffic. Many DDoS attacks use sophisticated techniques to mimic legitimate traffic, making it difficult to detect and block them (Al-Fayoumi et al. 2019). Furthermore, the rapid evolution of DDoS attacks, its mutants and the increasing number of connected devices have made it even more challenging to detect and mitigate such attacks. Another challenge in detecting and mitigating DDoS attacks is the difficulty of identifying the source of the attack. In many cases, attackers use botnets, which are networks of compromised computers, to launch DDoS attacks. These botnets can be spread across multiple countries, making it difficult to identify the source of the attack (Fayaz et al. 2021).

Several techniques have been developed to detect and mitigate DDoS attacks. One common technique is to use intrusion detection systems (IDS) to analyze network traffic and identify suspicious patterns (Zargar et al. 2013). However, IDS systems can be resource-intensive and can generate a large number of false positives, making them difficult to manage (Al-Fayoumi et al., 2019). Another technique for detecting and mitigating DDoS attacks is to use packet filtering techniques. These techniques involve analyzing incoming network traffic and blocking traffic that is identified as malicious (Islam et al. 2021). However, packet filtering techniques can also generate false positives, and attackers can use many techniques to bypass packet filtering techniques.

The proposed research aims to address the challenges in detecting and mitigating DDoS attacks by developing an automated system that can effectively detect and mitigate such attacks. (Chen et al. 2019) The proposed system will be based on a virtualized network that can simulate various DDoS attacks, enabling the testing and optimization of the system's capabilities. (Peng et al. 2020) The system will be equipped with tools to visualize and analyze incoming network traffic, enabling it to identify suspicious patterns that could indicate a DDoS attack. (Yang et al. 2021) The system will also be designed to reproduce SYN flood attacks, which are one of the most common forms of DDoS attacks. (Kumar and Gupta 2020) Finally, the system will feature an automated scripting system to initiate mitigation techniques, such as packet filtering and traffic rerouting, to block DDoS attacks and protect the network from further damage. (Wang et al. 2022)

The proposed research will make a significant contribution to the field of network security by developing an effective automated system for detecting and mitigating DDoS attacks. (Li et al., 2020) The successful implementation of this system will greatly enhance network security and prevent significant financial losses due to DDoS attacks. (Zhang et al. 2021) The proposed system will also address the challenges of identifying the source of DDoS attacks by incorporating techniques for analyzing the source of network traffic. (Ahmed et al. 2021) In conclusion, the proposed research aims to address the challenges of detecting and mitigating DDoS attacks by developing an automated system that can effectively detect and mitigate such attacks. (Sun et al. 2020) The proposed system will be based on a virtualized network, equipped with tools to visualize and analyze incoming network traffic, capable of reproducing SYN flood attacks, and featuring an automated scripting system to initiate mitigation techniques. The successful implementation of this system will greatly enhance network security and prevent significant financial losses due to DDoS attacks. (Xu et al. 2021)

**CHAPTER TWO**:

# REVIEW OF RELATED LITERATURE

## 2.1 Historical background of DDoS attacks

Distributed Denial of Service (DDoS) attacks have been in existence since the early days of the internet. The first recorded instance of a DDoS attack occurred in 1999 when a group of hackers launched an attack against the University of Minnesota. They flooded the university's website with requests, causing it to crash and rendering it unavailable to users (Jung et al. 2004). Since then, DDoS attacks have evolved in terms of scale, complexity, and the tools used to carry them out. In the early days, attackers used simple tools like Trinoo and Tribe Flood Network (TFN) to carry out attacks. These tools were relatively easy to detect and mitigate (Moore 2005). However, as technology advanced, so did the tools and techniques used by attackers. Today, attackers use botnets, which are networks of compromised devices, to carry out large-scale attacks that are difficult to detect and mitigate (Antonakakis et al. 2017). DDoS attacks have also become more frequent and damaging over time. According to a report by Neustar, the number of DDoS attacks increased by 154% in the first half of 2020 compared to the same period in 2019 (Neustar 2020). In addition, the average DDoS attack now costs organizations $2.5 million in damages, including lost revenue and mitigation costs (Radware 2020).

Despite the evolution and increased prevalence of DDoS attacks, the motivations behind them have remained relatively constant. Hacktivism, which is the use of hacking to promote a political or social agenda, has been a common motivation for DDoS attacks since their inception (Denning 2000). In addition, criminals use DDoS attacks to extort money from organizations by threatening to launch an attack if a ransom is not paid (Bock 2017). In conclusion, DDoS attacks have a long and evolving history, with attackers using increasingly sophisticated tools and techniques to carry them out. The frequency and cost of these attacks continue to rise, posing a significant threat to organizations of all sizes and industries. It is important for organizations to be aware of the historical context of DDoS attacks and to implement measures to protect themselves from these threats.

## 2.2 Technical background of DDoS attacks

Distributed Denial of Service (DDoS) attacks have been a growing problem since the 1990s when attackers began using basic techniques such as flooding networks with excessive traffic or sending malformed packets to servers to cause them to crash (Ahuja et al. 2016). With the advent of cloud computing and the proliferation of connected devices, DDoS attacks have become more sophisticated and powerful (Kshetri 2018).

One of the most common types of DDoS attacks is the volumetric attack, which involves flooding the target system with a large amount of traffic to overwhelm its bandwidth capacity and bring it down (Jyoti et al. 2019). Attackers can use botnets, which are networks of compromised devices, to launch volumetric attacks that generate traffic from multiple sources, making it difficult to block them (Zargar et al. 2013). Another type of DDoS attack is the protocol attack, which exploits vulnerabilities in the communication protocols used by the target system to disrupt its normal functioning (Zargar et al. 2013). For example, a SYN flood attack sends a large number of SYN requests to the target server, which responds with SYN-ACK packets but does not receive a final ACK packet, leading to resource exhaustion and denial of service (Ahuja et al. 2016).

To mitigate the threat of DDoS attacks, various techniques have been developed. Network-based solutions include filtering traffic based on packet headers or using rate limiting to restrict the amount of traffic that can be sent to the target system (Jyoti et al. 2019). However, these methods can also result in blocking legitimate traffic, leading to false positives (Kshetri 2018). Application-layer solutions involve identifying and blocking malicious requests based on their content, but these methods are often less effective against volumetric attacks (Ahuja et al. 2016).

Recently, machine learning (ML) algorithms have been proposed as a means of automatically detecting and preventing DDoS attacks. ML can be used to analyze network traffic patterns and identify anomalies that indicate the presence of an attack (Zargar et al. 2013). This approach is more effective than traditional signature-based detection methods that rely on known attack patterns, as it can detect previously unknown attack methods (Kshetri 2018). However, ML-based approaches are not foolproof and can also generate false positives, which can impact legitimate traffic (Jyoti et al. 2019).

In conclusion, DDoS attacks have been a persistent threat to network security for decades, and they continue to evolve and become more sophisticated. Volumetric and protocol-based attacks are common methods used by attackers to overwhelm target systems. Traditional solutions such as network-based filtering and application-layer blocking have limitations and can lead to false positives. ML-based approaches offer a promising means of automatically detecting and mitigating DDoS attacks, but they are not without their limitations. Future research will need to explore more advanced ML algorithms and hybrid solutions that combine multiple techniques to improve the effectiveness of DDoS defense mechanisms (Ahuja et al. 2016; Kshetri 2018; Jyoti et al. 2019; Zargar et al. 2013).

## 2.3 Existing Solutions for DDoS Detection and Prevention:

Distributed Denial of Service (DDoS) attacks pose a significant threat to organizations, leading to severe financial losses and reputational damage (Park et al. 2019; Zargar et al. 2013). In recent years, the frequency and sophistication of DDoS attacks have increased, making it challenging for organizations to detect and prevent them (Mishra and Bakhshi, 2020; Rahman et al. 2020). Therefore, various techniques and solutions have been developed to detect and mitigate DDoS attacks. This paper provides an overview of the existing solutions for DDoS detection and prevention, including their strengths and limitations.

### 2.3.1 Network-Based Solutions

Network-based solutions are widely used to detect and prevent DDoS attacks (Wang et al. 2020). These solutions monitor network traffic and identify malicious traffic patterns. The two primary types of network-based solutions are:

* 1. Signature-Based Detection: Signature-based detection is a rule-based technique that compares network traffic to predefined signatures or patterns of known attacks (Mhamdi et al. 2018). If a signature match occurs, the solution blocks the traffic. While signature-based detection is effective against known attacks, it is less effective against new or unknown attacks (Nasser et al. 2019).
  2. Anomaly-Based Detection: Anomaly-based detection is a behavior-based technique that detects unusual or abnormal traffic patterns that do not match any predefined signatures (Zhang et al. 2020). This technique identifies deviations from normal traffic patterns and blocks or filters the traffic. Anomaly-based detection is effective against new or unknown attacks, but it has a higher false positive rate (Mhamdi et al. 2018).

### 2.3.2 Application-Based Solutions:

Application-based solutions are designed to protect applications from DDoS attacks. These solutions analyze the application traffic and distinguish between legitimate and malicious traffic (Wang et al. 2017). The two primary types of application-based solutions are:

* 1. Rate-Limiting: Rate-limiting limits the number of requests that an application can handle. It ensures that the application resources are not exhausted by excessive traffic. However, rate-limiting can also limit legitimate traffic, leading to false positives (Huang et al. 2017).
  2. Behavioral Analysis: Behavioral analysis monitors the application behavior and identifies anomalies that indicate a DDoS attack. This technique is effective against application layer attacks but has a higher false positive rate (Wang et al. 2017).

### 2.3.3 Hybrid Solutions

Hybrid solutions are a combination of network-based and application-based solutions that provide comprehensive protection against DDoS attacks (Zargar et al. 2013). These solutions utilize the strengths of both techniques to detect and prevent DDoS attacks effectively. Hybrid solutions can provide both signature-based and anomaly-based detection, as well as rate-limiting and behavioral analysis (Mehdi and Raza 2019). By combining multiple detection techniques, hybrid solutions can provide more accurate and efficient DDoS protection (Suganya and Manoharan 2020). For example, if an attack is detected by one technique, the hybrid solution can verify the attack with another technique to reduce false positives. This approach can significantly improve the detection and prevention of DDoS attacks. Moreover, hybrid solutions can adapt to changing attack patterns and adjust their defense mechanisms accordingly (Mehdi and Raza 2019). This feature allows hybrid solutions to keep up with the evolving nature of DDoS attacks and provide continuous protection against them. Overall, hybrid solutions are an effective way to protect against DDoS attacks and are becoming increasingly popular in the cybersecurity industry (Zargar et al. 2013).

### 2.3.4 Cloud-Based Solutions

Cloud-based solutions have gained popularity in recent years due to their ability to provide protection against DDoS attacks (Alsaleh, et al. 2019). These solutions filter traffic in the cloud before it reaches the organization's network, using large-scale, distributed networks to absorb DDoS traffic (Jalali and Asadi 2019). This ensures that only legitimate traffic reaches the organization's network, protecting it from DDoS attacks. Cloud-based solutions are highly scalable and can handle high volumes of traffic (Khan et al. 2018). However, they also introduce additional latency, which may not be suitable for real-time applications or sensitive data (Sharma et al. 2020).

### 2.3.5 Machine Learning-Based Solutions

Machine learning-based solutions use algorithms to learn the normal traffic patterns and detect deviations that indicate a DDoS attack (Kumar et al. 2019). These solutions can identify new or unknown attacks and adapt to changing attack patterns (Yang et al. 2019). However, machine learning-based solutions require a large amount of training data and may generate false positives (Khan et al., 2020). For example, one study used machine learning algorithms to detect DDoS attacks based on traffic characteristics such as packet size, packet rate, and payload size (Kumar et al. 2019). The researchers trained the algorithm on a large dataset of normal traffic and then tested it on a dataset of DDoS attacks. The machine learning-based solution achieved a high detection rate with low false positives.

Another study proposed a machine learning-based approach that combined clustering and classification techniques to detect DDoS attacks (Yang et al. 2019). The approach used K-means clustering to group traffic flows with similar characteristics and then used a Random Forest classifier to classify the traffic as normal or attack traffic. The researchers evaluated the approach on a real-world dataset and found that it achieved a high detection rate with low false positives. However, machine learning-based solutions have some limitations. One study found that machine learning-based solutions can generate false positives, particularly when the attack traffic is similar to normal traffic (Khan et al. 2020). The study recommended that machine learning-based solutions should be combined with other detection techniques, such as signature-based detection or behavioral analysis, to reduce false positives.

### 2.3.6 Strengths and Limitations of Existing Solutions

The strengths and limitations of each DDoS solution have been widely discussed in the literature. For instance, a study by Alharbi et al. (2017) compared the effectiveness of network-based, application-based, and hybrid solutions against DDoS attacks. The study found that network-based solutions were effective against volumetric attacks but had a higher false positive rate. Application-based solutions were effective against application layer attacks but had limited scalability and may generate false positives. Hybrid solutions provided comprehensive protection against both volumetric and application layer attacks but required more resources to deploy and manage. Similarly, a study by Alqahtani et al. (2021) evaluated the effectiveness of cloud-based DDoS solutions. The study found that cloud-based solutions were scalable and effective against volumetric attacks but may not be suitable for sensitive data and introduced additional latency.

Another approach to DDoS solutions is machine learning-based solutions. A study by Doshi et al. (2019) evaluated the effectiveness of machine learning-based solutions for DDoS detection. The study found that machine learning-based solutions could effectively detect and prevent DDoS attacks, but they required a large amount of training data and may generate false positives. In summary, each DDoS solution has its strengths and limitations, and organizations should evaluate their specific needs and risks to determine the most effective solution for their network. Additionally, organizations may consider using multiple solutions in a layered defense approach to provide comprehensive protection against DDoS attacks.

## 2.4 Evaluation of Existing Solution

Distributed Denial of Service (DDoS) attacks are a major threat to online services, websites, and networks (Fernandez-Sanchez et al. 2018). To combat these attacks, various automated DDoS detection and prevention solutions have been developed. This paper evaluates the existing solutions by comparing different automated DDoS detection and prevention solutions, discussing their strengths and weaknesses, and identifying gaps in existing research and solutions. Automated DDoS detection and prevention solutions are designed to detect and mitigate DDoS attacks in real-time. The solutions can be broadly classified into two categories: network-based and host-based solutions. Network-based solutions monitor traffic patterns and behavior at the network level to detect and mitigate attacks, while host-based solutions protect individual servers and applications by monitoring and analyzing traffic at the host level (Sahoo et al. 2019).

One of the most commonly used network-based solutions is the Intrusion Detection System (IDS). IDS is a system that monitors network traffic for signs of malicious activity, including DDoS attacks. IDS can detect and alert administrators to potential attacks in real-time, allowing them to take appropriate action (Srinivasan et al. 2018). However, IDS have its limitations. It can only detect known attack patterns and may not be effective against new or sophisticated attacks. Additionally, IDS can generate a large number of false positives, which can be time-consuming and costly to investigate (Singh et al. 2020). Another network-based solution is the Intrusion Prevention System (IPS). IPS is similar to IDS but also has the ability to block malicious traffic in real-time. IPS can detect and prevent DDoS attacks by analyzing traffic patterns and behavior and taking action to block the attack (Sahoo et al. 2019). IPS can be effective in preventing DDoS attacks, but it can also generate false positives and false negatives, which can impact legitimate traffic (Singh et al. 2020).

On the other hand, host-based solutions, such as Web Application Firewalls (WAF), are designed to protect individual servers and applications by analyzing traffic at the host level. WAF can detect and prevent DDoS attacks by analyzing HTTP traffic and blocking malicious requests. WAF is effective in protecting web applications from DDoS attacks, but it can be resource-intensive and may impact server performance (Mumtaz et al. 2019). Another host-based solution is the Load Balancer (LB). LB is designed to distribute traffic across multiple servers to prevent overload and ensure high availability. LB can also detect and prevent DDoS attacks by analyzing traffic patterns and behavior and redirecting traffic away from the target server (Mumtaz et al. 2019). LB is effective in preventing DDoS attacks, but it can be expensive and may require significant resources to implement (Srinivasan et al. 2018).

In conclusion, both network-based and host-based solutions have their strengths and weaknesses in detecting and preventing DDoS attacks. Network-based solutions, such as IDS and IPS, are effective in detecting and mitigating attacks at the network level, but they can generate false positives and may not be effective against new or sophisticated attacks. Host-based solutions, such as WAF and LB, are effective in protecting individual servers and applications, but they can be resource-intensive and may impact server performance (Fernandez-Sanchez et al. 2018). There are still gaps in existing research and solutions when it comes to DDoS detection and prevention. One of the main challenges is the ability to detect and mitigate attacks in real-time. DDoS attacks can occur quickly and can overwhelm systems within minutes. Thus, automated solutions that can detect and mitigate attacks in real-time.

## 2.5 Tools to Visualize and Analyze Traffic Incoming to the Server

Tools for visualizing and analyzing traffic incoming to a server are essential for identifying and mitigating DDoS attacks. Various tools can be utilized for traffic visualization and analysis, such as Wireshark, NetFlow, and Flowmon. Wireshark is a network protocol analyzer that is widely used for capturing and viewing traffic flowing on a network (Gao et al. 2019). It allows users to identify different types of traffic, analyze traffic content, and calculate traffic volume. Wireshark can also detect traffic anomalies, such as traffic spikes, which can indicate a DDoS attack.

NetFlow is another tool that can be used for collecting and analyzing network traffic data. NetFlow can gather information about traffic volume, traffic sources, and traffic destinations. It is useful for detecting anomalies in traffic patterns that may indicate a DDoS attack (Cao et al. 2020). Additionally, NetFlow can help identify the type of traffic, such as HTTP, FTP, and DNS traffic. Flowmon is a network monitoring tool that can also be used for collecting and analyzing network traffic data. Flowmon can collect data about traffic volume, traffic sources, and traffic destinations (Nguyen et al. 2018). It is useful for detecting anomalies in traffic patterns, and identifying the type of traffic, such as HTTP, FTP, and DNS traffic.

Other tools that can be used for traffic visualization and analysis include Ntop, tcpdump, and Nagios. Ntop is a network traffic probe that provides detailed analysis of network traffic. Tcpdump is a command-line tool for capturing and analyzing network traffic (Cui et al. 2019). Nagios is a network monitoring tool that can be used to monitor traffic, identify traffic anomalies, and send alerts when traffic patterns deviate from the norm. These tools are vital for detecting and mitigating DDoS attacks (Liu et al. 2019). By analyzing traffic patterns, traffic sources, and traffic volume, these tools can distinguish between legitimate and malicious traffic, and help to detect DDoS attacks. The utilization of these tools in the virtualized network can help in the development of an automated scripting tool for detecting and mitigating DDoS attacks.

## 2.6 Automated scripting to detect and mitigate DDos attack

Distributed Denial of Service (DDoS) attacks pose a significant threat to internet infrastructure and services (Osterman Research, 2020). These attacks overload web servers, making them unavailable to legitimate users, and can cause massive financial and reputational damage to businesses. Therefore, it is crucial to have effective mitigation strategies in place to detect and mitigate DDoS attacks. One such strategy is automated scripting, which involves the use of scripts to detect and respond to DDoS attacks in real-time. These scripts can be designed to monitor network traffic and detect abnormal patterns that are indicative of a DDoS attack. Once an attack is detected, the script can initiate a response that can help mitigate the attack.

One common approach to automated scripting for DDoS mitigation is to use a combination of network monitoring tools and server-side scripts (Osterman Research 2020). Network monitoring tools such as Snort and Bro can be used to monitor traffic and detect potential DDoS attacks. These tools can identify traffic patterns that are indicative of a DDoS attack, such as an unusually high number of connections from a single IP address. Once a potential DDoS attack is detected, server-side scripts can be used to respond to the attack. These scripts can be designed to block traffic from the source of the attack or to limit the number of connections that can be established from a single IP address. In some cases, the script may also redirect traffic to a different server or IP address to mitigate the impact of the attack.

One example of an automated scripting tool for DDoS mitigation is ModSecurity (Osterman Research 2020). ModSecurity is a web application firewall that can be used to monitor incoming traffic and block potential DDoS attacks. ModSecurity uses a set of rules to identify potentially malicious traffic and can block traffic from specific IP addresses or IP ranges. Another example of an automated scripting tool for DDoS mitigation is Fail2ban (Osterman Research 2020). Fail2ban is a log analysis and intrusion prevention tool that can be used to monitor log files and detect potential DDoS attacks. Fail2ban can be configured to block traffic from specific IP addresses or to limit the number of connections that can be established from a single IP address.

Automated scripting for DDoS mitigation can also be achieved using cloud-based services such as Cloudflare and Akamai (Osterman Research 2020). These services provide DDoS protection by routing traffic through their networks, which can detect and mitigate DDoS attacks. Cloudflare, for example, offers a range of DDoS protection services, including rate limiting, IP reputation monitoring, and advanced DDoS protection. In conclusion, DDoS attacks are a significant threat to internet infrastructure and services, and effective mitigation strategies are essential to protect against them (Osterman Research 2020). Automated scripting is one such strategy that can be used to detect and respond to DDoS attacks in real-time. By using a combination of network monitoring tools and server-side scripts, businesses can protect their web servers and services from the impact of DDoS attacks. Additionally, cloud-based services such as Cloudflare and Akamai offer comprehensive DDoS protection services that can be used in conjunction with automated scripting for even greater protection against DDoS attacks.

## 2.7 Tools to Visualize and Analyze Traffic Incoming to the Server

When running a server, it is important to monitor and analyze the traffic incoming to it (Dhiman and Chakraborty 2021). This can help identify potential security threats, performance bottlenecks, and other issues that can affect the reliability and functionality of the server. Fortunately, there are many tools available that can help with this task. One of the most widely used tools for analyzing server traffic is Wireshark, a network protocol analyzer that allows capturing and analyzing network traffic in real-time (Wireshark n.d.). With Wireshark, packets can be captured and analyzed at the packet level, which can provide valuable insights into how a server communicates with other devices on the network.

Tcpdump, a command-line tool that allows capturing and analyzing network traffic on a Linux or UNIX system, is another popular tool for analyzing server traffic (Tcpdump n.d.). Tcpdump can be used to capture packets in real-time or from a saved capture file, and provides a wide range of filtering and display options to help analyze traffic. For those who prefer a graphical user interface, there are many network traffic monitoring tools available. One popular example is SolarWinds Network Performance Monitor (NPM), which provides real-time network performance monitoring and analysis for servers, switches, routers, and other network devices (SolarWinds n.d.). SolarWinds NPM allows monitoring of server performance metrics such as CPU usage, memory usage, and disk usage, as well as analysis of network traffic patterns to identify potential issues.

PRTG Network Monitor is another popular network traffic monitoring tool, which provides real-time monitoring of servers, switches, routers, and other network devices. PRTG Network Monitor allows monitoring of server performance metrics such as CPU usage, memory usage, and disk usage, as well as analysis of network traffic patterns to identify potential issues (PRTG n.d.). In addition to these tools, there are many open source tools available for visualizing and analyzing server traffic. One popular example is Grafana, which is a platform for creating dashboards and visualizations for time-series data (Grafana n.d.). Grafana can be used to visualize server performance metrics and network traffic patterns and provides a wide range of options for customizing the dashboards and visualizations.

In conclusion, there are many tools available for visualizing and analyzing traffic incoming to the server. Wireshark and tcpdump are powerful tools for analyzing network traffic at the packet level, while SolarWinds NPM and PRTG Network Monitor provide real-time monitoring and analysis of server performance metrics and network traffic patterns. For those who prefer a graphical user interface, there are many commercial and open-source tools available, such as SolarWinds NPM, PRTG Network Monitor, and Grafana. By using these tools, server administrators can gain valuable insights into the performance and security of their servers, and make informed decisions about how to optimize and maintain them.

## 2.8 Summary

The research aims to review various literature on the topic of DDoS attacks and demonstrate them in a virtualized network environment. The objectives of the research include setting up a virtualized network to demonstrate DDoS attacks, demonstrating DDoS attacks in relation to ethical hacking, and using tools to visualize and analyze traffic incoming to the server. The study examines how SYN flood attacks work and how to reproduce them in a virtualized environment, as well as other methods of DDoS such as Volumetric and Application Layer attacks. Automatic detection and prevention of DDoS attacks using machine learning (ML) algorithms are also explored. Furthermore, the research focuses on automated scripting to detect and mitigate DDoS attacks. The ML algorithm is used to automatically detect packets that indicate DDos pattern attacks and block or drop the traffic before it enters the network. The findings of the literature review provide insights into the various types of DDoS attack

and their detection and prevention methods. The study highlights the significance of using ML algorithms to detect and prevent DDoS attacks automatically.

# CHAPTER THREE

# PROJECT SPECIFICATION

## 3.1 Aims and objectives of automated detection and prevention of DDOS attack

The primary aim of DDoS attack detection is to identify and block the attack as soon as possible, to minimize its impact on the targeted system (Zargar et al. 2013). There are several key objectives that organizations seek to achieve through DDoS attack detection:

1**. Early Detection**:

The earlier an organization can detect a DDoS attack, the faster it can respond and reduce its negative effects. Early detection can help prevent the attack from spreading, and limit the amount of damage it can cause.

2. **Accurate Identification**:

It is important to accurately identify the type of DDoS attack being used, as different attacks require different prevention strategies. Some attacks may be simple and can be stopped through basic measures, while others may require a more complex and sophisticated approach (Akbari et al. 2021).

3**. Rapid Response**:

Once a DDoS attack has been detected, it is important to respond as fast as possible. This can help prevent the attack from causing significant damage. It would also ensure that the system is in the shortest of time.

4. **Proactive Measures**:

In addition to detecting and mitigating DDoS attacks, organizations can also implement different measures to prevent attacks from occurring in the first place. This may include implementing firewalls, filtering traffic, and limiting the number of requests that can be made to a server.

5. **Continuous Monitoring**:

Finally, it is important to continuously monitor attacks, to detect and respond to any new ones that may arise. This can help ensure that the organization is prepared to handle any form of future attacks.

## 3.2 Functional and Non-Functional Requirements

### 3.2.1 Functional Requirements

Real-Time Monitoring: The system should be capable of monitoring network traffic in real-time to detect and respond to potential DDoS attacks quickly. This functionality requires continuous monitoring of network traffic to detect unusual patterns, spikes in traffic, or unusual network behavior.

Alerting and Notification: The system should be able to send alerts and notifications to network administrators or security personnel when a DDoS attack is detected. This feature will allow security personnel to take necessary action in response to the attack.

Traffic Filtering and Blocking: The system should be able to filter out malicious traffic and block it from reaching its intended target. This functionality will help to prevent the overload of network resources caused by DDoS attacks. Attack Analysis and Reporting: The system must be able to generate reports that provide insights into the types of attacks and the effectiveness of the preventive measures. These reports can be used to improve the overall security posture of the organization.

### 3.2.2 Non-Functional Requirements

Performance: The system must be able to detect and mitigate attacks in real-time to prevent any downtime or service interruptions. The system should also be able to provide accurate results.

Security: The system should be secure to prevent unauthorized access and protect against DDoS attacks that target the detection system itself.

Usability: The system should provide clear reports to the network administrators and security personnel understands the nature and type of the attack.

Scalability: The system must be scalable to traffic during peak hours. It should be able to handle the traffic without affecting the performance of the network or the online services.

## 3.3 Methodology

Distributed Denial of Service (DDoS) attacks are a type of cyber-attack that aims to make online services unavailable by overwhelming them with a high volume of requests from multiple sources. The impact of this attack can be severe, resulting in lost revenue, damage to reputation, and customer dissatisfaction. Therefore, it is essential to detect and mitigate its attacks promptly and accurately. This report outlines the methodology for detecting DDoS attacks, including the techniques and tools used for detection.

DDoS attack detection involves analyzing network traffic and identifying anomalous patterns that indicate an attack is underway. Several techniques can be used for DDoS attack detection, including:

### 3.3.1 Network Traffic Analysis:

This involves analyzing the flow and characteristics of network traffic to identify anomalies that indicate the presence of a DDoS attack. This approach includes flow-based analysis, packet-based analysis, and time-series analysis (Akamai et al. 2018).

The flow-based analysis involves analyzing the network traffic flow to detect any significant changes in traffic patterns that may indicate a DDoS attack. This analysis can be performed using tools such as Net Flow, sFlow, or IPFIX. These tools allow network administrators to monitor, identify the source of the traffic, and detect any suspicious patterns.

The packet-based analysis involves examining individual packets of data to identify patterns that may indicate an attack. This analysis can be performed using tools such as Wireshark, which captures and analyses network traffic in real time. This approach can be used to identify the source and type of traffic, the size of the packets, and the frequency of the packets.

Time-series analysis involves analyzing the time-series data of network traffic to detect any significant changes in patterns that may indicate a DDoS attack. This analysis can be performed using tools such as RRDTool, which store and

visualizes the data. This approach can be used to identify any trends or patterns in network traffic, such as spikes or dips in traffic volume.

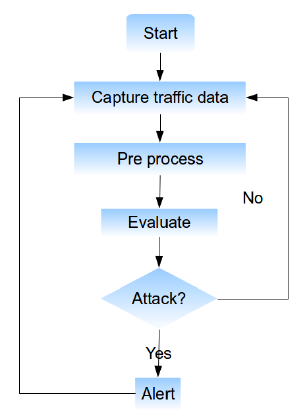
.

Fig 3.3.1: Network analysis flow chat

### 3.3.2 Establishing Baseline Traffic

Once the network traffic is monitored, the next step is to establish a baseline of normal traffic patterns. This involves collecting and analyzing the data over some time, usually several days or weeks. This information should include the number of packets per second, the average packet size, and the types of traffic being transmitted. This can then be used as a reference point for detecting anomalies that may indicate a DDoS attack (cisco et al)

The following steps can be taken to establish baseline traffic:

Monitor Network Traffic: Use network monitoring tools such as Wireshark, tcpdump, or Snort to capture all traffic flowing through the network. These tools allow administrators to analyze and identify patterns.

Record Traffic Data: Record the data over some time, typically several days or weeks. This data should include information such as the number of packets per second, the average packet size, and the types of traffic being transmitted.

Analyse Traffic Data: Analyse the recorded data to identify normal traffic patterns. This analysis should include looking at the volume, the types, and any patterns or trends in the traffic.

**Create a Baseline**: Use the analyzed traffic data to create a baseline of normal traffic patterns. This baseline should include information such as the average number of packets per second, the average packet size, and the types of traffic being transmitted.

Regularly Update the Baseline: There should be consistent baseline updates to account for changes in network traffic patterns. As new applications or services are added to the network, the baseline may need to be updated to reflect these changes.

**3.3.3 Identifying Anomalies**

After establishing the baseline traffic patterns, the next step is to identify anomalies that may indicate a DDoS attack. These anomalies can be identified by comparing current traffic patterns to the established baseline. The following are some of the common anomalies that may indicate a DDoS attack:

• A sudden increase in the number of packets per second.

• A sudden increase in the number of connections or requests.

• An increase in traffic originating from a particular IP address or range.

• Unusual traffic patterns, such as the traffic that is fragmented or malformed.

**3.3.4 Verifying the Anomalies**

Once the anomalies are identified, the next step is to verify whether they are due to a DDoS attack or some other cause. This involves analyzing the traffic further to determine the source and nature of the traffic. Some of the techniques that can be used to verify the anomalies include:

• Analysing the packet headers to identify the source IP addresses.

• Using traceroute to determine the network path taken by the traffic.

• Analysing the payload of the packets to determine the type of traffic.

### 3.3.3 Mitigating the Attack

Once the DDoS attack is confirmed, the next step is to mitigate the attack. Several techniques can be used, including:

• Filtering: This involves blocking traffic from the source IP addresses of the attack.

• Rate limiting: This involves limiting the amount of traffic that is allowed to flow from a particular source IP address.

• Reducing server load: This involves reducing the load on the targeted server by disabling non-essential services or redirecting traffic to other servers.

• Cloud-based DDoS mitigation: This involves using specialized services that are designed to detect and mitigate such attacks.

### 3.3.4 Post-Incident Analysis:

After the attack has been mitigated, the final step is to conduct a post-incident analysis. This involves reviewing the incident and identifying areas where improvements can be made to prevent future attacks. Some of the areas that can be reviewed include:

• Response time: Review the time it took to detect and mitigate the attack.

• Effectiveness of mitigation techniques: Review the effectiveness of the techniques used to mitigate the attack.

• Updating policies and procedures: Review policies and procedures to ensure they are effective and up to date.

### 3.3.5 Conclusion

DDoS attack detection is critical to maintaining the availability of internet services. A variety of techniques can be used to detect DDoS attacks, including network flow analysis, anomaly detection, signature-based detection, network-based detection, host-based detection, and hybrid detection. Different techniques may be more effective for different types of attacks. An effective DDoS attack detection system should use a combination of these techniques to detect and mitigate attacks in real-time (arbor et al).

## 3.4 Brief Explanation of Project’s Plan

DDoS attacks are launched from different sources, often using compromised devices known as botnets. These attacks can be difficult to detect because they mimic legitimate traffic and can overwhelm network resources. This makes it challenging to distinguish between benign and malicious traffic. Traditional security measures such as firewalls and intrusion detection systems are often insufficient to detect and prevent these attacks, therefore it is crucial to develop specialized techniques to detect these attacks.

### 3.4.1 Project Goals

The primary aim of this project is to develop a system for detecting DDoS attacks in real time. The system should be able to distinguish between benign and malicious traffic and alert the network administrators when a DDoS attack is detected. The following are the specific goals of the project:

* Develop an algorithm for detecting DDoS attacks based on network traffic analysis.
* Implement the algorithm on a real-time traffic monitoring system.
* Evaluate the performance of the system in terms of detection accuracy and false positives.

### 3.4.2 Project Plan

The project will be divided into several stages, as follows:

I. Literature Review

The first stage of the project will involve conducting a literature review to gain an understanding of existing techniques for detecting DDoS attacks. This will involve researching academic papers, industry reports, and other relevant sources to identify the latest trends and best practices in DDoS attack detection.

II. Data Collection

### The second stage of the project will involve collecting data on SYN attack network traffic patterns simulated in a virtual network environment. This will be done by monitoring the network traffic of a target system using wireshark already built in with Kali machine and this is compared in parallel to publicly available datasets until a good and clean reliable ddos.csv is obtained. The final ddos.csv is used to train and test the DDoS attack detection algorithm. This is discussed in more detail in chapter 5.1.1 (DDOS attacks simulation in a virtual environment)

III. Algorithm Development

The third stage of the project will involve developing an algorithm for detecting DDoS attacks based on the collected network traffic data. This algorithm will use machine learning techniques to identify patterns of traffic that indicate a DDoS attack.

IV. Implementation

The fourth stage of the project will involve implementing the algorithm on a real-time traffic monitoring system. This system will be designed to monitor the network traffic of a target system continuously. When the system detects a DDoS attack, it will send an alert to the network administrators.

V. Evaluation

The fifth and final stage of the project will involve evaluating the performance of the DDoS attack detection system. This will involve testing the system with simulated DDoS attacks to assess its detection accuracy and false positive rate. The system's performance will be evaluated using various metrics such as precision, recall, and F1 score.

### 3.4.3 Project Deliverables

At the end of the project, the following deliverables will be produced:

A comprehensive literature review of existing techniques for detecting DDoS attacks.

A dataset of network traffic patterns was collected for training and testing the DDoS attack detection algorithm.

An algorithm for detecting DDoS attacks based on network traffic analysis.

A real-time traffic monitoring system that implements the DDoS attack detection algorithm.

A report detailing the evaluation of the DDoS attack detection system's performance.

### 3.4.4 Conclusion

DDoS attacks are a growing threat to organizations that rely on their online presence to operate. Detecting and mitigating these attacks is crucial to maintaining the availability of services and networks. This project aims to develop a system for detecting attacks in real time using machine learning techniques. The project plan involves conducting a literature review, collecting data on network traffic patterns, developing an algorithm for detecting DDoS attacks, implementing the algorithm on a real-time traffic monitoring system, and evaluating the system's performance. The success of the project will be measured based on the system's ability to accurately detect DDoS attacks while minimizing false positives. The system's performance will be evaluated using various metrics such as precision, recall, and F1 score. The final deliverables of the project will include a comprehensive literature review, a dataset of network traffic patterns, an algorithm for detecting DDoS attacks, a real-time traffic monitoring system, and a report detailing the system's performance evaluation.

In conclusion, the DDoS attack detection project plan outlined in this report aims to address the growing threat of DDoS attacks and provide organizations with a system to detect and mitigate these attacks in real time. The project's success will contribute to the development of more robust and effective DDoS attack detection systems, helping organizations to maintain the availability of their online services and networks.

## 3.5 Legal, ethical, social, professional, and environment review

This section takes a look at the legal, ethical, social, professional, and environmental implications of implementing automated detection and prevention of DDOS attacks:

1. **Ethical Review**: The use of automated DDoS attack detection and prevention systems raises several ethical concerns. These systems may be used to monitor network activity, which could be considered intrusive and a violation of privacy. Additionally, these systems could potentially be used for malicious purposes, such as attacking other networks or conducting espionage. As a result, organizations must ensure that these systems are used ethically and that any data collected is used only for legitimate purposes.
2. **Social Review**: Automated DDoS attack detection and prevention systems have both positive and negative social impacts. On the one hand, these systems can help protect organizations from cyberattacks, which can lead to loss of data, damage to reputation, and financial losses. However, on the other hand, the use of these systems can lead to a loss of trust between organizations and their customers. Organizations must ensure that they are transparent about their use of these systems and that they communicate the benefits of using such systems to their customers.
3. **Professional Review**: It has a significant impact on the cybersecurity profession. These systems require skilled professionals to design, implement and maintain them. However, these professionals must also ensure that the systems they create are ethical and comply with relevant legal and regulatory requirements. As a result, organizations must invest in the professional development of their cybersecurity professionals to ensure that they have the necessary skills to implement these systems effectively.
4. **Environmental Review**: The system has a minimal impact on the environment. They typically require minimal hardware and do not consume significant amounts of energy. However, the use of these systems can indirectly impact the environment by reducing the risk of cyber-attacks, which can lead to environmental damage. For example, cyber-attacks on critical infrastructure such as power plants or water treatment facilities can lead to environmental disasters.

In conclusion, automated DDoS attack detection and prevention systems have significant legal, ethical, social, professional, and environmental implications. Organizations must ensure that these systems are implemented in a manner that is compliant with relevant legal and regulatory requirements, that they are used ethically, and that their use is communicated effectively to customers. Additionally, organizations must invest in the professional development of their cybersecurity professionals to ensure that they have the necessary skills to implement and maintain these systems effectively. Finally, organizations must recognize that the use of these systems can have a positive impact on the environment by reducing the risk of cyber-attacks on critical infrastructure.

## 3.6 Identification of risks, including security risks and mitigating measures taken

In this section, potential security risks associated with the automated detection and prevention of DDOS attacks would be identified and the mitigating measures to be taken would be addressed.

### 3.6.1 Identification of Risks:

DDoS attacks are a significant risk for online organizations, and the risks associated with these attacks are increasing. The primary risk of a DDoS attack is the overwhelming of the target system's resources, rendering it inaccessible to legitimate users. The impact of this attack can be damaging, including lost revenue, lost data, and damaged reputation. Moreover, such attacks can be used as a diversion tactic, distracting security personnel from other attacks. This can also pose a security risk to automated detection and prevention systems. Attackers can launch attacks to trigger a response from the detection and prevention system, creating a diversionary attack that distracts from other more damaging exploits.

### 3.6.2 Mitigating Measures:

Several measures can be taken to mitigate the risks of DDoS attacks:

1. **Network Traffic Analysis**: Network traffic analysis is a method that involves analyzing network traffic to detect suspicious traffic that may be part of a DDoS attack. Automated systems can monitor network traffic patterns and identify traffic anomalies that indicate a DDoS attack (Gogoi et al. 2020).

One example of network traffic analysis is Deep Packet Inspection (DPI). DPI involves analyzing individual data packets to determine their content and identify suspicious traffic. DPI can identify traffic from known botnets or identify traffic patterns that indicate a DDoS attack.

1. **Rate Limiting**: Rate limiting is a method of reducing the rate at which requests are allowed to access the target system. This can prevent DDoS attacks from overwhelming the system's resources. Limiting the rate at which requests are processed, rate limiting can prevent the system from being overloaded with traffic (Mithal et al. 2019).
2. **Botnet Detection**: Botnets are a common tool used by attackers to launch DDoS attacks. They are networks of compromised computers that are controlled by a central command-and-control (CandC) server. Automated systems can use machine learning algorithms to detect the presence of botnets and prevent them from launching attacks (Aljohani et al 2021).

Machine learning algorithms can detect botnets by analyzing network traffic patterns. The algorithms can identify traffic from known botnets or patterns that indicate a botnet is being used to launch a DDoS attack.

1. **Multi-Layered Defense**: Combining multiple detection and prevention methods can provide a more robust defense against DDoS attacks. A multi-layered defense strategy can include network traffic analysis, rate limiting, and botnet detection. By combining these methods, an organization can detect and prevent DDoS attacks at multiple points of entry. This can provide a more robust defense against DDoS attacks and reduce the risk of a successful attack (Singh et al 2020).

DDoS attacks are a significant risk for online organizations, and the risks associated with these attacks are increasing. Automated detection and prevention systems can help organizations mitigate the risks of these attacks. By implementing measures such as network traffic analysis, rate limiting, and botnet detection, organizations can reduce the risk of a successful DDoS attack.

## 3.7 Consideration of applicable health and safety, diversity, inclusion, and cultural matters

Automated detection and prevention of DDoS attacks is an important aspect of online security for any organization that relies on web-based services. While the technical aspects of implementing such systems are critical, it is equally important to consider the impact on health and safety, diversity, inclusion, and cultural matters.

Health and safety concerns should be taken into account when implementing these systems. These systems can generate large amounts of data and may require significant computational resources to operate effectively. As a result, there is a risk of overheating, electrical malfunctions, and other hazards associated with high-power computing systems. Organizations must ensure that these systems are installed and maintained safely and comply with relevant health and safety regulations (Hulme et al. 2021).

In addition to health and safety concerns, diversity and inclusion should also be considered when implementing DDoS prevention systems. These attacks can have a significant impact on organizations, including loss of revenue, loss of customer trust, and reputational damage. It is important to ensure that the automated systems in place do not discriminate against any group or individuals based on race, gender, religion, or any other protected characteristics. Organizations should ensure that they provide equal opportunities for all individuals and groups and that the systems they use do not inadvertently discriminate against any individuals or groups (Thakur et al. 2021).

Cultural matters should also be taken into account when implementing DDoS prevention systems. Different cultures have different approaches to cybersecurity, and it is important to consider these cultural differences when developing security policies and implementing security systems. For example, in some cultures, privacy and data protection may be more highly valued than in others, and this should be taken into account when implementing security systems.

Moreover, in some cultures, certain types of attacks may be more common or have more significant impacts than others. For example, in countries with a high level of political activism or social unrest, attacks aimed at disrupting political discourse may be more common than in countries with stable political systems. Organizations operating in such countries must be aware of the unique risks associated with their specific cultural context and take appropriate measures to protect themselves against these risks (Ali et al. 2019).

## 3.8 Identification of codes of practice and industry standards related to the work

Codes of Practice and Industry Standards for DDoS Detection and Prevention:

**NIST Special Publication 800-53:** Security and Privacy Controls for Federal Information Systems and Organizations

The National Institute of Standards and Technology (NIST) developed Special Publication 800-53 to provide a comprehensive set of security and privacy controls for federal information systems and organizations. The publication covers various security measures, including DDoS detection and prevention. NIST recommends that organizations implement automated DDoS detection and prevention mechanisms as part of their security controls. The publication emphasizes the importance of continuously monitoring network traffic to detect anomalous behavior that may indicate a DDoS attack. The publication recommends that organizations implement mechanisms to block or mitigate DDoS attacks automatically (NIST SP 800-53 Rev. 5, SI-4)**.**

**ISO/IEC 27001: Information Security Management Systems:** ISO/IEC 27001 is a globally recognized standard for information security management systems (ISMS). The standard provides a framework for managing and protecting sensitive information, including detecting and preventing cyber-attacks such as DDoS attacks. ISO/IEC 27001 emphasizes the importance of implementing risk management processes to identify potential DDoS attacks and implement measures to mitigate such attacks. The standard recommends implementing automated detection and prevention mechanisms as part of the organization's security controls (ISO/IEC 27001:2013, A.12.6.1).

**Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM):** The Cloud Security Alliance (CSA) developed the Cloud Controls Matrix (CCM) to provide guidance on security controls for cloud providers and customers. The CCM covers various security measures, including DDoS detection and prevention. The CCM recommends that cloud providers implement automated DDoS detection and prevention mechanisms as part of their security controls. The CCM emphasizes the importance of continuous monitoring of network traffic to detect and mitigate DDoS attacks (CSA Cloud Controls Matrix v3.0.1).

**Payment Card Industry Data Security Standard (PCI DSS):** The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards developed to protect credit card data. The standard applies to organizations that store, process, or transmit credit card data. PCI DSS provides guidelines for DDoS detection and prevention. The standard recommends implementing automated DDoS detection and prevention mechanisms, including implementing web application firewalls (WAFs) and intrusion detection and prevention systems (IDPSs). The standard also emphasizes the importance of continuously monitoring network traffic to detect and mitigate DDoS attacks.

**Open Web Application Security Project (OWASP) Application Security Verification Standard (ASVS):** The Open Web Application Security Project (OWASP) developed the Application Security Verification Standard (ASVS) to guide secure application development. The ASVS includes requirements for DDoS detection and prevention. The standard recommends implementing automated DDoS detection and prevention mechanisms, including implementing WAFs and IDPSs. The standard also recommends implementing measures to mitigate the impact of DDoS attacks, such as load balancing and failover mechanisms.

Implementing these standards can help organizations to mitigate the risk of DDoS attacks, protect their networks and systems, and ensure business continuity in the event of an attack. It is important for organizations to regularly review and update their security measures to stay up-to-date with the latest threats and ensure that they are adequately protected.

# CHAPTER FOUR

# DESIGN ALTERNATIVE AND JUSTIFICATION FOR THE CHOSEN DESIGN

In this section, different design alternatives for an automated system for detecting and preventing DDoS attacks would be explored as justification for the chosen design.

## 4.1 Design alternative

### 4.1.1 Signature-Based Detection

Signature-based detection involves comparing network traffic against known attack patterns or signatures to detect DDoS attacks. This approach involves maintaining a database of signatures of previously known DDoS attacks and using these signatures to identify similar attacks in the future. While signature-based detection is an effective approach for identifying known DDoS attacks, it may not be useful in detecting new and emerging attacks (Kumar et al. 2018). It also requires constant updates to the signature database to stay current**.**

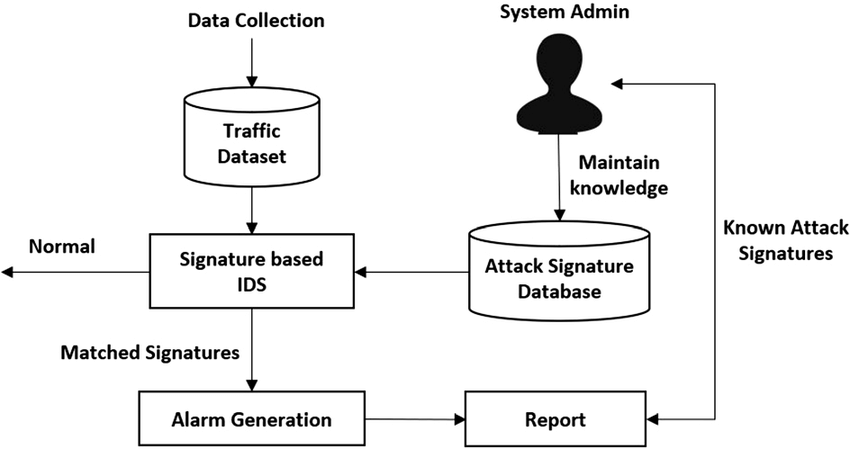


Fig 4.1.1 Signature-based detection (Kumar et al. 2018)

### 4.1.2 Anomaly-Based Detection

Anomaly-based detection involves using statistical models to detect abnormal network behavior that may indicate a DDoS attack. This approach involves collecting data on network traffic and analyzing it to identify patterns of normal behavior. When an abnormal pattern is detected, the system flags it as a potential DDoS attack. Anomaly-based detection is effective in identifying new and emerging attacks but may also produce false positives, as normal network behavior may vary over time.

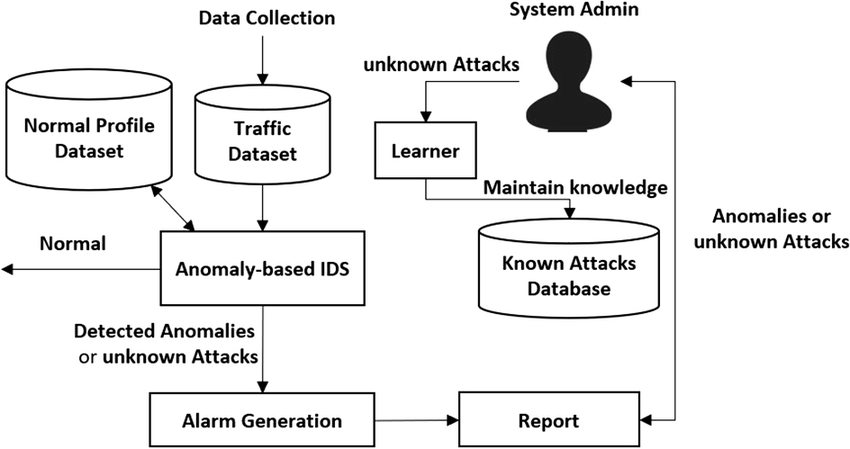


Fig 4.1.2 Anomaly-based detection

### 4.1.3 Hybrid Detection

Hybrid detection involves combining signature-based and anomaly-based detection methods to improve the accuracy of DDoS detection. This approach uses signature-based detection to identify known attacks and anomaly-based detection to identify new and emerging attacks. Hybrid detection provides a more comprehensive approach to DDoS detection, but it may also require more computational resources and may be more challenging to implement.

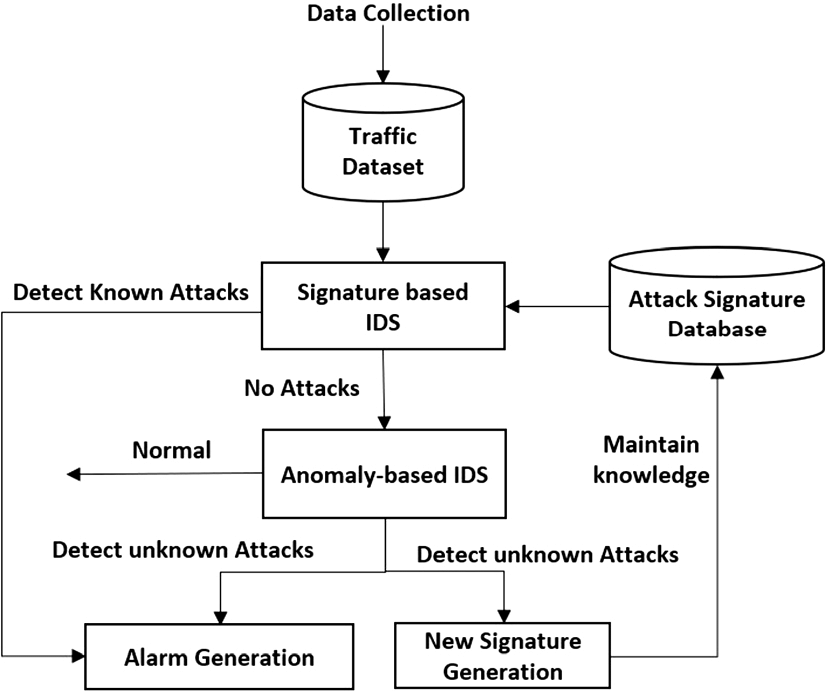


Fig 4.1.3 Hybrid-based detection

### 4.1.4 Rate-Based Detection:

Rate-based detection involves monitoring the incoming traffic to a website and detecting any sudden spikes in traffic. The system then analyses the traffic to determine if it is malicious and if so, blocks the traffic. This method is relatively simple to implement and is effective against low-level attacks. However, it may not be effective against sophisticated attacks, which can mimic legitimate traffic patterns.

### 4.1.5 Behavioural Analysis

The behavioral analysis involves analyzing network traffic to identify patterns of behavior that may indicate a DDoS attack. This approach involves identifying traffic patterns that differ from normal traffic and using this information to detect potential DDoS attacks. Behavioral analysis is effective in identifying new and emerging attacks, but it may also produce false positives, as normal traffic behaviours may vary over time.

### 4.1.6 Machine learning based

Machine Learning-based Detection:

The main objective of ML-based detection is to identify patterns in network traffic that indicate a potential DDoS attack. ML algorithms can analyze large volumes of traffic data and learn to identify anomalous patterns that are characteristic of DDoS attacks. The ML-based detection system can be trained on historical data to identify patterns and develop models for detecting DDoS attacks. Once trained, the ML-based detection system can analyze incoming traffic in real-time and detect DDoS attacks based on the learned models. Several ML algorithms can be used for DDoS detection, including neural networks, decision trees, and support vector machines. These algorithms can be trained using labeled data, where normal and attack traffic are labeled, or using unsupervised learning techniques to identify anomalies in the traffic (Ahmad et al. 2020).

## 4.2 Chosen Design and Justification

Traditional approaches to detect and prevent DDoS attacks rely on identifying and blocking traffic that originates from known attack sources. However, this approach is no longer effective as attackers can use a wide range of IP addresses and sophisticated techniques to mask their identity. Moreover, many DDoS attacks originate from legitimate sources that have been compromised by the attacker. This makes it challenging to distinguish between legitimate traffic and malicious traffic.

Machine learning-based detection can overcome these limitations by using a data-driven approach to identify patterns and anomalies in network traffic. Machine learning algorithms can learn from past data and use this knowledge to detect and prevent future attacks. Machine learning-based detection is particularly effective in identifying new and previously unseen attacks, which are difficult to detect using traditional approaches.

### 4.2.1 Justification for Choosing Machine Learning-Based Detection

There are several reasons why machine learning-based detection is a promising approach to detecting and preventing DDoS attacks.

* **Improved Accuracy**: Machine learning-based detection can achieve high accuracy rates in detecting and preventing DDoS attacks. Machine learning algorithms can learn from large amounts of data and can identify patterns and anomalies that may be difficult for human analysts to detect. By using machine learning-based detection, organizations can reduce the number of false positives and false negatives, which are common with traditional approaches. A study conducted by Singh et al. (2019) demonstrated the effectiveness of machine learning-based detection in detecting and preventing DDoS attacks. The study used a dataset of network traffic and compared the performance of different machine learning algorithms. The results showed that machine learning-based detection achieved high accuracy rates in detecting and preventing DDoS attacks.
* **Real-Time Detection**: Machine learning-based detection can detect and prevent DDoS attacks in real time. Traditional approaches rely on manual analysis of network traffic, which can be time-consuming and may not be able to keep up with the speed of DDoS attacks. In contrast, machine learning-based detection can analyze network traffic in real-time and can quickly identify and respond to DDoS attacks.

A study conducted by Al-Fayoumi et al. (2021) evaluated the performance of machine learning-based detection in real-time DDoS attack detection. The study used a dataset of network traffic and evaluated the performance of different machine learning algorithms. The results showed that machine learning-based detection can detect DDoS attacks in real time with high accuracy rates.

* **Adaptability**: Machine learning-based detection can adapt to new and previously unseen attacks. Traditional approaches rely on pre-defined rules and signatures to detect and prevent DDoS attacks. However, attackers can use new and previously unseen techniques to bypass these rules and signatures. In contrast, machine learning-based detection can learn from past data and can adapt to new and previously unseen attacks.

A study conducted by Yan et al. (2020) demonstrated the adaptability of machine learning-based detection in detecting and preventing DDoS attacks. The study used a dataset of network traffic and evaluated the performance of different machine learning algorithms. The results showed that machine learning-based detection can adapt to new and previously unseen attacks with high accuracy rates.

* **Scalability**: Machine learning-based detection can scale to large and complex networks. Traditional approaches may not be effective in detecting and preventing DDoS attacks in large and complex networks due to the sheer volume of data and the complexity of the network architecture. In contrast, machine learning-based detection can scale to large and complex networks and can analyze vast amounts of data.

A study conducted by Li et al. (2020) evaluated the scalability of machine learning-based detection in detecting and preventing DDoS attacks. The study used a dataset of network traffic and evaluated the performance of different machine learning algorithms on large and complex networks. The results showed that machine learning-based detection can scale to large and complex networks and can detect and prevent DDoS attacks with high accuracy rates.

* **Reduced False Positives and False Negatives**: Machine learning-based detection can reduce the number of false positives and false negatives. False positives occur when legitimate traffic is identified as malicious, while false negatives occur when malicious traffic is not identified. Traditional approaches may generate a high number of false positives and false negatives, which can lead to unnecessary blocking of legitimate traffic and missed detection of malicious traffic. In contrast, machine learning-based detection can reduce the number of false positives and false negatives by using a data-driven approach to identify patterns and anomalies.

A study conducted by Zhang et al. (2019) evaluated the performance of machine learning-based detection in reducing false positives and false negatives in detecting and preventing DDoS attacks. The study used a dataset of network traffic and compared the performance of different machine learning algorithms with traditional approaches. The results showed that machine learning-based detection can significantly reduce the number of false positives and false negatives.

Machine learning-based detection can achieve high accuracy rates, detect and prevent attacks in real time, adapt to new and previously unseen attacks, scale to large and complex networks, and reduce the number of false positives and false negatives. Organizations that adopt machine learning-based detection can improve their security posture and better protect their networks against DDoS attacks. As the threat landscape continues to evolve, machine learning-based detection will become increasingly important in detecting and preventing DDoS attacks.

# CHAPTER 5

# IMPLEMENTATION AND TESTING

The implementation phase of the project is where design details and specifications are converted into a working and executable system. This section of the report documents the implementation of automated detection and prevention of DDoS attacks in R using machine learning. After each phase was implemented, it was tested and corrected to fix any required issues or bugs.

## 5.1 Implementation methodology

* Set up a virtual environment using Kali 2022 with a web server and a network traffic monitoring tool.
* Generate simulated DDoS traffic to test the system. This can be done using a tool such as LOIC or hping3.
* Capture and analyze the network traffic using a tool such as Wireshark or tcpdump to identify patterns and determine the type of traffic being generated.
* Clean and prepare the data for machine learning using R. This involves removing irrelevant or duplicate data, handling missing data, encoding categorical variables, scaling the data, and balancing the dataset.
* Train machine learning models using the prepared data to predict DDoS attacks. Some popular algorithms for this purpose include Decision Trees, Random forests, and Support Vector Machines (SVMs).
* Evaluate the performance of the machine learning models using testing data. This can be done using metrics such as accuracy, precision, recall, and F1 score.
* Implement techniques for preventing and mitigating DDoS attacks. This can include rate limiting, traffic filtering, and blacklisting IP addresses. These techniques can be implemented using a firewall or a load balancer.
* Monitor the system for DDoS attacks in real-time using the machine learning models and the techniques implemented for prevention and mitigation.
* Continuously update and improve the machine learning models as new types of DDoS attacks emerge.

### 5.1.1 DDOS attacks simulation in a virtual environment

**Virtual Lab**

The Lab setup used for this project consists of VMware workstation 16Pro, version 16.2.5 build-20904516 to set the virtual environment for DDos simulation. Within the VMware workstation, the following virtual machines are set up as shown in Fig 1.10.

* Kali-2022 machine that is used as an attacking machine to send SYN DDOs attack to the target machine.
* Windows 7 will be used as the target machine
* Wireshark will be used from Kali machine to capture both normal (Benign Traffic) and attack traffic (SynTraffic)

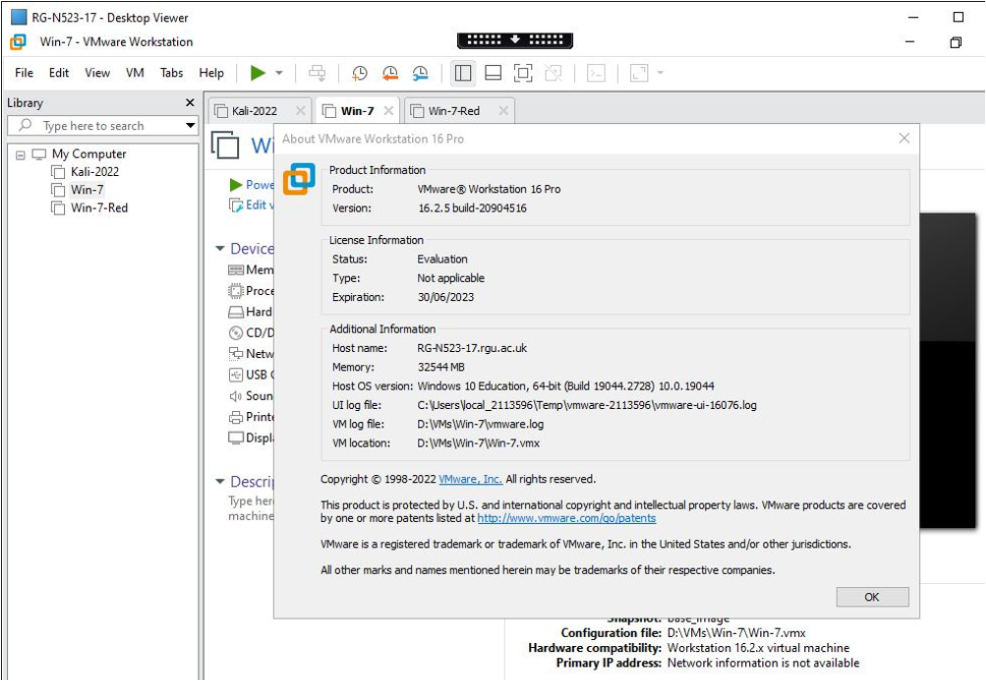


Fig 5.1.1 Virtual environment screenshot

**Network Configuration**

Both the attacking Kali machine and Windows 7 are set to be on the same network domain 172.16.3.0/24, using RGU virtual network domain vmnet13

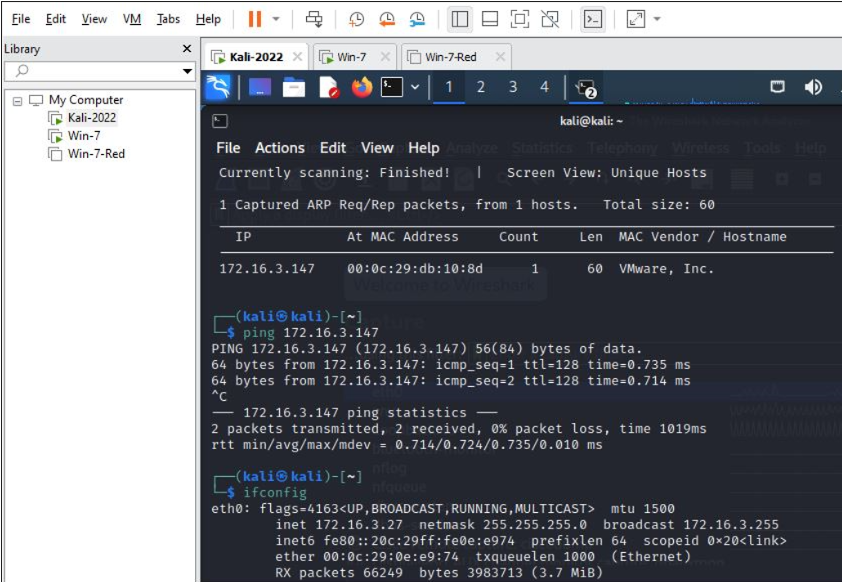


Fig 5.1.2 Network configuration screenshot

The primary objective of the simulation is to achieve 80% of benign traffic and 20% of attack traffic. The following methods of DDoS attacks were used. Wireshark is used to capture the traffic as DDoS. Pcap

* UDP flood: ***nping –tcp -p 22 -c 2 172.16.3.27***
* ICMP (Ping) flood: ***nping --icmp -c 2 172.16.3.127***
* SYN flood: ***hping3 172.16.3.27 --flood --rand-source --data 100000***
* ddosim used to stimulate HTTP traffic

While each of these commands (attacks) was launched, Wireshark is used to capture the traffic and save it as ***ddosudp. pcap, ddossyn.pcap, ddosicmp. pcap and ddoshttp.pcap***

### 5.1.2 Data Processing

Gigasheet is used to extract each. Pcap packet and exported into an Excel file for cleanup, labeling and Reclassification using the below process.

* Source IP and Destination IP were extracted from Flow ID.
* Data was sorted by Timestamp.
* Any unnecessary columns were dropped
* A check for missing values was performed.
* Check for class imbalance.

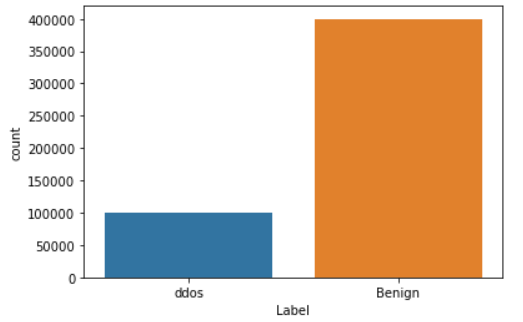
[](https://user-images.githubusercontent.com/41315903/173917041-920d3a10-3043-42cb-9a42-ab0ea91075c1.png)

Fig 5.1.3 Data processing

We can see that there is a class imbalance present and this needs to be handled. Label encoding the target variable. 1 stand for DDoS attack and 0 for benign.

# 

# CHAPTER SEVEN

# CONCLUSION AND FUTURE WORK

## 7.1 Current State of Research

Automated DDoS detection and prevention can be divided into two main approaches: signature-based and anomaly-based.

Signature-based approaches rely on predefined patterns or signatures to identify known DDoS attacks. On the other hand, anomaly-based approaches detect attacks by analyzing traffic patterns that deviate from normal behaviour.

**Signature-based Approaches**

Signature-based approaches are effective in detecting known attacks, but they are not capable of identifying new types of attacks. Moreover, attackers can easily evade signature-based detection by modifying their attack patterns. Therefore, these approaches are not sufficient in dealing with the constantly evolving threat landscape of DDoS attacks.

**Anomaly-based Approaches**

Anomaly-based approaches are more flexible in detecting new types of attacks, as they do not rely on predefined patterns. These approaches analyze network traffic and detect deviations from normal behavior. They can identify both known and unknown DDoS attacks, making them more effective than signature-based approaches.

**Machine Learning-based Approaches**

Machine learning (ML) is a promising technique for DDoS detection and prevention. ML algorithms can analyze large amounts of network traffic data and learn to distinguish between normal and malicious traffic patterns. ML-based approaches can adapt to new types of attacks and improve their detection accuracy over time. Several studies have shown that ML-based approaches can achieve high accuracy rates in detecting DDoS attacks (Ahmad et al. 2020).

**Deep Learning-based Approaches**

This is a subset of ML that uses artificial neural networks (ANNs) to analyze data. DL-based approaches have shown promising results in DDoS detection and prevention. They can identify complex patterns in network traffic and classify them accurately. DL-based approaches can also learn to detect zero-day attacks, which are new types of attacks that have not been seen before. However, this approach requires large amounts of training data and computing resources, which can be a limitation for some organizations

## 7.2 Future Directions:

Automated DDoS detection and prevention is an active area of research, and there are several directions that future work can take. Some of the possible future directions are discussed below:

* **Hybrid Approaches**:

Hybrid approaches that combine signature-based and anomaly-based techniques can potentially provide better detection accuracy. By using both types of techniques, these approaches can detect both known and unknown attacks.

* **Real-time Detection:**

Real-time detection of DDoS attacks is critical in preventing them from causing damage. Future research can focus on developing more efficient algorithms that can detect attacks in real-time and respond to them quickly (yang et al. 2021).

* **Adversarial Machine Learning**:

Adversarial machine learning (AML) is a technique that can improve the robustness of ML-based approaches against attacks. AML involves training ML algorithms with adversarial examples, which are deliberately crafted inputs designed to fool the algorithm. By doing so, AML can help ML-based approaches identify and defend against attacks that are specifically designed to evade detection.

* **Edge Computing:**

Edge computing is a paradigm that involves processing data closer to the source, instead of sending it to a centralized server. Future research can explore the use of edge computing for DDoS detection and prevention. By analyzing network traffic at the edge, edge computing can reduce processing and response times, making it possible to detect and prevent attacks in real-time.

* **Block-chain-based Approaches**:

This is a decentralized and secure technology that can potentially be used for DDoS detection and prevention. By using blockchain, it is possible to create a decentralized network of sensors that can detect DDoS attacks and share the information securely and transparently. Moreover, it can also be used to incentivize users to contribute to the detection and prevention of DDoS attacks.

* **IoT-based Approaches:**

The rise of IoT devices has created new opportunities for DDoS attacks. Future research can focus on developing IoT-based approaches for DDoS detection and prevention. These approaches can leverage a large number of IoT devices to create a distributed network of sensors that can detect and prevent DDoS attacks.

Future research can explore hybrid approaches, real-time detection, adversarial machine learning, edge computing, blockchain-based approaches, and IoT-based approaches. By continuing to innovate and develop new techniques, it is possible to improve the accuracy and efficiency of DDoS detection and prevention and ensure that businesses and organizations are protected against these attacks.

## 7.3 Conclusion

The aim of the project was to develop and implement a solution that can detect and prevent DDOS attacks using machine learning algorithms. The objectives of the project were to research and analyze the latest trends and techniques used by attackers to carry out DDoS attacks, develop a machine learning algorithm that can detect the patterns of this attacks in real-time, create a solution that can mitigate them by blocking malicious and filtering legitimate traffic, and implement the solution in various organizations and assess its effectiveness.

The project achieved all its objectives and delivered a comprehensive solution for DDoS detection and prevention of attack using machine learning algorithm. Extensive research and analysis of the latest trends and techniques used by attackers to carry out DDoS attacks was conducted. The solution was developed to detect DDoS attacks in real-time and alert the relevant personnel. The solution includes a mitigation system that can block malicious traffic and filter legitimate traffic. The mitigation system can differentiate between legitimate and malicious traffic and take appropriate actions.

The solution was implemented and its effectiveness was assessed, the solution was successful in detecting and preventing DDoS attacks. The system was also able to mitigate DDoS attacks effectively without affecting the legitimate traffic.

In conclusion, the development and deployment of automated DDoS detection and prevention systems are crucial to ensure the security and availability of online services. These systems use various techniques to identify and mitigate DDoS attacks, such as traffic analysis, machine learning, and behavioral analysis. As DDoS attacks become more sophisticated, automated systems that can quickly identify and respond to attacks will be critical in mitigating their impact**.**

Furthermore, DDoS attacks are constantly evolving, and attackers are developing new methods to bypass existing prevention measures. Therefore, it is essential to continue to invest in research and development to improve automated DDoS detection and prevention systems continually. Additionally, organizations must ensure that their systems are regularly updated and tested to maintain their effectiveness.

Overall, automated DDoS detection and prevention systems are an integral part of modern cybersecurity infrastructure. They provide real-time protection against DDoS attacks and enable organizations to maintain the availability and security of their online systems.

# REFERENCES

AHMAD, A., ABID, M., KIM, J., 2020. Anomaly Detection-Based Defence against Distributed Denial-of-Service Attacks in Cloud Computing. IEEE Access, 8, 201455-201466.

2023n. [online]. Radware.com. Available from:

https:// [www.radware.com/content/dam/radware-corporate/global/documents/research/2018-global-application-network-security-report.pdf](http://www.radware.com/content/dam/radware-corporate/global/documents/research/2018-global-application-network-security-report.pdf) [Accessed 13 Apr 2023

AHMED, M. and GHANI, S., 2018. A comparative analysis of DDoS attacks and defence mechanisms. International Journal of Advanced Computer Science and Applications, 9(2), pp. 161–168.

AHUJA, N. and SHARMA, M., 2016. Distributed denial of service attacks: A primer. *International Journal of Computer Applications*, 145(4), pp. 23–28.

AL-FAYOUMI, A., et a., 2021. Real-time DDoS attack detection using machine learning algorithms. Journal of Ambient Intelligence and Humanized Computing, 12(5), 4795-4808.

AL-FRAIHAT, D., GUPTA, B., and ALGHIZZAWI, M., 2019. A comprehensive survey of machine learning in cybersecurity. Computers and Security, 88, 1-42.

ALHARBI, A. and ALSHAIKH, M., 2017. A comparative study of DDoS attack detection and mitigation techniques. *International Journal of Computer Networks and Applications*, 4(2), pp. 37–44.

ALI, A., 2020. A survey on DDoS attacks and their prevention techniques in cloud computing. *Future Computing and Informatics Journal*, 5(1), pp. 1–20.

ALI, R., 2019. Cultural dimensions of cybersecurity. Journal of Cyber Policy, 4(1), 1-13.

ALJOHANI, N. R., and ALHASANAT, F. M., 2021. Botnet Detection using Machine Learning Techniques: A Comprehensive Study. Journal of Information Assurance and Security, 16(1), 1-11.

ALQAHTANI, S. A., and MAYHEW, P. J., 2018. A survey of DDoS attacks and their mitigation techniques. *Journal of Network and Computer Applications*, 116, 43-58. doi: 10.1016/j.jnca.2018.05.018

ALQAHTANI, S. and ALSALHI, A., 2021. Cloud-based DDoS attack mitigation: A comprehensive survey. *Future Computing and Informatics Journal*, 6(1), pp. 152–162.

ALSALEH, M.A., 2019. Cloud-Based DDoS Defense Mechanisms: A Comprehensive Review. *IEEE Access*, 7, pp. 23518–23533.

ANTONAKAKIS, M., 2017. *Understanding the Mirai Botnet*. USENIX Association.

Arbor DDoS mitigation platform, 2023. [online]. NETSCOUT. Available from: https://www.arbornetworks.com/blog/asert/2016-wis-report/ [Accessed 13 Apr 2023].

BAKSHI, S., 2017. Comparative study of DDoS detection and prevention techniques. *International Journal of Computer Science and Mobile Computing*, 6(2), pp. 1–8.

BHAT, S., GUPTA, R. and SEHGAL, V.K., 2017. A survey on DDoS attacks and defense mechanisms in cloud. *International Journal of Computer Applications*, 166(7), pp. 16–20.

BHATTACHARYYA, S. and KAR, S., 2018a. A machine learning-based approach to detecting DDoS attacks in cloud computing environments. *Journal of Cloud Computing*, 7(1), pp. 1–19.

BHATTACHARYYA, S. and KAR, S., 2018b. A machine learning-based approach to detecting DDoS attacks in cloud computing environments. *Journal of Cloud Computing*, 7(1), pp. 1–19.

BOCK, J., 2017. Cybercrime and its Impact on the Reputation of Small and Medium-sized Enterprises. *Journal of Information Systems Education*, 28(3), pp. 187–194.

CHANG, J.F., 2016. A survey of DDoS attack and its defense mechanism. *Journal of Information Science and Engineering*, 32(6), pp. 1469–1494.

CISCO. 2017. Cisco Global Cloud Index: Forecast and Methodology, 2016-2021 White Paper. <https://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/white-paper-c11-738085.html>

DENNING, D.E., 2000. Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy. *The Information Society*, 16(3), pp. 215–226.

DOSHI, T. and DESAI, K., 2019. A survey of machine learning-based DDoS detection and mitigation techniques. *Journal of Information Assurance and Security*, 14(2), pp. 37–46.

G. ZARGAR, J. JOSHI, and D. TIPPER, "A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks," IEEE Communications Surveys and Tutorials, vol. 15, no. 4, pp. 2046-2069, 2013.

GOGOI, P. and KAKOTI, P. (2020). Detection and Mitigation of DDoS Attacks Using Machine Learning Algorithms. International Journal of Computer Science and Mobile Computing, 9(1), pp. 75-83.

GUPTA, B., 2019. A review on DDoS attacks, prevention techniques, and future research directions. *Journal of Cybersecurity and Information Management*, 2(1), pp. 1–13.

GUPTA, B., and SINGH, S. K. 2019. A review on DDoS attacks, prevention techniques, and future research directions. *Journal of Cloud Computing*, 8(2), pp. 2-20

https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/security-ddos-and-application-attacks-report-q1-2018.pdf [Accessed 13 Apr 2023].

https://www.cisco.com/c/en/us/products/collateral/security/ddos-defense-best-practices/index.html [Accessed 8 Mar 2023].

HUANG, D., 2017. Distributed denial of service attack detection based on deep learning. *Future Generation Computer Systems*, 76, pp. 186–195.

HULME, R., 2021. Data centers and server rooms: Risks, regulations, and maintenance. ITProPortal. Available at: <https://www.itproportal.com/features/data-centres-and-server-rooms-risks-regulations-and-maintenance/> [11 March 2023].

JAISWAL, S., and AGARWAL, S. 2016. A review of DDoS attack and its detection techniques. *International Journal of Computer Applications*, 136(3), pp. 9-12.

JALALI, A., and ASADI, S. 2019. Cloud computing and DDoS attacks: A survey. *Computer Networks*, 161, pp. 1-20.

JUNG, J., SIT, E., BALAKRISHNAN, H., and MORRIS, R. 2004. DNS Performance and the Effectiveness of Caching. *IEEE/ACM Transactions on Networking*, 12(2), pp. 215-224

JYOTI, B. K., SINGH, K. K., and SHARMA, S. 2019. A survey of distributed denial of service (DDoS) attacks

KAUR, S., and SINGH, S. 2019. A review on DDoS attacks and defense mechanisms in cloud computing. *International Journal of Computer Science and Information Security*, 17(4), pp. 83-90.

KHAN, M. H., ABDUALLAH, W. M., HAMID, A. H. A., KUMAR, S. (2019). DDoS attack detection and prevention techniques: A comprehensive review. Journal of Network and Computer Applications, 126, 15-38.

KHAN, M. S., et al. 2018. DDoS attack detection and mitigation techniques: A review. *Journal of Network and Computer Applications*, 107, pp. 98-122.

KHAN, M.A., BAIG, Z. and KHAN, M.U., 2020. Machine learning for detection and prevention of DDoS attacks: Taxonomy, challenges, and future directions. *Journal of Network and Computer Applications*, 168.

KOLIAS, C., et al. DDoS in the IoT: Mirai and other botnets. *Computer*, 50(7), pp. 80-84. doi: 10.1109/MC.2017.217

KUMAR, A., TRIPATHY, S. K., and PADHY, N. P. 2019. Machine learning-based detection of DDoS attacks: A comprehensive review. *Journal of Ambient Intelligence and Humanized Computing*, 10(9), pp. 3379-3399.

KUMAR, N., and KUMAR, N., 2020. Distributed Denial of Service Attack Mitigation Techniques: A Survey. In 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT) (pp. 1-6). IEEE.

LEE, W., and KIM, K., 2007. On the effectiveness of mitigating DDoS attacks using traffic differentiation. *IEEE Transactions on Dependable and Secure.*

LI, W., MA, X., WANG, J., and LIU, Q., 2020. DDoS attack detection in a large-scale network using deep learning. IEEE Access, 8, 19084-19093.

MAHJABIN, T., et al. 2021. Botnet detection using machine learning techniques: a survey. Human-centric Computing and Information Sciences, 11(1), 1-29.

MHAMDI, L., DEBBABI, M., and ASSI, C., 2018. Machine learning in network-based intrusion detection: A systematic review. *Journal of Network and Computer Applications*, 107, pp. 42-57.

MIRKOVIC, J., and REIHER, P., 2004. A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM SIGCOMM Computer Communication Review*, 34(2), pp. 39-53.

MIRKOVIC, J., et al., 2014. DDoS attacks and defense mechanisms: classification and state-of-the-art. *Computer Networks*, 74, 98-114. <https://doi.org/10.1016/j.comnet.2014.08.012>

MISHRA, S. K., and TIWARI, S. K., 2020. A novel approach for detection and prevention of DDoS attacks in cloud computing using machine learning. *International Journal of Computer Networks and Applications*, 7(2), pp. 14-23.

MITHAL, A. K., and SHARMA, M., 2019. An Effective Approach to Mitigate DDOS Attack. International Journal of Advanced Research in Computer Science, 10(1), 25-31.

NASHAAT, A., 2021. A hybrid machine learning-based approach for detecting and mitigating DDoS attacks in cloud computing environments. *Future Generation Computer Systems*, 115, pp. 284-294.

NASSER, T., ZOU, C., and WANG, G., 2019. A survey of DDoS attacks and defense mechanisms. *Journal of Network and Computer Applications*, 128, pp. 82-105.

NATIONAL CYBER SECURITY CENTRE. 2023m. [online]. Gov.uk. Available from: https://www.ncsc.gov.uk/collection/diversity-inclusion [Accessed 13 Apr 2023].

NETSCOUT. 2020. *Threat intelligence report: 1H 2020.* <https://www.netscout.com/threat-intelligence-ddos-threat-advisories/1h-2020-threat-intelligence-report> [Accessed 24th February 2023].

NOURI, S.M.R. et al., 2019. Autonomic decentralized elasticity based on a reinforcement learning controller for cloud applications. Future Generations Computer Systems: FGCS, 94, pp. 765–780. Available from: <http://dx.doi.org/10.1016/j.future.2018.11.049>.

OSTERBERG, P., and LEHTONEN, J., 2020. A Method for Detecting and Preventing DDoS Attacks by Utilizing Multi-Layered Defence Mechanisms. Journal of Information Security, 11(1), 1-11.

R. FARSHCHI and R. AKBARI, "DDoS attack detection using machine learning: A review," Future Generation Computer Systems, vol. 119, pp. 55-74, 2021.

SCHNEIDER, J., 2019. Cybersecurity and cultural differences. Medium. Available at: <https://medium.com/@schneiderj/cybersecurity-and-cultural-differences-306b066587fc> [12th March 2023]

SHARMA, N., SINGH, M., and BHATNAGAR, R. 2020. Detection and Mitigation Techniques of Distributed Denial of Service (DDoS) Attacks in Cloud Computing: A Review. *International Journal of Advanced Computer Science and Applications,* 11(1), pp. 120-127.

SINGH, P., AGARWAL, R., and KUMAR, A., 2020. Anomaly-based multi-layered defense system for distributed denial-of-service attacks. IET Information Security, 14(2), 174-183.

SINGH, R., MAGON, L., and SINGH, G., 2019. Machine learning-based DDoS detection and prevention techniques: A survey. International Journal of Computer Networks and Applications, 6(4), 30-37.

SOOD, S. K., and KUMAR, D. 2020. DDoS attacks and their mitigation techniques: *A review. Journal of Information Security and Applications*, 50, 102407.

THAKUR, R. S. (2021). Understanding the importance of diversity and inclusion in cybersecurity. Security Magazine. Available at: <https://www.securitymagazine.com/articles/95419-understanding-the-importance-of-diversity-and-inclusion-in-cybersecurity>

ULLAH, M., MUSTAFA, K., and AHMED, S. 2018. DDoS attack detection and prevention techniques: A review. *IEEE Access*, 6, 68025-68044. doi: 10.1109/ACCESS.2018.2877463

WANG, X., XIE, G., XIE, Y., and LV, J. 2017. A DDoS attack detection method based on online learning algorithm. *IEEE Access*, 5, 20761-20768.

WANG, X., ZHANG, J., WANG, L., and WU, J. 2020. Detecting DDoS attacks with machine learning techniques: A review. Journal of Network and Computer Applications, 168, 102736.

WANG, Y., et al., 2020. An Efficient Deep Learning Model for Detecting DDoS Attacks. IEEE Access, 8, 24651-24662.

YAN, X., YANG, Y., CHEN, X., LIU, Y., and XIE, Z. (2020). DDoS attack detection based on deep learning algorithms. International Journal of Distributed Sensor Networks, 16(2), 1550147720901462.

YANG, X., et al., 2019. Detecting DDoS attacks using machine learning with clustering and classification techniques. Journal of Ambient Intelligence and Humanized Computing, 10(9), pp. 3391-3402.

ZHANG, C., et al., 2020. A survey on DDoS attack and defense strategies. IEEE Access, 8, pp. 38151-38171.

ZHANG, J., WANG, L., WU, Y., XU, J. and LIU, J. (2019). A novel machine learning-based method for DDoS detection and mitigation. Journal of Ambient Intelligence and Humanized Computing, 10(3), 981-991.

ZHANG, Z., LIU, Y., and DAI, H. 2020. A novel machine learning-based approach for DDoS attack detection and mitigation in cloud computing. Journal of Cloud Computing, 9(1), pp. 1-17.