CHAPTER 1
INTRODUCTION

Today's digital infrastructures globally are under high risk of being attacked by Distributed Denial of Service (DDoS) attacks (Husák, M et al., 2019). These assaults can only be done using sophisticated equipment to determine malicious behavior in huge network traffic. To advance IDS, complexity-aware intelligent intrusion systems with higher feature engineering are necessary (Aamir, M. and Zaidi, S.M.A., 2019). The aim of this thesis to enhance feature engineering as an approach to intelligent DDoS incursion detection. The developed detection systems in the research are based on cutting-edge feature selection methods and ML algorithms. As an interconnected digital environment grows, such enhanced machinery will immensely facilitate the identification of DDoS attacks with regard to important data and infrastructure.

1.1. Security

Distributed Denial of Service (DDoS) attacks are one of the significant challenges to digital infrastructure security. Some of the contemporary approaches to DDoS prevention are often ineffective, particularly when firewalls cannot adapt to the change by themselves and do not recognize intrusion patterns (Yu, Z et al., 2023). To overcome these issues this research provides a new system to enhance security in complex digital networks. The research applies intelligent IDS to enhance security measures mainly focusing financial and online shopping firms; data breach in such firms can lead to severe consequences.

Intrusion Detection System is integrated into digital structures to find out about suspicious or illegitimate action. Traditional Intrusion Detection System are not suitable for dynamic structures (Zhong, M et al., 2024) (Liu, M et al., 2018) (Wang, H et al., 2024). As a result of their distributed nature and the contemporary infrastructure of the modern world, DDoS attacks are very hard. The anomaly-based approach proposed in this research to address these problems intrusion detection system for sophisticated digital networks. This method seeks to overcome the difficulties of protecting digital systems by identifying invasions with better accuracy. The efficiency of the suggested strategy in improving security and reducing the dangers of DDoS assaults is examined in terms of performance on relevant data.

1.2. Cyber Security Challenges

The security threats in the digital environment are numerous due to the nature of the environment and the distributed responsibility. These challenges include (Chivukula R et al., 2021) (Singh, C., and Jain, A. K, 2024) (Admass, W.S., Munaye, Y.Y. and Diro, A.A., 2024) (Rajasekharaiah, K.M., Dule, C.S. and Sudarshan, E., 2020):

- **Cyberattacks:** There is frequent danger from hackers through phishing, malware, ransomware, and denial-of-service attacks in organizations and people.
- **Data Breaches:** Should an unauthorized individual have access to certain data, it would cause financial loses, damage the company's reputation, and can become a punishable action.
- **Insider Threats:** Spiteful behavior or even a lack of attention from an organization's employees can lead to data vulnerability and contamination.
- **Cloud Security:** Protecting data and application running on the cloud against possible intrusions and leaks.
- **Mobile Security:** Securing the mobile devices and their applications primarily in the cases when users bring their own devices to work.
- **IoT Security:** Internet of Things gadgets tend to have lower levels of protecting measures, thereby they become prone to different cybercrimes and hacks.
- **Identity and Access Management (IAM):** Limit access to all system and info only to those who are eligible and authorized to use it.
- **Social Engineering:** Intentionally persuading the people to reveal secrets to them without telling them the truth.
- **Emerging Technologies:** Threats related to the new generation technologies, such as AI, blockchain, and quantum computing, in which new risks and threats are identified.
- **Supply Chain Vulnerabilities:** Liabilities that are inherent in using third-party vendors and suppliers that thereof have access to the firm's information technology systems.
- **Security Patching and Maintenance:** Checking that computers, networks and servers are updated frequently with protective patch files in cases of known exposures.

Solving these problems is possible only with the help of an integrated approach that implies the use of technology, process development, and the encouragement of risk prevention among users. Defending against cyber-attacks is important since they correlate to other security risks in detailing step-by-step to guard against and respond to cyber-attacks, we establish that there is a reciprocal relationship between cyber risks and other security threats. Managing cyber-attacks effectively improves the security of an organization as it is capable of protecting environments well. This research is centered on the design of an intelligent solution for the identification of cyber threats and counteraction to them in order to enhance the security measures effectively.

1.3. Types of Attacks

Cyber ecosystem is threatened by different attacks some of which take advantage of the features of these systems (Bhol, S.G et al., 2023). Here is the broad classification of Cyber-Attacks on Cyber Security principles (Li, Y. and Liu, Q., 2021) (Duo, W., Zhou, M. and Abusorrah, A., 2022) (Kaur, J. and Ramkumar, K.R., 2022) in Figure 1.1:

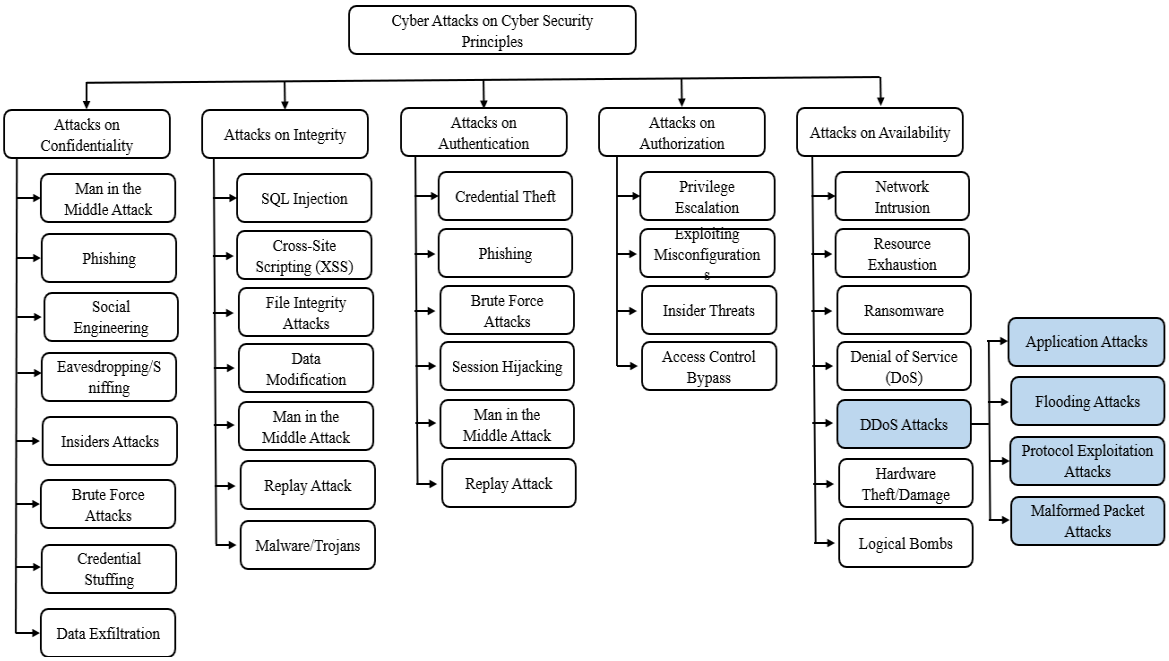

Figure 1.1 Cyberattacks against Cybersecurity Fundamentals

Cyber threats are diverse, and organizations need to know the types of attacks that exist to protect cybersecurity principles. These strikes can be detected early, and this makes it easy to reduce the impact of the damage that has been done. Through the use of effective

detection and mitigation systems, organizations can avoid large losses, meet legal requirements, retain public confidence and prevent business disruption. For this, users should be raised, and security has to be changed to avoid such acts and future risks. Threats are vital to realize in a highly technical world along with suitable solutions for protecting cyber security and assets. DDoS assaults and other attacks must be prevented to guarantee service security and dependability in traditional computing environments.

1.4. Denial of Service Attacks

An intrusion known as a DoS assault overloads the network, interrupting network connectivity or the service offered by the host to the legal user is reduced (Eliyan, L.F. and Di Pietro, R., 2021) (Nuiaa, R.R., Manickam, S. and Alsaeedi, A.H., 2021). The DoS attacks occur in the following possible ways,

- Disbursing computational resources such as bandwidth, storage capacity and CPU time.
- Disruption of network and the information of a computing system configuration.
- Interruption of network components.

The attackers usually target the DNS servers, routing devices, web sites and electronic mail services. The victim being attacked is usually unaware of the identity of attackers. The identification of DoS attack is a tedious task because the attackers usually imitate the activities of genuine users. Since the DoS tools for attack are powerful and easily accessible via internet, they are easy to bring them into the system but hard to detect. Because it floods the target system with traffic, the attack is very susceptible and prevents those with authorization from using it. These attacks may seriously disrupt networks by taking advantage of flaws in the infrastructure.

1.5 Distributed Denial of Service Attacks

The DoS is used as the fundamental module for the Distributed Denial of Service (DDoS). The DDoS attack is characterized by flooding huge amount of attack packets by zombies into victim system. Due to this, unwanted traffic is created which completely disconnect the network of the system of victims. While the attack was happening, the attacker makes one-to-one mapping with the server to overwhelm the resources of the

server. They will hide their identity, and this imposes a huge challenge on Intrusion Detection System to identify malicious and legitimate user. Eavesdroppers are serious attackers, who tries to identify the contents of the transmitted packet over the network and sometimes to modify the contents also. The characteristics of spoofing attack replace the legitimate node with illegitimate one. Botnets are agents that flood a network, opening the door for further assaults including spoofing, phishing, and denial-of-service attacks and so on (Sharafaldin, I et al., 2019) (Gupta, B.B. and Dahiya, A., 2021) (de Neira, A.B., Kantarci, B. and Nogueira, M., 2023). Figure 1.2 shows a particular DDoS assault scenario.

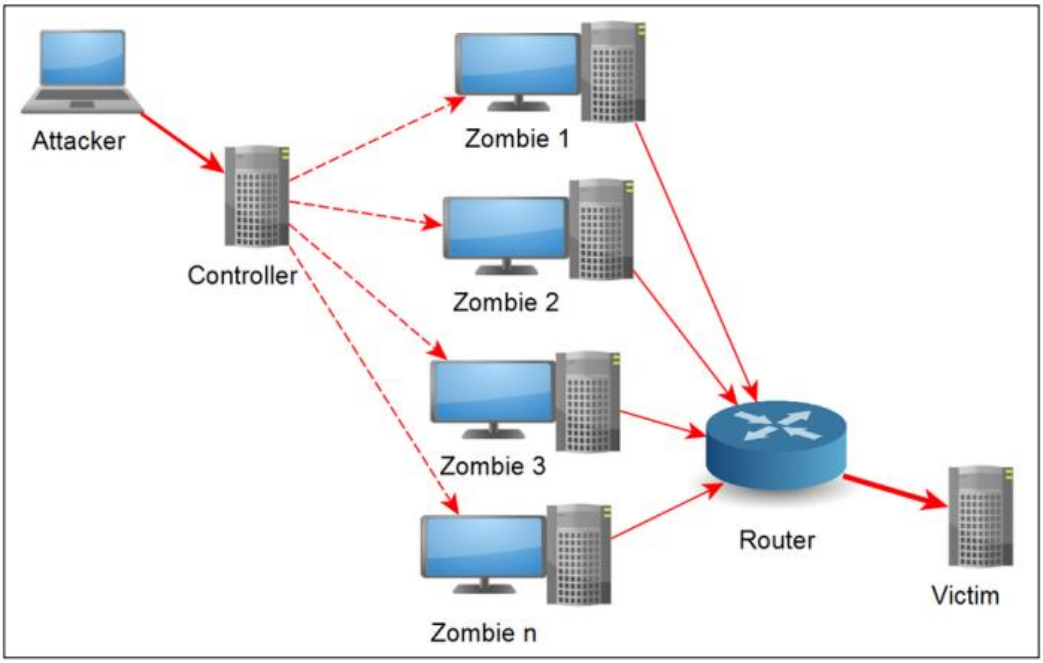

Figure 1.2: Example Scenario of DDoS attacks

A DDoS attack is carried out in several phases and has four main actors: an attacker, a controller, a victim, and zombies (Wang A et al, 2018). The attacker looks for remotely accessible system ports that are susceptible in order to initiate an assault. After identifying the vulnerability, the attacker sends malicious malware that replicates itself and initiates the attack when it is run on the targeted computer. Disguising the virus as a genuine Internet packet—for instance, by sending it as an attachment to an email—is another method of distributing it. The attacker has remote control over all of this. Spoofing is used to impede attack detection and characterization in order to stop agent machines from being discovered, with the exception of reflecting assaults.

1.5.1 DDoS Attack Types

Based on the method utilized, DDoS (Distributed Denial of Service) assaults may be roughly divided into three primary groups overwhelm the target. Each category encompasses various subtypes, focusing on different layers of network communication. Here is a detailed classification: These are a few typical DDoS attack kinds observed in the literature along with their categories and subtypes (Navruzov, E. and Kabulov, A., 2022) (Saini, P.S., Behal, S. and Bhatia, S., 2020) (Gaurav, A et al., 2022) seen in Figure 1.3.

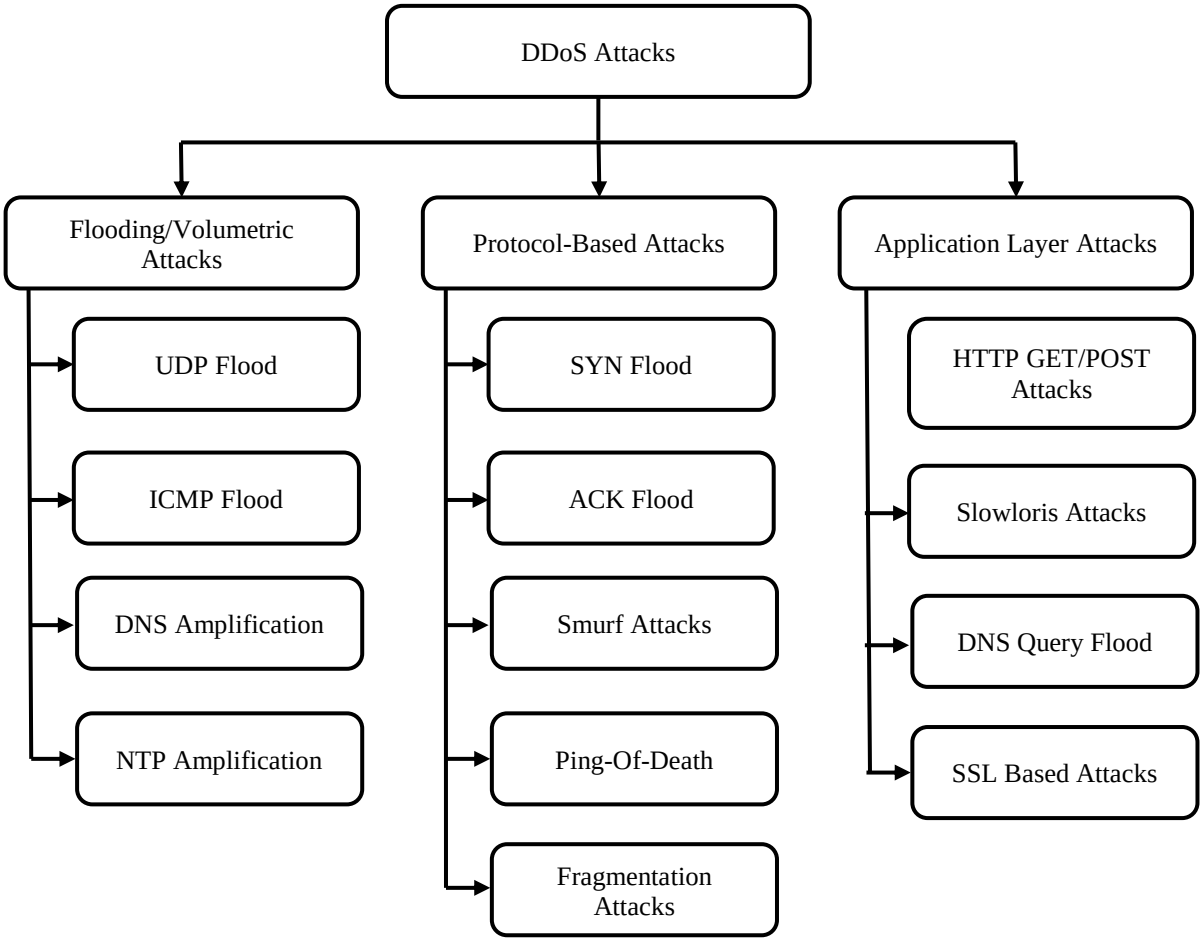

figure 1.3: DDoS attacks classification

1.5.1.1 Flooding/Volume-Based Attacks

The Flooding/In order to use up the target's available bandwidth, volumetric assaults bombard it with a lot of traffic. These assaults come in the following varieties (Jose, A.S., Nair, L.R. and Paul, V., 2021)

- **ICMP Flood:** Uses ICMP packets for echo requests (pings) to bombard the target.
- **UDP Flood:** Delivers numerous UDP packets to randomly selected ports on the target.
- **DNS Amplification:** Transmits a large amount of DNS responses to the target by taking advantage of DNS servers.
- **NTP Amplification:** Uses NTP servers to amplify traffic directed at the target.

1.5.1.2 Protocol-Based Attacks

These assaults take use of flaws in network protocols to disrupt communication between the target and legitimate users. Further the protocol-based attacks are classified into five, namely,

- **SYN Flood:** Exploits TCP handshakes by flooding SYN requests.
- **ACK Flood:** Sends a TCP ACK flood to overwhelm the destination.
- **Smurf Attack:** Floods target with ICMP queries from a fake source.
- **Ping of Death:** Sends large or faulty packets to crash target system.
- **Fragmentation Attacks:** Sends fragmented packets to exhaust target resources (e.g., IP/UDP fragmentation).

1.5.1.3 Attacks at the Application Layer

By taking advantage of holes in the application layer, these attacks target certain services or apps. It come in four varieties,

- **HTTP GET/POST Flood:** Overwhelms web servers with GET or POST requests, exhausting server resources and causing service disruption.
- **Slowloris:** Holds as many connections as feasible are kept open to the destination web server.
- **DNS Query Flood:** overloads DNS by sending the victim a barrage of DNS requests servers.
- **SSL-Based Attacks:** Exploits the SSL handshake process to exhaust server resources (e.g., SSL Renegotiation).

1.5.2 DDoS Attack Vector Classification

DDoS attacks are further categorized according to the kind of assault into two types, shown in Figure 1.4.

1. Flooding attacks
    a. Single Vector DDoS Flooding attacks
    b. Multi Vector DDoS Flooding attacks
2. Multiple DDoS attacks

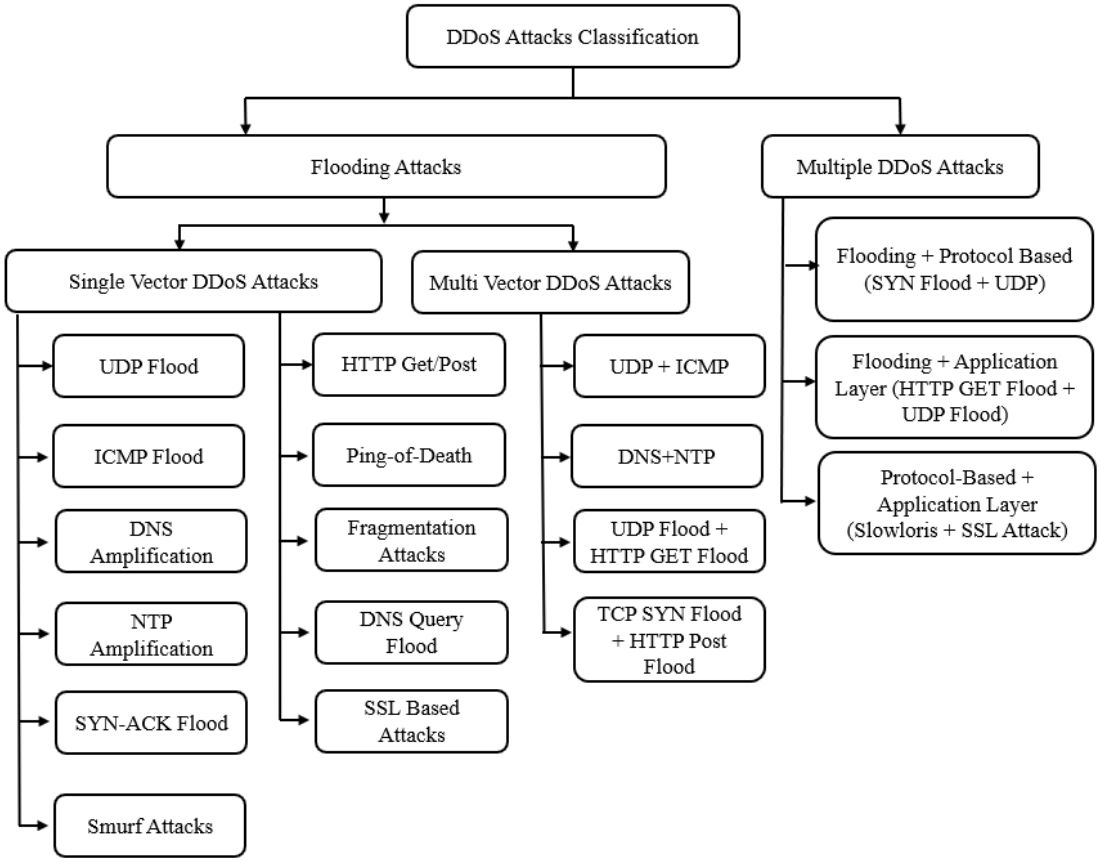

Figure 1.4: DDoS attack vector classification

Flooding Attacks:

- Single Vector DDoS Flooding Attacks: These attacks use one method to overpower a target.
- Multi Vector DDoS Flooding: These assaults overload a victim by combining many techniques.

Multi DDoS Attacks:

- Combine different attack types for greater impact.

1.5.2.1 Single Vector DDoS Flooding attack

A Single Vector DDoS Flooding Attack involves using one type of attack vector to overwhelm the target system. They are specific resource targeting attacks typically targeting one specific resource characteristics the target, such the CPU, RAM, bandwidth, or a particular protocol as depicted in Figure 1.5.

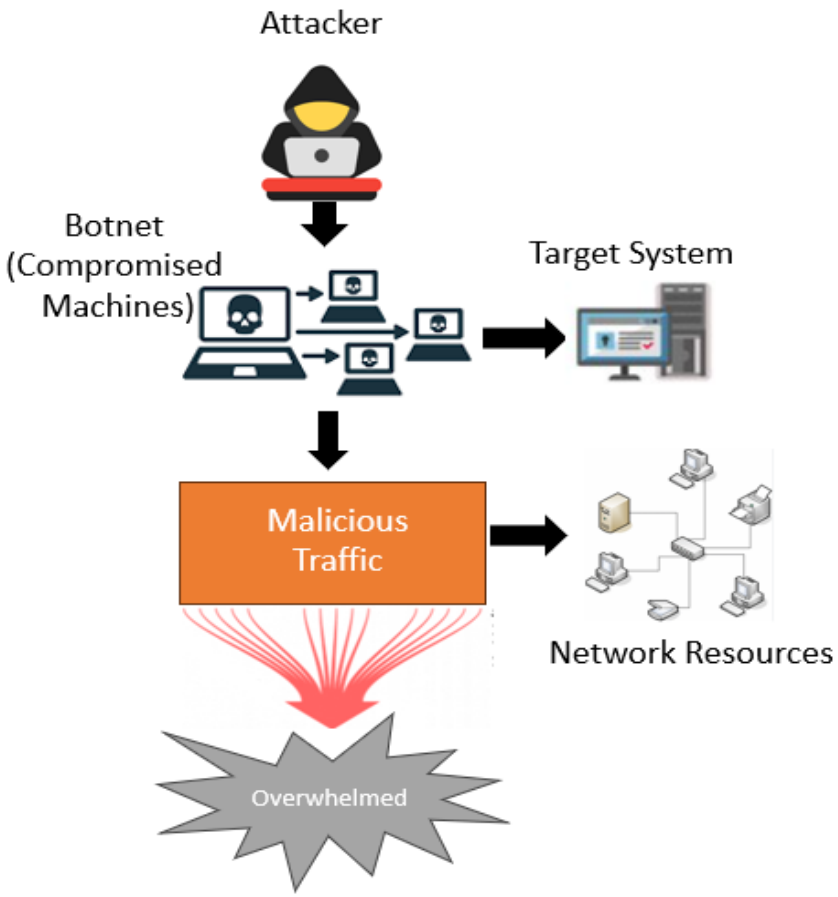

Figure 1.5 Single vector DDoS Flooding attack scenario

1.5.2.2. Multi Vector DDoS Flooding Attacks

A multi-vector DDoS Flooding Attack employs multiple attack vectors simultaneously or in succession to overwhelm the target system. Broad Resource Targeting, targeting multiple resources and layers of the target's infrastructure, making it harder to defend against. Figure 1.6. shows the scenario.

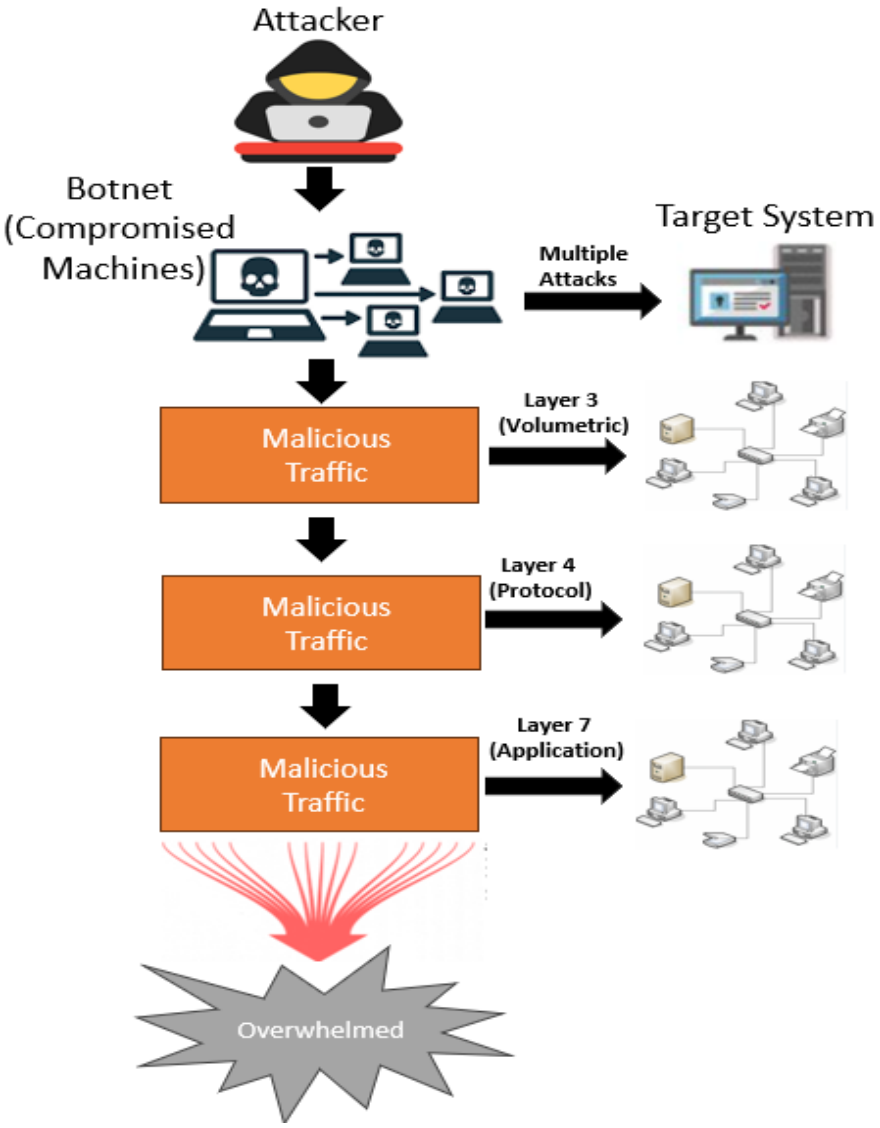

Figure 1.6 Multi vector DDoS Flooding attack scenario

1.6 Methods to handle Cyber Attacks

Handling cyberattacks requires a proactive and multifaceted approach to safeguard data and services (John, J. and Norman, J., 2019) (Kadri, M.R et al, 2023) (Ahmetoglu, H. and Das, R., 2022) Figure 1.7 shows different methods and best practices to mitigate and respond to cyberattacks.

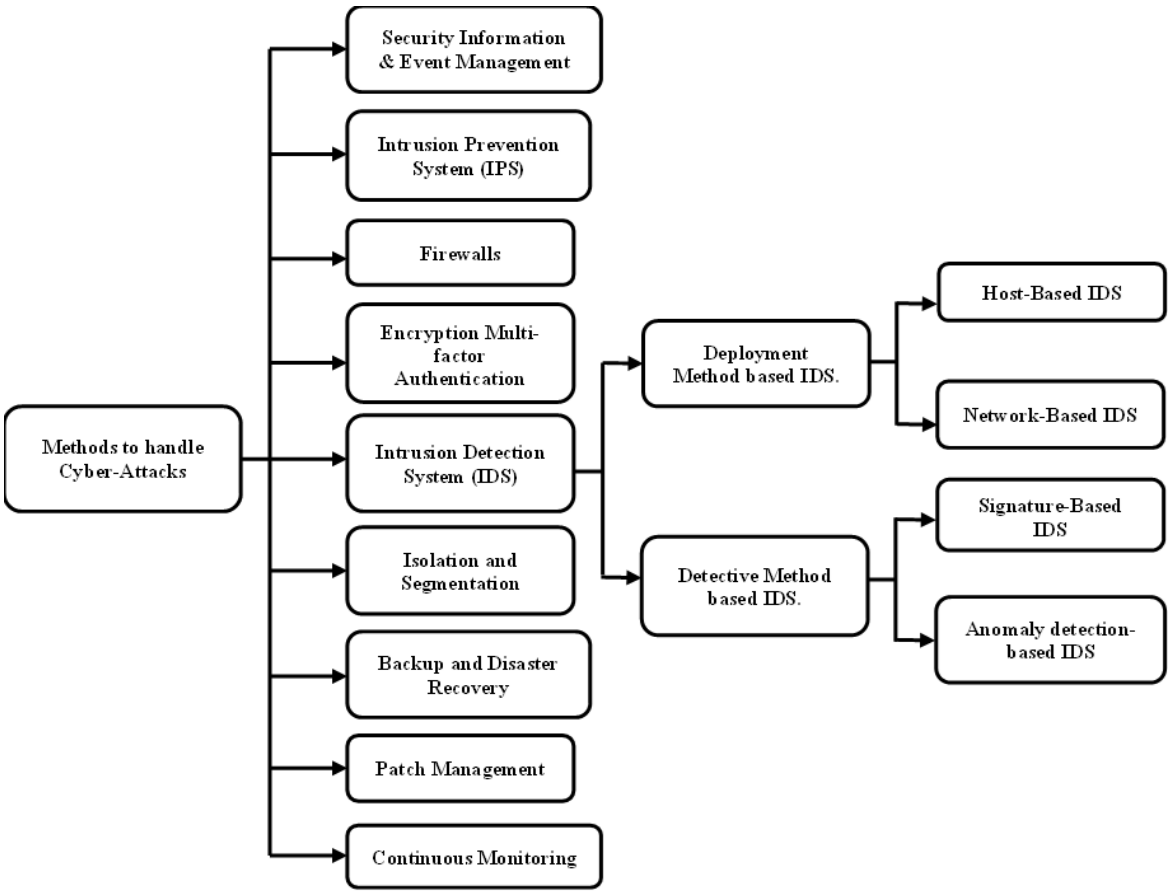

Figure 1.7 Methods to handle Cyber-Attacks

For the purpose of managing cyberattacks, IDS implementation is essential. Maintaining security and integrity requires being able to quickly identify and address threats, which IDS can do by monitoring network traffic and detecting malicious or suspicious activity in real-time.

1.6.1 Intrusion Detection System (IDS)

The intensity and features of cyberattacks described in the preceding sections make it abundantly evident that hackers are very skilled at seriously harming network resources without the victim's awareness. The customer should get continuous, high-quality service by implementing the proper cyber security measures. Many detection as well as mitigation approaches have been established over the past few decades as these are important study fields to take into consideration. This section covers a few of the conventional approaches. The two primary categories of IDS systems are anomaly and signature-based IDS (Li, Qg, et al., 2023) (Salman Iqbal et al., 2016) (Bharati, M. and Tamane, S., 2017) (Hussain, Y.S., 2020) (Khraisat, A., 2019).

1.6.1.1 Signature-based IDS (SIDS)

The SIDS utilize a knowledge-based approach, mapping intrusion signatures with stored instances in a database. Intrusions are identified through if-then rules, triggering alarms when current activity matches historical signatures. Despite SIDS' reported accuracy, when there are no database references, it has trouble with zero-day attacks. SIDS searches for pre-established patterns or indicators of recognized online dangers. It can successfully detect previously known malware and intrusion attempts, but it can fail to detect new ones. It was also pointed out that SIDS strongly depends on the up-to-date signature databases. It needs other supplementary methods to cope with new, complex threats.

1.6.1.2 Anomaly-based IDS (AIDS)

The AIDS is that differentiates between invasive and regular computer system activity using knowledge-driven, statistical and machine-learning methods (Jyothsna, V.V.R.P.V., Prasad, R. and Prasad, K.M., 2011). Initially, trained with a dataset of normal traffic profiles and then tested with known data to check its capability to predict unknown intrusions. This approach is emerging in research for solving the drawbacks of Signature based Intrusion Detection Systems (SIDS). Above all, AIDS provides a predictive model of security based on machine learning and statistical analysis, which aimed at making preventive detection of potential threats and cyber threats.

1.6.1.3 Deployment Based IDS

IDS deployment may be done in two primary ways: the network deployment and the host deployment. NIDS are located at critical stages in the network to splutter traffic while HIDS are resident on individual hosts to scan for local activity and signs of an attack.

1.6.1.4 IDS based on hosts

A HIDS is installed on computer servers in a cloud to watch for host internal activities including file modification and system journal (Liu, M et al., 2018) (Satilmiş, H., Akleylek, S. and Tok, Z.Y., 2024). Operating based on predefined rules and employing the anomaly detection means, HIDS identifies signs of violation of security or presence of malware. It creates finer level visibility into the host security, helps in threat identification, and responds quickly to security threats, making it more valuable to prevent both She & Internal threats, and advanced persistent threats. HIDS improves security by identifying

threats that are unique to cloud instances and shields applications, data, and services from cyber threat.

1.6.1.5 IDS based on networks

The purpose of NIDS is to monitor network traffic and flag questionable activities (Ring, M et al., 2019). Located inside a network, it looks at the incoming and outgoing traffic for familiar attack patterns, viruses, DoS attacks, and unauthorized attempts to gain access. NIDS provides real-time alerts and continuous monitoring, enabling proactive defense, vulnerability detection, and response to security breaches. It offers real-time alerts, enhancing security and availability by safeguarding applications and data from network-based risks.

1.6.2 Hybrid Deep Learning Detection Method

Deep Learning (DL) a sub-class of Artificial Intelligence methodology, has revolutionized almost every industry providing solutions for endless applications. Undoubtedly, Deep learning provides an advanced form of threat protection in cybersecurity with accurate prediction and detection. Deep learning is based on brain learning capacity. Once a brain can recognize a thing, it becomes second nature to do so. Deep learning uses NN, CNN, RNN (Karatas G, and Sahingoz O.K, 2018) (Ferhi, W et al, 2023) to detect cyber threats based on the patterns, and their prediction capabilities become natural. This prevents and predicts any cyber threat, known or unknown or new before it can be successfully executed at zero time. It acts as proactive approach in real-time. It is a simple explanation with accurate predictions and effective with less computation time. Based on the study of the relevant literature it is noted that the Computational Intelligence methods bring accurate results for all kinds of complex problems. There is a scope for improving the existing Computational Intelligent methods for better performance.

1.7 Motivation and Justification

The increasing significant events from 2016 to 2023 demonstrate the frequency and intensity of DDoS assaults, underscoring the pressing need for better detection and mitigation techniques. From the severe disturbances of the Dyn attack in 2016 to the record-breaking 71 million requests per second attack on Cloudflare in 2023, these events underscore the escalating threat posed by DDoS attacks.

Table 1.1 Year-wise overview of Major DDoS attacks

Year	Attack	Details	Peak Traffic
2016	Dyn Attack	Disrupted major websites like Twitter, Netflix, and Reddit.	Not specified
2017	Google Attack	Record-breaking attack over six months.	2.54 Tbps
2018	GitHub Attack	Used Memcached servers to amplify traffic.	1.35 Tbps
2019	AWS Attack	Set a new record for the largest DDoS attack at the time.	2.3 Tbps
2020	New Zealand Stock Exchange	Disrupted trading for several days.	Not specified
2021	Yandex Attack	Largest in history at the time, attributed to the Meris botnet.	21.8 million RPS
2022	Microsoft Azure Attack	Mitigated massive attack on cloud services.	3.47 Tbps
2023	Cloudflare Attack	Largest HTTP DDoS attack observed.	71 million RPS
2024	Cloud Strike Attack	Highly sophisticated, targeting critical infrastructure globally	4.5 Tbps

Table 1.1 shows the year-wise overview of major DDoS attacks that highlight the growing threat and evolving nature of these cyberattacks (Tandon, R., 2020). This research is inspired by the need to come up with new approaches that can detect and prevent such assaults to prevent disruption of crucial online services and support systems that are vulnerable to modern day cyber threats.

According to Radware's 2024 Global Threat Analysis Report, (https://www.radware.com/threat-analysis-report/) DDoS attacks are changing, as hackers modify their tactics to thwart expanding mitigating methods. The amount of DDoS assaults per customer increased by 94% in 2023 over 2022, which was on top of the 99% increase in

2022. Since the first quarterly of the year 2021, the average monthly attack rate per subscriber has been 106 attacks, or 3.48 assaults per day. An average Radware client had to defend against 49 assaults per day in the first quarter of 2023. As shown in Figure 1.8, the attack volume per customer rose by 48% in 2023 over 2022. Assaults with traffic below 1 Gbps increased by 63% in 2023, while assaults peaking between 100 and 250 Gbps increased by 177%, and massive attacks peaking above 500 Gbps increased by 150%. In 2023, about half of all DDoS assaults worldwide were directed against the United States. The EMEA area had to combat 65% of the worldwide DDoS attack volume, which accounted for 39% of the assaults. Nearly 12% of all DDoS assaults worldwide were concentrated in the APAC region.

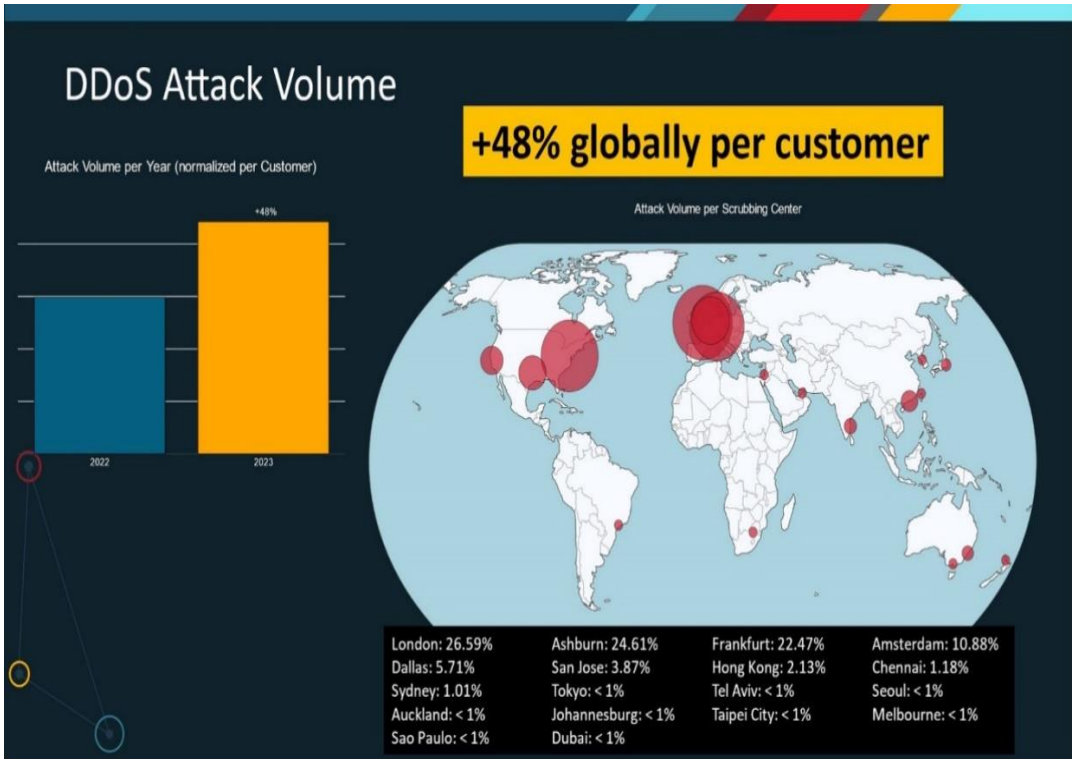

Figure 1.8 Increased Organizational DDoS Attacks in 2023

Courtesy: Radware

Based on the Akami statistical reports shown in Figure 1.9, the banking and in 2023, the financial services sector had the most number of DDoS assaults. (https://www.akamai.com/blog/security/a-retrospective-on-ddos-trends-in-2023), a dubious distinction reflecting its growing vulnerability. Since 2021, financial institutions have faced

an escalating threat from DDoS attacks. Previously, around 10% of DDoS attacks targeted this sector. This figure surged to approximately 20% in 2021 and 2022, and peaked at around 35% in 2023, indicating a significant increase in the focus on financial services by cyber attackers.

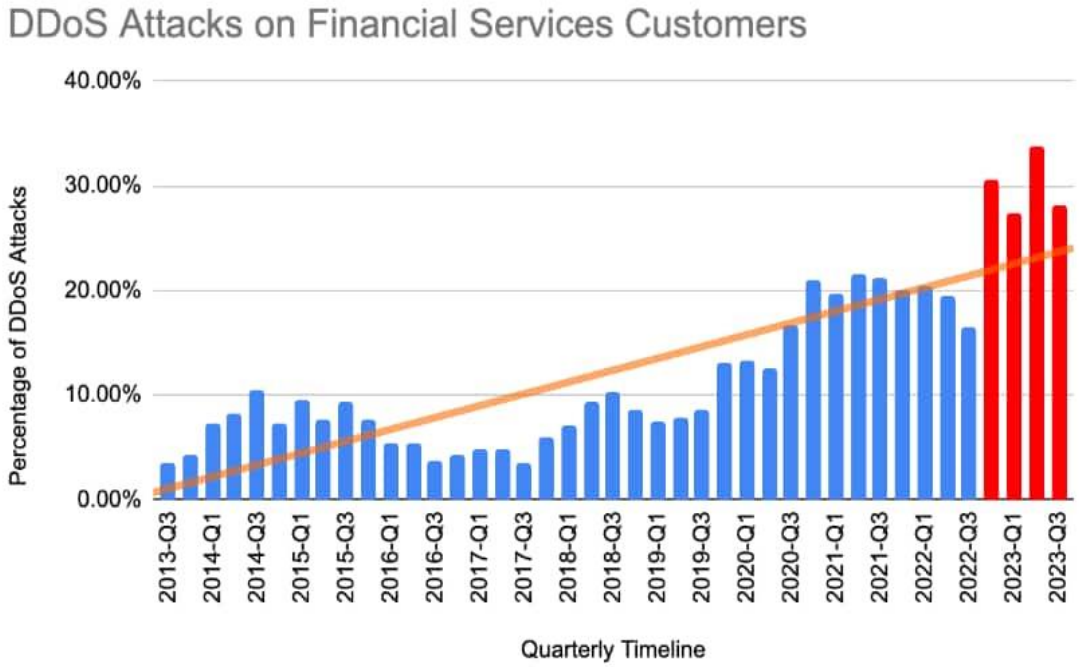

Figure 1.9 Prevalence of DDoS Attacks Targeting the Financial Sector in 2023

Courtesy: Akami

It is essential to choose dependable security measures today because the number of online services is rapidly increasing. Traditional Intrusion Detection Systems (IDS) often fall short because they are based on signatures. Advanced IDS based on machine learning and AI approaches evaluate data in real-time, recognize threats and take proactive measures in response to new threats with regard to the given security threats. These systems are important for the defense of the data, the applications, and the infrastructure from complex threat such as the DDoS attacks (Hamarshe, A., Ashqar, H.I. and Hamarsheh, M., 2023). Security of networks is still an issue of significant importance with the ever-changing technology and networks. This research fulfills the existing void of an intelligent IDS that is designed to identify and respond to DDoS assaults. Through the application of DL algorithms, this study aims to improve attack detection efficiency and develop strategies for preventing DDoS assaults to strengthen security of networked systems.

1.8 Problem Statement

To develop a complexity aware intelligent intrusion detection system for DDoS attacks with emphasis on single vector and multi vector flooding attacks and different types of DDoS attacks.

1.9 Research Questions

Given the current landscape, existing approaches and the statistics provided by reports prompt the following research questions when examining security challenges involving DDOS attacks.

RQ1: Is it possible to develop a system that can identify both single and multi vector DDoS Flooding attacks with reduced detection time and higher accuracy.

RQ2: Can ML and Computational Intelligence techniques be effectively leveraged to enhance the detection of DDoS attacks with reduced computational complexity?

RQ3: How to devise a complexity-aware detection solution for efficiently identifying DDoS assaults in a variety of datasets?

1.10 Objectives of Thesis

The goals are formed after the study of literature to overcome the limitations of the existing architectures. The foremost objective of the research work is to devise a complexity aware intelligent intrusion detection mechanism for detecting DDoS attacks with enhanced feature engineering. Based on the above discussions, the secondary goals of the research are formulated as follows.

(i) To accurately detect single-vector DDoS flooding attacks with improved detection accuracy and minimized computational time.

(ii) To detect multi-vector DDoS flooding attacks with a low false alarm rate and excellent performance.

(iii) To accurately detect multiple DDOS assaults that are scalable, have low false alarm rates, and execute well.

(iv) To precisely identify DDOS assaults that exists in various datasets using reduced computational complexity and enhanced performance.

1.11 Significant Thesis Contributions

To fulfill the objectives of the thesis a framework is proposed which is explained in four phases. Each phase is achieved as a significant contribution and explained below.

Contribution 1: Detecting Single Vector DDoS Flooding attack using ensemble-based combination filter for decision tree classification and feature selection.

Contribution 2: Detecting Multi Vector DDoS Flooding attacks using Improved Dragonfly Optimization and Decision Tree Classifier

Contribution 3: Multiple DDoS attack Intrusion Detection Model for detecting multiple attacks Panthera Leo Optimized Multilayer Feed Forward Learning

Contribution 4: Intrusion Detection Model for DDoS Attacks in multiple datasets using AEGRN and Deep Learning

Contribution 1: Identification of Single Vector DDOS Flooding attack using feature selection and decision tree classifier using an ensemble-based combination filter.

This thesis's initial contribution is a feature selection technique intended for DDoS cyberattack identification. The primary goal is to identify individual DDoS flooding assaults. To improve DDoS attack detection, an integrated filter for feature selection that resolves competing goals is proposed and implemented. This will help choose the best features from the datasets. To get beyond the restrictions and difficulties of DDoS traffic patterns and increase detection accuracy, a novel DT classification technique is put forward. Additionally, the approach allows users to choose the best feature set with various performance attributes and takes into account finding feature subsets as a Pareto-front. The effectiveness of the suggested approaches is extensively assessed using the most recent CICDoS2019 dataset and standard performance indicators. To facilitate the improvement in the detection of individual DDoS flooding assaults, this innovation combines an ensemble-based combination filter with enhanced machine learning (ML) strategies. The outcome of the CFFS-DT module excels in detecting single-vector DDoS attacks with 97.69% accuracy, over 98% precision and recall, and minimized computational time of 1.2 units.

Contribution 2: Detecting Multi-Vector DDOS Flooding attacks using Improved Dragonfly Optimization and Decision Tree Classifier

This thesis's second contribution is the suggestion of a machine learning and bio-inspired optimization technique for the identification and categorization of DDoS flooding assaults. The primary goal is to identify numerous DDoS flooding assaults. To improve DDoS attack detection, the Improved Dragonfly Optimization method is suggested in combination with DT techniques. Comparing several ML models to watch which one performs best using common performance indicators is another aspect of this work. Using the CICDDoS2019 dataset and standard performance metrics, a thorough assessment of the suggested model is conducted. To find out how well the suggested algorithm detects DDoS flooding assaults, its performance is contrasted with other ML strategies. The IDOA-DT hybrid technique produced impressive results, with recall scores close to 98% and accuracy of 98.89% with precision, alongside an efficient execution time of 0.69 units, validated through 10-fold cross-validation for robust and reliable performance.

Contribution 3: Multiple DDOS attacks Intrusion Detection Model using Panthera Leo Optimized Multilayer Feed Forward Learning

Designing an IDS that uses Panthera Leo Optimized Multilayer Feed Forward Learning to identify numerous DDoS attempts is the third contribution of this thesis. Identifying several DDoS assaults using PLO in conjunction with a multilayer feedforward network is the primary goal. On a high-performance computer, the suggested IDS is extensively evaluated using a number of common evaluation criteria to gauge its effectiveness. Additionally, the potency of the recommended method is tested with regard to identify DDoS assaults in comparison to other algorithms already in use. As a consequence of the proposed PLO-MLFFN framework is highly effective in identifying multiple DDoS attacks with an accuracy of 96.8% and 96.89% F1-score and the minimum detection time of 7.6 units with different training-test ratios. Its scalability and low false alarm rates are better than those of SVM, CART, and BAT-ELM algorithms.

Contribution 4: Detecting DDoS Attacks using ML and DL on multiple datasets through proposed Attention Enabled Gated Recurrent Network (AEGRN) model

Presenting an intrusion detection system to find DDoS attack is the fourth contribution of this thesis with multiple datasets using AEGRN and deep learning. The main

goal is to identify DDoS attacks on various dataset that uses AEGRN for attack detection and comprehensive assessments Regarding NSL-KDD-99, UNSW-2019, and the proposed design CICDDoS2019 datasets using performance metrics. The proposed IDS is implemented on a high-performance computer and its efficiency is measured using different assessment parameters. The experiments also indicate that the recommended model outperforms other models based on DL that provide the highest prediction accuracy and the lowest computational complexity. The proposed AEGRU-DFFN model combining self-attention maps with GRU has shown accuracy greater than 98% with error rates of approximately 1% and small prediction errors (RMSE: 0.001). It outperforms other IDS models in detection efficiency, reduced complexity, and faster processing times.

1.12 Organization of Thesis

This thesis is presented in nine chapters and structured as follows:

Chapter 1: This chapter presents security challenges, different types of attacks, and their classification specific to DDoS attacks. Following a thorough explanation of the thesis's history and inspiration, the four primary contributions are examined, and finally, the thesis' structure is explained.

Chapter 2: This chapter provides an extensive review of the relevant literature to the thesis, addressing the problem statement and existing approaches to counter various cyber-attacks, with a specific focus on DDoS attacks and their numerous types. It delves into IDS and examines their application across different network environments, highlighting the databases that are often used for intrusion detection and the methods employed for feature selection to enhance detection accuracy. The chapter also explores computational intelligence techniques, including deep learning, as effective tools for identifying cyber-attacks. Alongside these, it analyzes the strengths and limitations of current approaches, discusses key findings from recent research, and identifies open challenges and gaps in DDoS detection strategies

Chapter 3: This chapter describes the research framework based on the four-step methodology. This chapter discusses the four different contributions proposed to address the stated problem.

Chapter 4: This chapter presents the framework for detecting Single-vector DDoS flooding attacks using Combined Filter for Feature Selection method and ML. Experiments are conducted, and the results are obtained and compared.

Chapter 5: In this chapter, a strategic-level framework is proposed for identifying multi-vector DDoS flooding attacks that incorporates bio-inspired optimization techniques, ML and feature engineering procedures. Additionally, the suggested models are contrasted with other ML techniques.

Chapter 6: An intrusion detection model using a multi-layer feedforward network ensembled using PLO is presented in this chapter for detecting multiple DDoS attacks. Experiments are conducted, and the results are obtained and compared.

Chapter 7: This chapter presents Intrusion detection model that is integrated with Self-attention maps with GRU and Deep Feed Forward network for securing against the multiple DDOS attacks in multiple datasets. Experiments are conducted and the results are compared.

Chapter 8: This chapter presents Statistical validation of the proposed model and their performance comparison in detection of DDoS attack. Experiments are conducted, the outcomes of which are gathered and contrasted.

Chapter 9: This provides the summary, conclusion and suggested future directions of the research work.

1.13 Chapter Summary

Chapter 1 offers a thorough overview of the foundational research undertaken in this thesis, clearly explaining the problem statement, and outlining the topics to be elaborated on in subsequent chapters. This chapter details the objectives of the proposed complexity aware intelligent IDS, emphasizing the rise DDoS attacks are a serious and growing danger to the security and stability of digital infrastructures worldwide. It highlights the necessity for sophisticated methods to accurately identify malicious activity amidst vast amounts of network traffic. This also discusses the importance of complexity aware intelligent detection system with enhanced feature engineering to enhance the system's performance. The next chapters further cover the goals of the research project and the thesis's contribution.

Building on this framework, the next chapter provides an extensive assessment of published work on DDoS detection, intrusion detection systems, datasets, feature selection methods, and computational intelligence techniques, along with an analysis of unresolved issues in the field.