AN ENHANCED MECHANISM TO DETECT DRDOS ATTACKS ON DNS USING ADAPTIVE THRESHOLDING TECHNIQUE

RIYADH RAHEF NUIAA AL OGAILI

UNIVERSITI SAINS MALAYSIA

2023

AN ENHANCED MECHANISM TO DETECT DRDOS ATTACKS ON DNS USING ADAPTIVE THRESHOLDING TECHNIQUE

by

RIYADH RAHEF NUIAA AL OGAILI

Thesis submitted in fulfilment of the requirements
for the degree of
Doctor of Philosophy

March 2023

DEDICATION

To my appreciated father "Rahef Nuiaa Al-Ogaili"

To my dearest mother "Ashaifa Guniah Al-Ogaili"

To my beloved wife "Zeinab Ali Dashoor"

To my lovely kids "Ali and Jaafar"

To my dearest Family

ACKNOWLEDGEMENT

With the name of Allah, Most Gracious, Most Merciful.

All praise and thanks are due to ALLAH SUBHANH WA TAALA, the Lord of the world, for giving me the health, strength, knowledge and patience to complete my PhD. Now, I would like to express my deep gratitude to my main supervisor associate professor DR. Selvakumar Manickam and TS. DR. Shankar A/L Karuppayah for all their support, patience and guidance during this research. They have widened my horizon in conducting the research. Their contributions were invaluable, extraordinary and their way of directing a student was unique during the entire period of my PhD at National Advanced IPv6 Centre of Excellence (NAv6), which is a high-profile organization. I also wish to thank my research committee members for providing insightful and constructive comments. I would like to express my gratitude and thanks to all NAv6 centre members my colleagues, technicians, and administrative staff. Most importantly, I thank my parents, Rahef and Ashaifa, for their faith in me and for allowing me to be as ambitious as I wished. It was under their watchful eye that I gained the drive and ability to tackle challenges head-on

Most importantly, I would like to thank my wife Zeinab. Her support, encouragement, patience, and unwavering love were undeniably the foundation upon which the past eleven years of my life have been built. Her tolerance of my occasional discourteous moods is a testament to her unyielding devotion and love. Last but not the least, I wish to dedicate this work to my kids Ali and Jaafar.

TABLE OF CONTENTS

LIST OF TABLES

Page

LIST OF FIGURES

Page

LIST OF SYMBOLS

=	Equal to
-	Subtraction
+	Addition
×	Multiplication
–	Division
√	Square Root
∑	Summation
≠	Not Equal To
{	Left curly bracket
θ	Theta
Δ	Increment
^	Power
>	Greater Than
ϵ	Belong to
β	Beta
<	Less Than
≤	Less Than or Equal to
| |	Absolute value

LIST OF ABBREVIATIONS

AT	adaptive threshold
BA	Bat algorithm
C&C	command and control
CIC	Canadian Institute for Cybersecurity
CMR	Crystal Market Research
CPU	Central Processing Unit
CRM	Customer relationship management
DA	detection accuracy
DDoS	distributed denial-of-service attacks
DE	Differential Evolution algorithm
DNS	Domain Name System
DoS	denial-of-service attacks
DRDoS	Distributed Reflection Denial of Service attack
EDFC	Evolving Dynamic Fuzzy clustering
EDNS	extension mechanisms for DNS
EDoS	Economic Denial of Sustainability
EMDDMAT	enhanced mechanism to detect DRDoS attacks on DNS using modified metaheuristic algorithms and adaptive thresholding techniques based on machine learning algorithms
FFA	firefly optimization
FP	False Positive
GA	genetic algorithm
GWO	grey wolf optimizer
ICMP	Internet Control Message Protocol
IP	Internet Protocol

KNN	K Nearest Neighbor
MA	metaheuristic algorithm
MMA	modified metaheuristic algorithms
NoC	number of clusters
NTP	Network Time Protocol
NXDOMAIN	Non-Existent Domain
PFS	Proactive feature selection
PRSD	Pseudo-random subdomain attack
PSO	particle swarm optimization
Q1	The First Quarter
Q2	The Second Quarter
Q3	The Third Quarter
Q4	The Fourth Quarter
RF	Random Forest
RRL	Response Rate Limiting
SC	Silhouette Coefficient
SDN	Software-defined networking
SLD	second-level domain
SVM	Support Vector Machine
SWEVO	Swarm Optimization and Evolutionary Algorithms
TCP	Transmission Control Protocol
TTL	Time to Live
UDP	User Datagram Protocol
WWW	World Wide Web

LIST OF APPENDICES

MEKANISME YANG DIPERTINGKATKAN UNTUK MENGESAN SERANGAN DRDOS PADA DNS MENGGUNAKAN TEKNIK AMBANG ADAPTIF

ABSTRAK

Permintaan untuk perkhidmatan yang didayakan ruang siber telah berkembang secara mendadak dalam beberapa tahun kebelakangan ini, seiring dengan perkembangan populasi pengguna Internet global. Permintaan yang meningkat untuk perkhidmatan ini telah meningkatkan bilangan ancaman siber yang dilancarkan oleh penyerang, serta kepelbagaian dan kecanggihan strategi serangan yang digunakan untuk menyasarkan perkhidmatan tersebut. Dengan mengeksploitasi kelemahan DNS, penyerang siber melakukan serangan Penafian Perkhidmatan Refleksi Teragih (DRDoS). Hasilnya, jenis serangan ini mengeksploitasi kaedah, kefungsian dan pengendalian penyelesai DNS terbuka untuk menjejaskan DNS. Selain itu, untuk memperhebatkan serangan dengan meningkatkan jalur lebar serangan untuk mengatasi mangsa dengan sejumlah besar jawapan DNS. Hasilnya, mekanisme tradisional tidak dapat mengesan jenis serangan siber ini. Maka, mekanisme pengesanan sedia ada tidak dapat mengesan bentuk pencerobohan siber ini. Justeru, tesis ini membentangkan mekanisme untuk mengesan serangan DRDoS ke atas DNS yang diperkukuh dengan penggunaan algoritma metaheuristik yang diubah suai dan teknik ambang adaptif berdasarkan algoritma pembelajaran mesin (EMDDMAT). Mekanisme EMDDMAT dibina daripada dua model: pemilihan ciri proaktif (PFS) dan Pengelompokan Fuzzy Dinamik Berkembang (EDFC). Mekanisme EMDDMAT terdiri daripada tiga peringkat: (1) pra-pemprosesan data; (2) Pemilihan ciri DNS berdasarkan model PFS

(peringkat pemilihan ciri); dan (3) pengesanan serangan DNS DRDoS berdasarkan model PFS (peringkat pengesanan). Akhir sekali, menggunakan model EDFC, meningkatkan hasil peringkat sebelumnya. Berdasarkan set data penanda aras CICDDoS2019 (DRDoS DNS), mekanisme EMDDMAT yang dicadangkan dinilai. Sasaran utama tesis adalah untuk mencapai ketepatan pengesanan maksimum 95.44% dan kadar positif palsu terendah sebanyak 0.22% apabila mengesan serangan DNS DRDoS. Selain itu, keberkesanan mekanisme yang dicadangkan dinilai dengan perbandingan dengan teknik berasaskan DNS yang terkenal. Pendekatan yang dicadangkan mengatasi alternatif sebelumnya, seperti yang dinyatakan oleh keputusan.

AN ENHANCED MECHANISM TO DETECT DRDOS ATTACKS ON DNS USING ADAPTIVE THRESHOLDING TECHNIQUE

ABSTRACT

Demand for cyberspace-enabled services has expanded dramatically in recent years, in lockstep with the global Internet user population expansion. This rising demand for these services has increased the number of cyber threats launched by attackers, as well as the diversity and sophistication of the attack strategies used to target those services. By exploiting DNS flaws, cyber attackers conduct a Distributed Reflection Denial of Service (DRDoS) attack. As a result, these types of attacks exploit the method, functionality, and operation of open DNS resolvers to compromise the DNS. Additionally, to intensify the attack by boosting the attack bandwidth to overwhelm the victim with a vast number of DNS answers. As a result, traditional mechanisms are incapable of detecting these types of cyberattacks. As a result, existing detection mechanisms are unable to detect these forms of cyber intrusions. Thus, this thesis presents a mechanism for detecting DRDoS attacks on DNS that is strengthened by the use of modified metaheuristic algorithms and adaptive thresholding techniques based on machine learning algorithms (EMDDMAT). The mechanism of EMDDMAT is built of two models: proactive feature selection (PFS) and Evolving Dynamic Fuzzy Clustering (EDFC). The EMDDMAT mechanism comprises three stages: (1) data pre-processing; (2) DNS feature selection based on the PFS model (feature selection stage); and (3) detection of DNS-based DRDoS attacks depending on the EDFC model (detection stage). Based on the CICDDoS2019 (DRDoS DNS) benchmark datasets, the suggested EMDDMAT mechanism is evaluated. The thesis's primary target is to

achieve the maximum detection accuracy of 95.44% and the lowest false positive rate of 0.22% when detecting DRDoS DNS attacks. Additionally, the suggested mechanism's effectiveness is evaluated by comparison to well-known DNS-based techniques. The proposed approach outperforms previous alternatives, as demonstrated by the results.

CHAPTER 1

INTRODUCTION

1.1 Introduction

The rapid growth of Internet use during the last decade attests to the Internet's expanding social significance. As seen in Figure 1.1, this increase demonstrates the Internet's utility as a research tool and as a critical component of a global society's infrastructure. This increase can be attributed to changes in traditional responsibilities associated with conducting business via the Internet, which allows for the electronic handling of all transactions. Additionally, the government makes use of the Internet to communicate with its citizens and the rest of the world, as well as to provide government services. Universities and research institutions rely on the Internet for collaboration to advance scientific discoveries. Taking past years into account, particularly 1995, when the world population began to use the Internet for the first time, and evaluating the growth curve through 2021 (*Internet Growth Statistics 1995 to 2021 - the Global Village Online*, 2021).

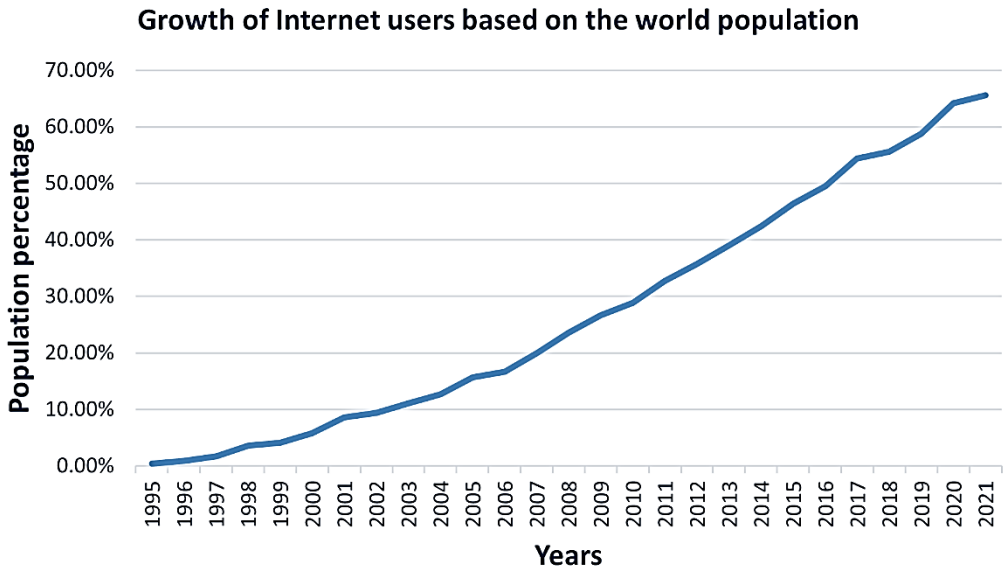

Figure 1.1: Growth of Internet users.

As stated by Shears (2017) the Internet economy will undergo substantial changes during the next decade as a result of technology and business model developments. Furthermore, the capability for sharing has resulted in the open development of critical Internet components such as the Domain Name System (DNS), and the World Wide Web (www). This capability is contingent upon the principle of fair use and the right to create and use open-source software. Thus, the security and confidence of the consumer will be critical. Our coordinated response to the volume and extent of attacks will decide the Internet's continued expansion. Besides, the figure below illustrates the Internet's growth from 1995 to 2021, based on the world's population. In 1995, only 0.4% of the world's population used the Internet; by 2021, that figure had risen to 65.60% (*Internet Growth Statistics 1995 to 2021 - the Global Village Online*, 2021).

Jang-Jaccard and Nepal (2014) emphasized that the rapid expansion of Internet connectivity has frequently resulted in a major increase in cyberattacks with catastrophic and severe repercussions. According to Meeker (2019) a 2019 Internet trends analysis, Internet penetration was 24% in 2009 but increased to 51% in 2018. As well, the increased use of the Internet will result in increased security issues; therefore, to address this issue, we must set certain rules, defining Internet security as the process of establishing rules and procedures to be done to protect against Internet threats.

Then, the importance of boosting cybersecurity and network security grows constantly as threats evolve at a breakneck pace. Cyberattacks and criminal activity will reshape the Internet and our interaction with it. Inadequate risk management endangers users, erodes public faith in the Internet, and jeopardizes the Internet's capacity to foster economic and social growth. Attacks are getting increasingly

sophisticated, and many fear that catastrophic cyberattacks are a certain conclusion in the future (Shears, 2017). Hence, Figure 1.2 shows the Internet security issues types but cannot be limited to specific attacks, but we can review the common and important types (Juta Gurinaviciute, 2021; University of North Dakota's, 2021).

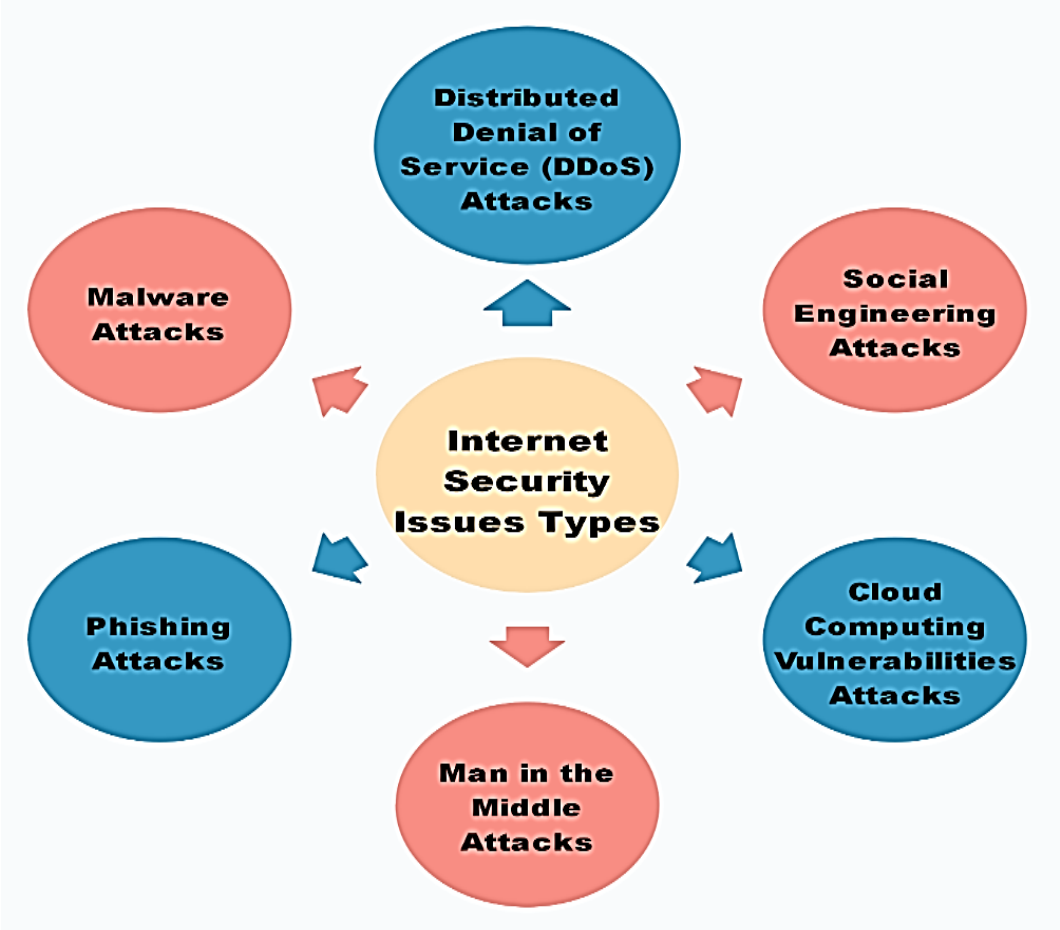

Figure 1.2: The common types of Internet security issues.

1.2 Background of Study

As discussed in section 1.2.3, these attacks continue to threaten the Internet's existing status. As a result, according to Nexusguard reports attacks for the year of 2019 reports, these attacks were spread across the four quarters of 2019, i.e., from Q1 to Q4. The case study involves DNS amplification/reflection. This section discusses DRDoS attacks, DNS, and ways for detecting DRDoS attacks using DNS.

1.2.1 DDoS Attacks

Different firms, including Cloudflare, Kaspersky, Imperva, and Cisco, define distributed denial-of-service (DDoS) attacks as an attempt by a malicious party to flood a service, targeted server, or network with Internet traffic to disrupt normal traffic. DDoS attacks pose a significant threat to company continuity. As businesses have become more reliant on the Internet and web-based applications and services, accessibility has become as vital as power. As a result, DDoS is a threat to all businesses, not just those reliant on uptime in the retail, financial, and gaming industries. In addition, DDoS attacks target mission-critical business technology, including email, salesforce automation, and customer relationship management (CRM), on which your organization depends to conduct daily operations. Other industries, such as manufacturing, pharmaceuticals, and healthcare, also have internal web domains that are used to conduct daily business activities by the supply chain and other business partners. All of these are targets for today's highly competent cyber assailants.

David Dennis may have launched the first-ever distributed denial-of-service attack. He built a program in 1974 that sent a difficult order to 31 PLATO terminals and shut them down. No malice was intended, as this was an experiment. Although this principle was initially intended to be beneficial, it would quickly become exploited (Dayanandam et al., 2019; Rick Davis, 2021). The following Figure 1.3 displays the largest DDoS attacks based on attack volume over the last few years (CloudFlare, 2020; Nicholson, 2021). There are numerous sorts of DDoS attacks; some are protocol-based, while others are volume-based.

Masdari and Jalali (2016) observed that the distributed reflective denial-of-service (DRDoS) attack employs attacker-controlled zombies to overwhelm the reflector node with request packets, effectively shutting down the target. The attackers can employ botnets to conduct more sophisticated reflection attacks undetected. Attackers use DDoS attacks to take advantage of protocols such as TCP, UDP, DNS, and ICMP. Smurf is a well-known DRDoS attack.

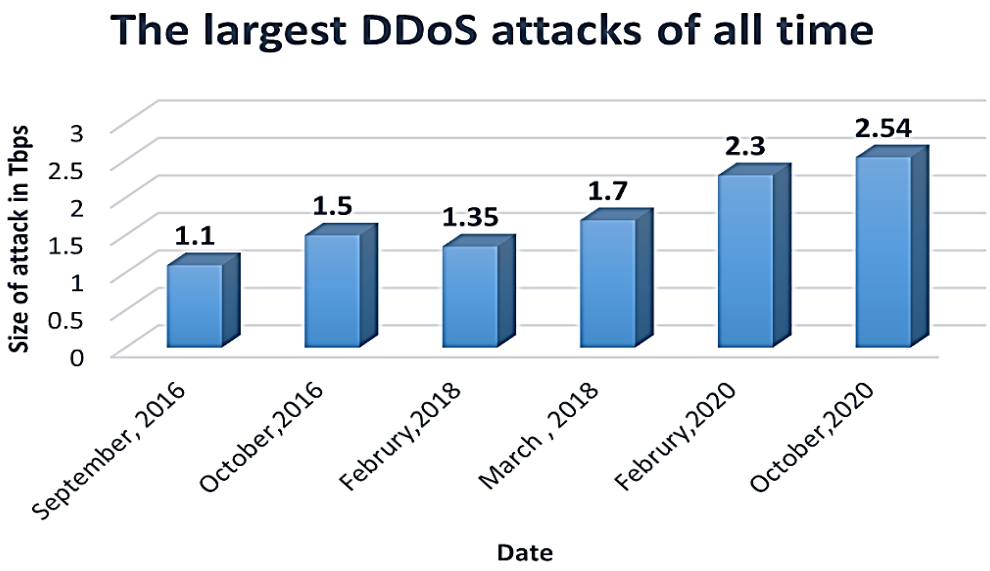

Figure 1.3: The biggest DDoS attacks based on the size of the attack.

Figure 1.4 illustrates the frequency of DDoS attack types between January 2020 and March 2021. As can be observed, volumetric attacks have grown greatly in popularity in comparison to other types of attacks (David Warburton, 2021). Thus, Gao et al. (2016) proposed that this section discusses two recent and critical distinctions between the various categories. A DRDoS attack combines DDoS and IP spoofing methods. This form of attack is more sophisticated than DDoS and has a greater impact on the network that has been infected as a result of its attack plan. Because traditional DDoS attacks differ in their mechanism of operation and attack methods, the latest update of DDoS attacks, i.e., DRDoS attacks, consists of two

components: the first is reflection and amplification, and the second is IP spoofing. In other words, offenders utilize the IP spoofing source address to conceal their identity and allow third parties to transmit data to the victims as determined by the IP packet's source address field. This is referred to as reflection because harmless service servers are duped into "reflecting" the victims' attacks.

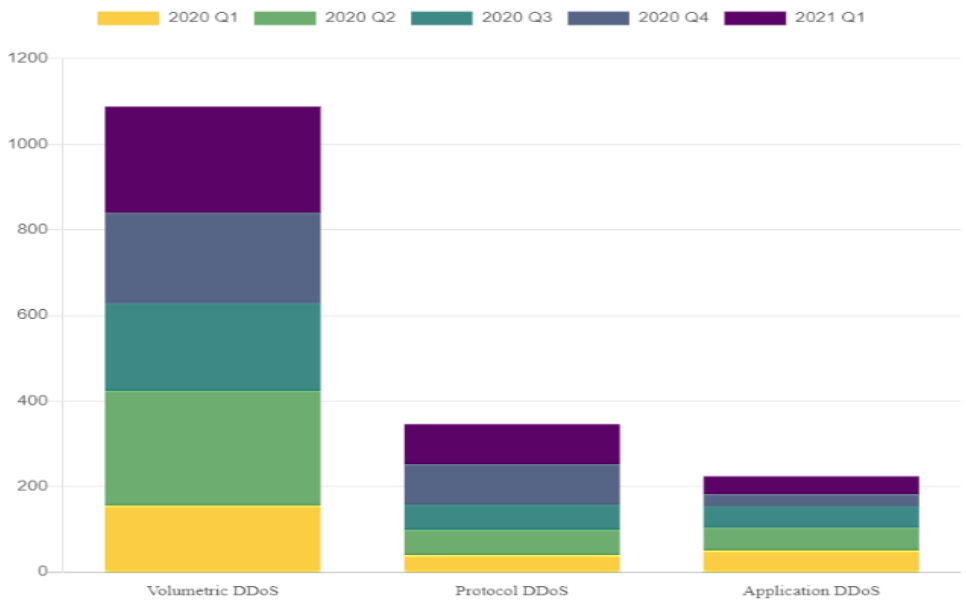

Figure 1.4: Frequency of DDoS attack types, January 2020 through March 2021.

Amplification: in some protocols, the scale of the answer packet is greater than that of the message packet. By abusing this function, attackers can produce a significant amount of traffic from a relatively little amount of traffic. From this role, abused servers are referred to be amplifiers (Böttger et al., 2015; Makita, 2017). Due to their unique characteristics, DRDoS attacks are among the most damaging. To begin, they protect the attacker's anonymity by faking the IP address. As a result, identifying attackers and stopping their services is difficult. Second, these attacks violate certain UDP-based network protocols by sending answers that are larger than the size of the request. Numerous studies have also demonstrated that DRDoS attacks can be amplified by a factor of 500 using UDP-based bandwidth amplification (Berti-

Equille & Zhauniarovich, 2017; Rossow, 2014). As a result, certain systems that do not verify sources, such as protocols that supply services through UDP, begin sending response packets without confirming the sources of the demand packets.

Shawahna et al. (2018) said that the economic Denial of Sustainability (EDoS) attack as numerous studies has noted, this type specifically targets cloud computing. Economic Denial of Service (DDoS) attacks are one of the most prevalent cloud-based risks. The EDoS attack exploits the cloud's elasticity and auto-scaling capabilities to charge an excessive amount of money to a cloud purchaser's account, resulting in widespread service termination or insolvency (Masood et al., 2013) EDoS is distinct from traditional DDoS. The latter is designed to consume all of the Web Server's resources (memory, bandwidth, CPU, and so on), rendering it unreachable to normal users. EDoS, on the other hand, is separate from classic DDoS. The latter is designed to exhaust the Web Server's resources (memory, bandwidth, CPU, and so on), leaving it inaccessible to normal users (N. Agrawal & Tapaswi, 2020).

1.2.2 Domain Name System (DNS)

Khormali et al. (2020) revealed that the Internet, the means through which the majority of communications are currently transmitted in the modern world, is based on the DNS. DNS is widely used nowadays for a variety of purposes, including the conversion of domain names to Internet Protocol (IP) addresses. A computer can locate a website using the domain name system by looking up the IP address associated with the name. Besides, the attackers exploit the functionality of open DNS resolvers to magnify a small number of DNS queries into a large payload directed at a target server or network, rendering it unreachable. These are referred to as amplification attacks (Zheng et al., 2018).

1.2.3 Distributed Reflection Denial of Service Attack on DNS

According to cybersecurity researchers, DDoS attacks have become more widespread over the last several years. Additionally, the growth of DDoS attacks has had a substantial influence on the functioning of businesses and organizations worldwide, causing financial and technical harm as a result of its damaging effect on DNS infrastructure (Jang-Jaccard & Nepal, 2014; Nuiaa et al., 2021). The DNS amplification attack is more prevalent than other DNS attacks due to the attacker's preference for attacks with a high impact and a cheap cost. Additionally, DNS reflection attacks have a significant and deadly impact due to their attack-unique properties. While all of these protocols have witnessed a rise in activity this year, DNS continues to be the most prominent. DNS can be regarded as the dominating protocol in reflection/amplification attacks since attack numbers exceed all other attack vectors combined, and the response packet size is bigger than the demand. Recent years have seen a surge in this type of attack, particularly against protocols that can be abused to amplify the packet size, such as DNS and other protocols.

Due to the unique properties of DNS reflection attacks, they have a significant and deadly impact. In the 2016 year (NETSCOUT, 2019), a poll included a question about the reflection/amplification techniques employed in Figure 1.5.

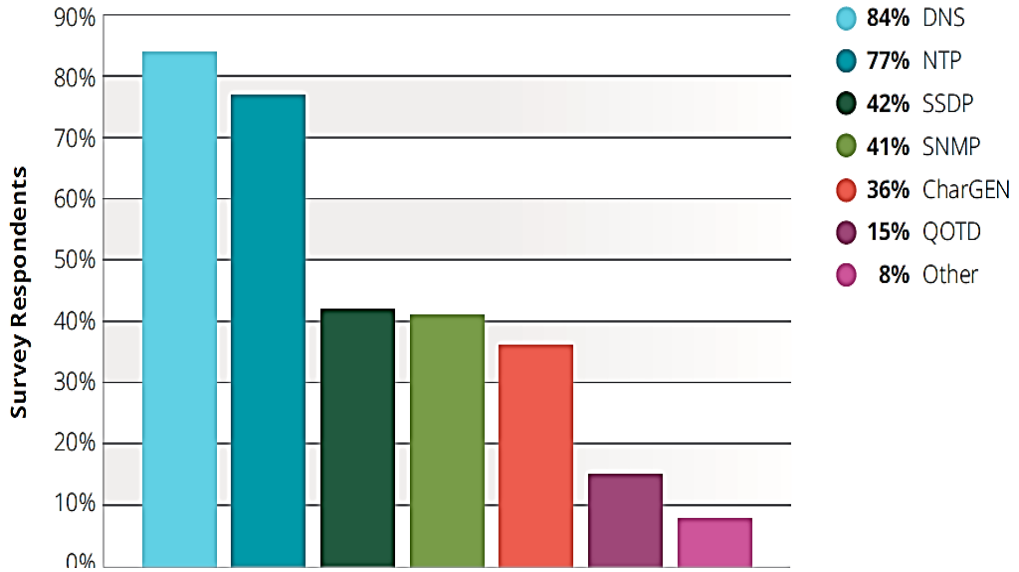

Figure 1.5: Protocols Used for Reflection/Amplification. Source Arbor Networks, Inc (NETSCOUT, 2019).

Figure 1.6 explains the prevalence of various DDoS attack strategies between January 2020 and March 2021. and As we can see, DNS Reflection attacks are rising in popularity alongside other sorts (David Warburton, 2021).

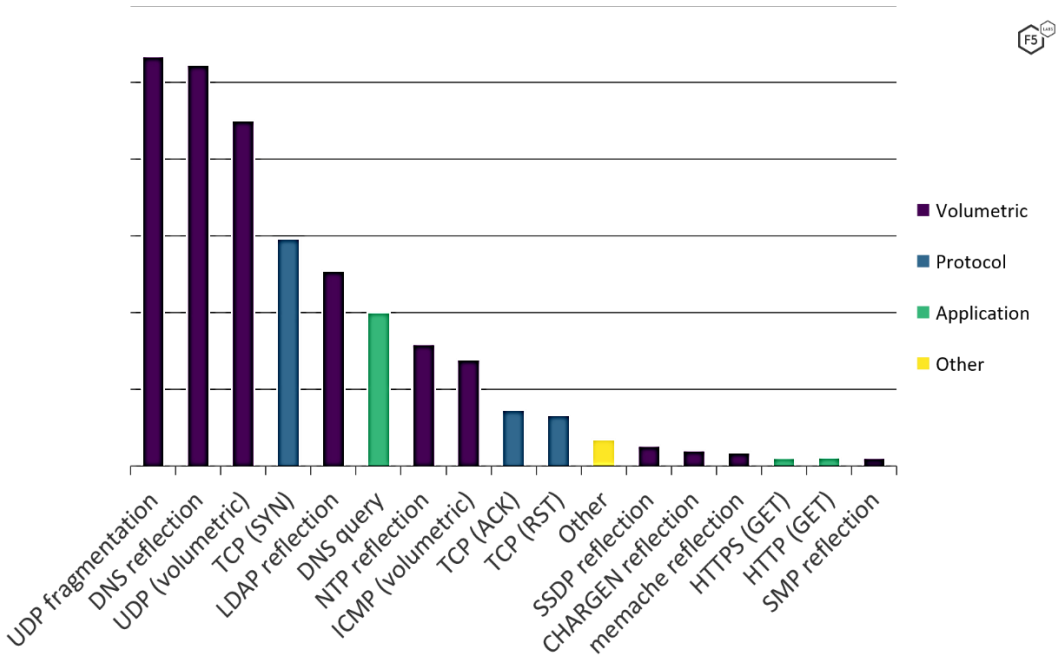

Figure 1.6: Frequency of different DDoS attack tactics, January 2020 through March 2021. Source (David Warburton, 2021).

1.3 Research Motivation

DDoS attacks, particularly their extension is known as distributed reflection denial of service DRDoS attacks, are one of the most significant and complex security difficulties and issues. As a result of this status, researchers have proposed a mechanism for detecting and mitigating this novel sort of attack. The following are the research's motivations. DDoS attacks are one of the most often seen types of attacks. Additionally, DRDoS attacks are a subset of DDoS attacks. These types of attacks are notoriously difficult for typical detection systems to detect. DRDoS attacks take advantage of vulnerabilities in certain protocols, such as DNS, NTP, and so on. DNS is the protocol that is most frequently attacked by DRDoS attacks, which distinguishes it from other protocols. In terms of DNS, it can be used to amplify the response size relative to the request size and then utilize them as platforms to start an attack on the prey and flood it with responses from spoofing sources. As a result, tracing the source of an attack to mitigate or halt it is challenging.

The research examines how DRDoS attackers exploited pre-existing DNS vulnerabilities to begin their attacks. According to many claims from security firms, the EMDDMAT technique will be demonstrated to detect DRDoS attacks directed at DNS.

- ❖ According to the threat report DDoS 2019 Q2 Tony et al. (2019b), Increasingly more of today's security vulnerabilities exist at the application layer. Apart from other sorts of attacks, the most well-known is the DNS amplification attack. Yet, as illustrated in Figure 1.7, the DNS amplification attack predominates, accounting for 65.95% of all attacks.

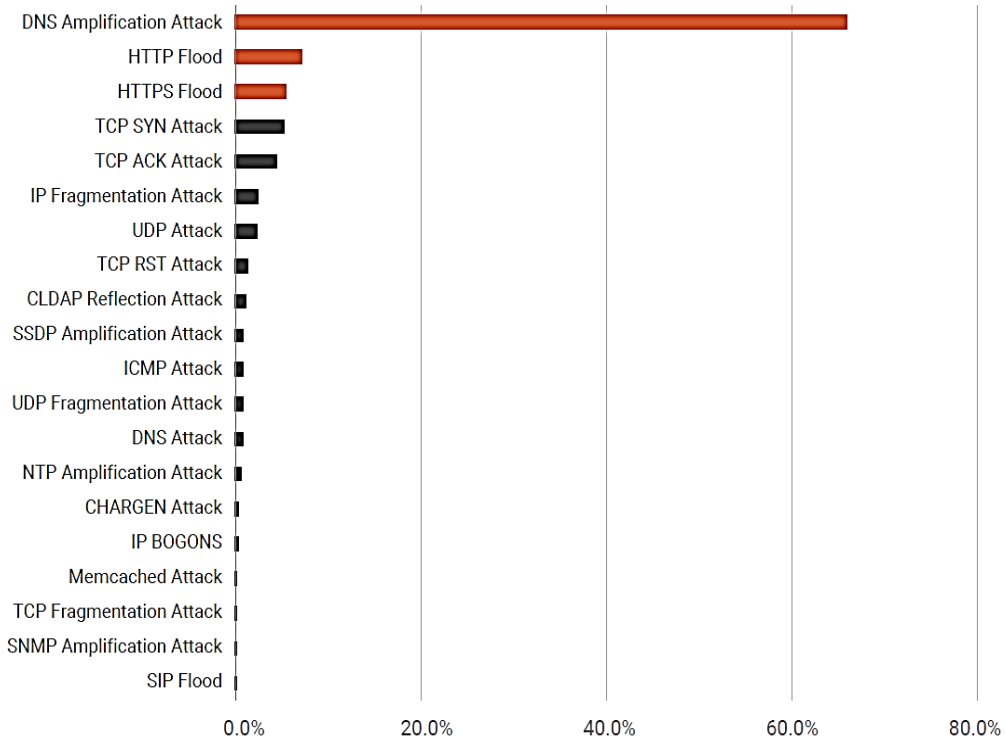

Figure 1.7: Distribution of DDoS attack vectors Q2 2019.

- The DNS is a critical component of the Internet's operation, as it is the medium over which the majority of modern communications are transmitted. Attackers are constantly on the lookout for novel methods of compromising the DNS infrastructure by continuously seeking new vulnerabilities. Therefore, the advancement of DNS security and its concerns are critical. This effort is important to direct the community's attention to an unresolved issue that deserves additional attention. Understanding the DNS's evolution is critical given the DNS's critical position in the networking infrastructure (Khormali et al., 2020).

1.4 Research Problem

Among the most significant security issues in the cyber security domain are the nature and vulnerabilities of DNS. Therefore, cybercriminal attacks are carried out

by making use of those characteristics. Hence, open DNS resolvers are used to start and spread the attack in the case of a DRDoS attack (Huraj et al., 2018; Saharan & Gupta, 2022).

Furthermore, the massive size of DNS traffic and its continuously changing dynamic behavior at a particular period of time will lead to a huge number of features, most of which may be unhelpful, repetitive, incomplete, or irrelevant. Therefore, the mechanisms that use the traditional methods that are based on predefined or trained threshold to detect DRDoS attacks based on DNS responses will be ineffective and useless as the predefined or trained thresholds are not useful in constantly changing dynamic environments and may not keep up with the constant change in data traffic, all of these reasons will lead to low detection accuracy and also a high rate of false positive alerts. therefore, the best solution is to utilize the adaptive threshold for the continuously changing dynamic behavior environment. The appropriate selection of features has a significant favorable effect on the performance of the detecting mechanism. Therefore, DRDoS attack detection mechanisms require optimization of the chosen feature set to capture the relevant DNS responses that are affected during DRDoS attacks. wherefore, for the massive number of features, the meta-heuristic is to select the salient features from other features (Sharafaldin et al., 2019).

Furthermore, the existing DNS responses-based DRDoS attacks detection mechanisms can detect real-world DRDoS attacks with a considerably low detection accuracy and high false positives, which leads to a reduction in the accuracy of DNS responses-based DRDoS attacks detection because they do not take into consideration the features that significantly contribute to detecting DRDoS attacks based on DNS responses (Fachkha et al., 2015; Han et al., 2020; Thorat et al., 2021). Therefore, we proposed our mechanism that is designed by using modified meta-heuristic algorithms

based on adaptive thresholding techniques and clustering techniques. As a result, this the thesis seeks to address the following points:

- Signature-based detection mechanisms and those that are designed based on predefined or trained thresholds that are incapable of detecting DRDoS DNS attacks because these attacks are highly sophisticated and do not rely on specific signatures and trained or predefined thresholds.
- The majority of existing mechanisms used to detect DRDoS attacks that are based on DNS responses that suffer from low detection accuracy and a high false-positive rate because they do not take into consideration the salient features of DNS responses that can aid in improving accuracy metrics.

1.5 Research Objectives and Goals

The primary purpose of this research is to offer an enhanced mechanism for identifying DRDoS attacks based on DNS responses. The proposed mechanism has been designed based on modified metaheuristic algorithms, adaptive thresholding techniques, and clustering techniques. The proposed mechanism aims to enhance accuracy metrics such as DA and FP. As a result, the following goals have been established to help accomplish the research's primary objective:

1. Research objective 1 (RO1): To propose a model based on modified meta-heuristic algorithms and adaptive thresholding techniques to select the salient features to distinguish between the normal DNS r and malicious DNS responses.

2. Research objective 2 (RO2): To propose a detection model based on clustering and evolving techniques to detect the DNS-based DRDoS attacks based on the features that were selected in RO1.

1.6 Research Contribution

This research makes a significant addition by presenting an enhancing mechanism for detecting DRDoS attacks based on DNS responses that is designed based on modified metaheuristic algorithms, adaptive thresholding techniques and clustering techniques. The proposed mechanism achieved an acceptable accuracy metric in terms of high detection accuracy and low false positive. This research will make the following contributions:

- A model called the Proactive Feature Selection (PFS) model has been designed to be applied as a feature selection model to identify the most salient features used to distinguish between DNS responses during DRDoS attack occurrences. As a result, the PFS model produces a new set of features from the CICDDOS2019 dataset that aids in the detection of DRDoS attacks based on DNS answers.
- A model called the Evolving Dynamic Fuzzy Clustering (EDFC) model has been designed to be applied as a prediction model to detect DNS-based DRDoS attacks. The performance efficiency of the EDFC model has been measured based on accuracy metrics like DA and FP.

1.7 Research Scope and Limitation

This research is limited to the proposed mechanism for detecting DRDoS DNS attacks, which reflects and amplifies DDoS attacks utilized in DNS attacks at the application layer, as illustrated in Table 1.1.

Table 1.1: The research Scope.

Items	Scope of Research
Environments	IPv4
Protocol	DNS
Attack type	DRDoS Attack
Targeted layer	Application layer
Transport Layer	UDP
Network traffic	DNS Responses
Detection	Anomaly-based detection
Dataset	Benchmark dataset (CICDDoS2019)
Evaluation metrics	Detection Accuracy and False Positive
DNS over https	The DNS over HTTPS is out of this research scope.

1.8 Research Methods

This research employs metaheuristic methods based on adaptive thresholds and machine learning to provide additional options for detecting DRDS DNS attacks with greater accuracy. To accomplish the purpose of this research, follow the stages and techniques outlined below: (i) discover DNS security flaws by observing and analyzing DNS answers to differentiate DRDoS attacks, (ii) Analyze pertinent studies and literature, (iii) Propose a mechanism for boosting the detection of DRDoS DNS attacks by analysis of DNS answers, (iv) Design and implementation of the proposed mechanism and (v) design and execution of the planned mechanism experiment, as

well as evaluation and discovery of the outcome. The methodological stages of the research model are illustrated in Figure 1.8.

The first stage is to conduct a review and define the research's primary objectives. DRDoS DNS attacks are among the most serious DNS security vulnerabilities. And then determine the optimal solution in terms of DA and FP for these attacks. *The second stage* establishes and verifies the research problem accurately by a thorough evaluation of recent works. As a result, this stage discusses an existing solution area and the potential for future research on DRDoS DNS attack detection. Present a solution to the problem presented in the third step. This approach comprises numerous phases that consolidate the detection fineness of DRDoS DNS attacks. The proposed mechanism would be implemented by developing an enhanced mechanism for detecting DRDoS DNS attacks that are based on SWEVO and machine learning algorithms.

Whereas, the *fourth stage is* primarily concerned with the implementation and design of the proposed mechanism based on SWEVO and machine learning algorithms. The proposed approach employs the feature selection method to isolate and analyze DNS responses to distinguish DRDoS DNS attacks from normal DNS responses. The final section of this step employs the clustering strategy to improve DA and FP. *In the fifth stage,* test and evaluation results in the accomplishment of the research objectives. To begin, the proposed mechanism was examined and tested on its ability to increase anomaly detection in DNS environments using a real-world traffic dataset generated by an actual DNS-based DRDoS attack. Finally, this process was compared to established detection methods. The results indicated that our method was capable of detecting these types of attacks with a high DA and a low FP, which corresponded to the impacts discussed in Chapter five.

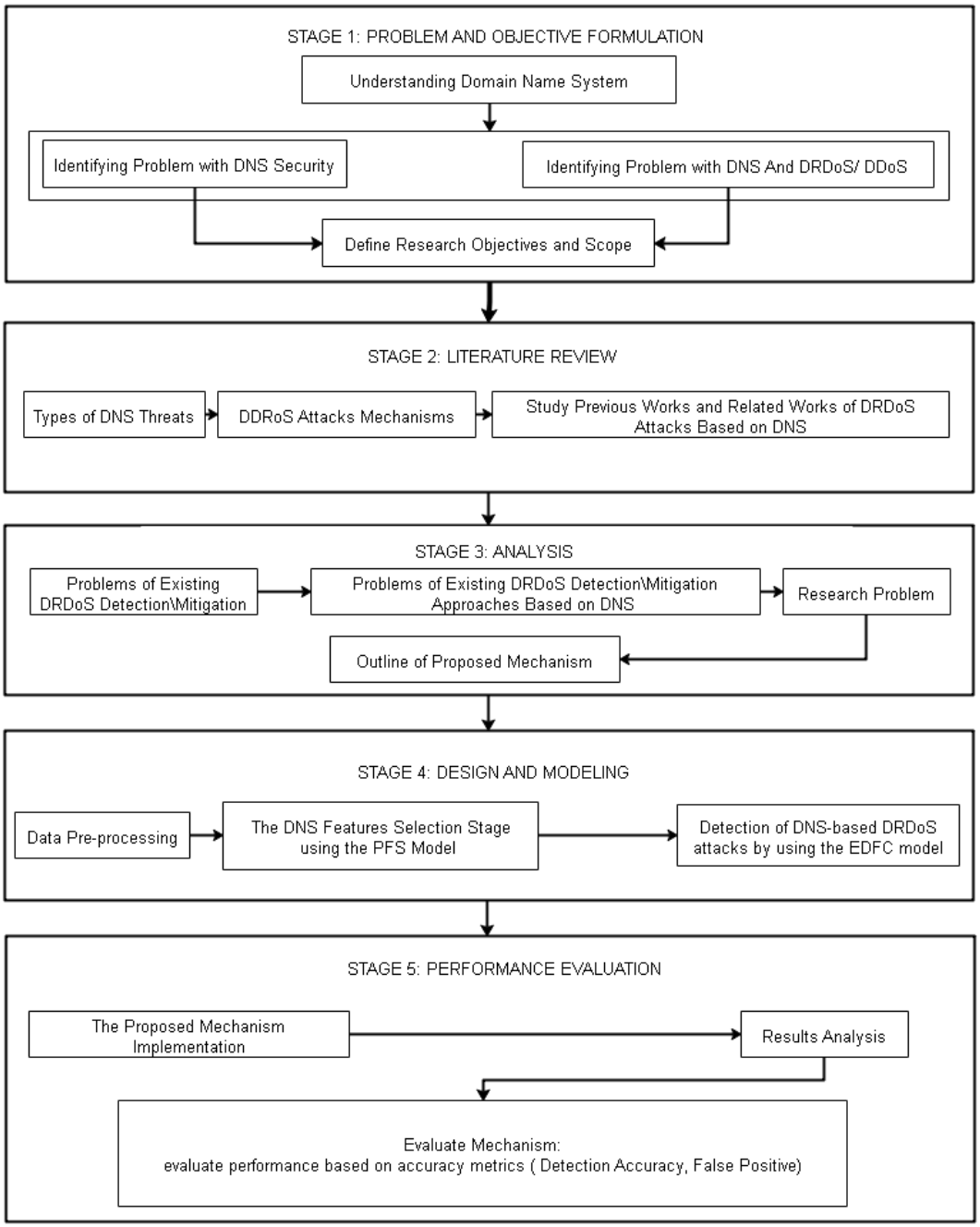

Figure 1.8: Main Stages of Research Process.

1.9 Thesis Organization

This thesis is divided into six chapters:

Chapter 1: This chapter provides information regarding the Internet and its growth in a variety of ways, including trends and economics; it also sheds light on internet security and cybersecurity. This chapter defines the research motivation, the

research scope, the research techniques, the research problem, the research objectives, and the research contribution.

Chapter 2: The (Literature Review): This chapter discusses DRDoS attacks in detail and the available tools for detecting DNS-based DRDoS attacks.

Chapter 3: This chapter elucidates the proposed mechanism by demonstrating in detail that it consists of two models: the first is the PFS model. The EDFC model is the second. It sequentially discussed the technique steps and illustrated them with flowcharts.

Chapter 4: This chapter discusses the design and implementation of the proposed mechanism, outlining the phases involved in developing the PFS and EDFC models. explains how the PFS model distinguishes between normal and anomalous traffic. Finally, the EDFC model is used to improve the DA and FP of the PFS model.

Chapter 5: This chapter proposed a mechanism lid and conducted an in-depth analysis of the rendering based on the results of the trials. This chapter tests and explains the suggested mechanism for detecting DRDoS DNS attacks and compares the results to those of existing models based on the DA and FP of attack detection and response.

Chapter 6: This chapter summarises the entire argument and concludes the issue presented in this thesis—along with some recommendations for future work and directives to improve the proposed system.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

This chapter presents a comprehensive critical review of the state-of-the-art published kinds of literature to display the existing research gaps. It is composed of six broad sections which cover the relevant key concepts, previous research to detect DRDOS attacks on DNS, with a particular emphasis on DNS-based DRDoS attacks. Also, it offers an overview of the primary approaches for detecting DRDoS attacks based on DNS traffic characteristics to facilitate comprehension of the planned study in this area. As well, this chapter discusses the most widely used DNS-based DRDoS attack detection techniques. So, the following table summarises the chapter's organization. To begin, section 2.2 discusses cybersecurity risks such as DDoS attacks. Then, in section 2.3, an overview of the DNS is presented. Section 2.4 details the most common and well-known types of DNS attacks. Section 2.5 summarises DRDoS attacks on DNS. Section 2.6 defines the feature selection criteria for detecting DRDoS threats based on DNS. Section 2.7 describes similar efforts on the detection of DRDoS attacks using DNS. And finally, in section 2.8, this chapter is summarised.

2.2 Background

This section provides an overview of cybersecurity risks and the procedures used to detect them. Thus, DDoS and DRDoS attacks are the primary cybersecurity problem in terms of detection efficiency.

2.2.1 Cybersecurity Threats

Kilincer et al. (2021) point out that the increased use of the internet has forced the development of more sensitive technologies by cybersecurity firms. As a result, proactive cybersecurity solutions are being developed, including network behavior monitoring, machine learning, and threat analysis. Nowadays, detection methods are one of the most widely utilized technologies for enhancing security against online dangers. The taxonomy of cybersecurity attacks presented in Figure 2.1 is based on numerous characteristics, including the type of cybersecurity attack, the duration of the attack, the methodology used, the layer and protocol destination targeted, and so on. Numerous researchers have attempted to categorize cybersecurity threats (Ferdinand & Benham, 2017; *General Cyber Security Taxonomy*, 2022; Marinos, 2016; Syafrizal et al., 2021).

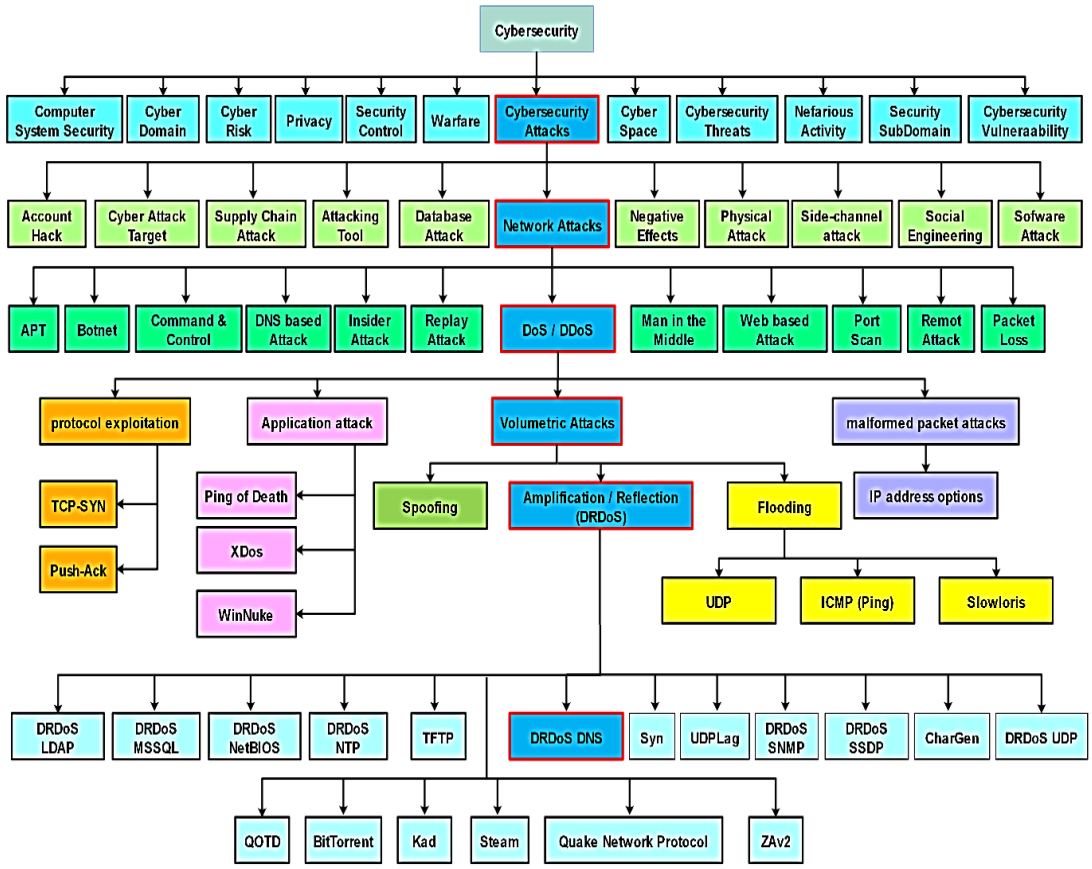

Figure 2.1: Cybersecurity attacks taxonomy.

Bårli et al. (2021) mentioned that Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks have increased in volume and frequency over the last decade, and present detection and mitigation methods are largely useless. Likewise, protecting against denial-of-service and distributed denial-of-service attacks is more challenging than defending against other types of malicious cyber-attacks. It has been difficult to develop techniques for detecting these attacks at the packet or flow, level due to their ability to masquerade as normal communication.

Accordingly to Khormali et al. (2020) declared that while DNS-based DDoS attacks are designed to deplete server resources, managing Internet and application usage, including preserving user data, privacy, integrity, and availability, is becoming increasingly difficult as our dependency on the Internet grows in our daily lives. The Internet has become increasingly important in our daily lives in recent years, especially in the areas of communication, education, government services, banking, and e-commerce. Though, as the number of available applications increases, the threat to user privacy and data security increases proportionately (Jing et al., 2018). This section defines DNS, discusses how DRDoS attacks spread and explains how DRDoS attacks exploit DNS functionality.

2.3 Overview of Domain Name System (DNS)

Cloudflare, Papadopoulos et al. (2020; 2020) added that DNS uses a human-readable language to convert domain names to computer IP addresses. Thus, an end-user can reach a website via a web browser and a combination of names. DNS is a critical component of the Internet's infrastructure. Besides, network security devices formerly employed to monitor DNS traffic have been rendered ineffective, increasing illicit DNS activity (Rajendran, 2020; Y. Wang et al., 2021). As a result, the firewall's

default configuration allows data transport over the UDP 53 port used by the DNS service, even though this port is not designed for data transfer (J. Ahmed et al., 2019). As a result, DNS traffic across the network's edge can flow freely without being slowed down by restrictive security measures. Similarly, the host frequently places a high premium on the DNS server's response information (Y. Wang et al., 2021).

2.4 DNS Attacks

The following list of DNS-related attacks is the most well-known. Numerous scholars in this field have compared various forms of DNS attacks, however, in this study, we will focus exclusively on the reflection/amplification DNS attack, or DRDoS DNS attack. This section examines how this sort of attack become the most serious of the other types of attacks and how quickly it has grown in recent years. DNS attacks fall into four categories (Bushart & Rossow, 2018; Soliman et al., 2018; W. Sun et al., 2019; Torabi et al., 2018) as shown in Figure 2.2:

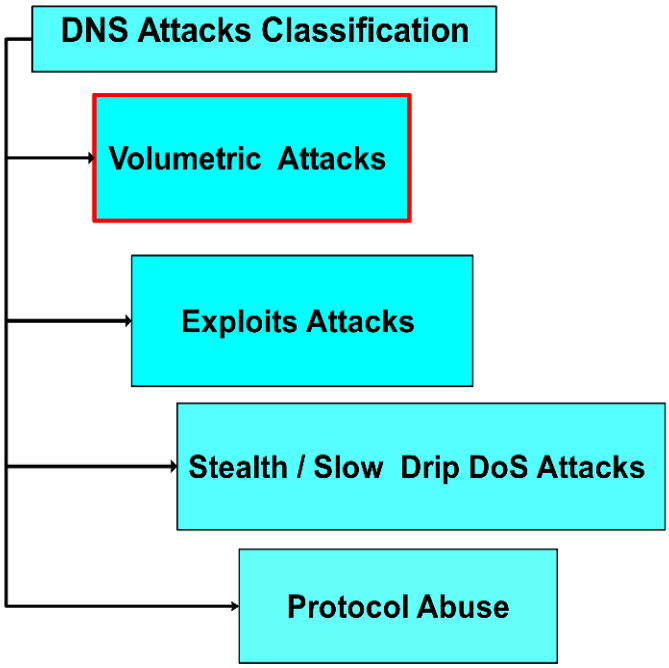

Figure 2.2: DNS attacks classification.

2.4.1 Volumetric Attacks

DNS-based DDoS attacks are designed to deplete server resources, resulting in a denial of service (DoS) attack. For instance, flooding the DNS server with queries from a single source or distributed origins until it becomes saturated or overloaded, at which point the service is terminated or degraded. The types of volumetric attacks are depicted in figure 2.3. volumetric attacks are a sort of DDoS attacks that are differentiated by the size of the attacks directed at the victim. The scenario for this type of attack begins with flooding the target with massive amounts of traffic until the server becomes saturated and unresponsive. As a result, the network's resources and services will be unavailable to legitimate users, will be extremely slow, or will have inconsistent access. This form of attack uses the victim's bandwidth by flooding it with traffic (Gondim et al., 2020). The volumetric attack occurs when DNS concentrates only on exhausting the host's available bandwidth. When the attack is successful, the legal users receive no response from the DNS hosts, as the legitimate DNS queries are dropped. Accordingly, volumetric attacks are classified into four subtypes (Bushart & Rossow, 2018). Figure 1.4 illustrates the frequency of DDoS attack types from January 2020 to March 2021. As can be seen, volumetric attacks have grown significantly in popularity in comparison to other types of attacks (David Warburton, 2021).

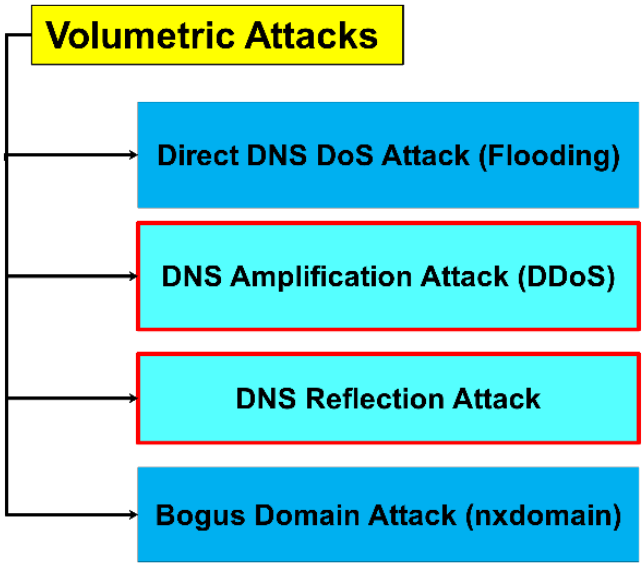

Figure 2.3: Volumetric attack types.

- Direct DNS dos attack (flooding): the server is specifically designed to defend against this type of flooding attack. Moreover, it will receive a high number of fake requests from the attacker, causing the system's resources and network bandwidth to become overburdened. At this state, no incoming requests to the DNS server can be processed, and the server cannot respond. This type of attack is detected by a specialized firewall (Boro & Bhattacharyya, 2017; Georgiev & Nikolova, 2017).
- DNS Amplification Attack (DDoS): the DNS amplification attack is a highly sophisticated DDoS attack variation with deadly repercussions (Abou El Houda et al., 2020). In addition, this attack targets open DNS servers by flooding the prey's network with fake DNS reply traffic (Kim et al., 2017) and its CPU or memory (Trejo et al., 2019). So, DNS's reply message is more lengthy than what is required in this type of attack (Prasad et al., 2020) , This DNS traffic is aimed toward the victim (Samta & Sood, 2020). Usually, the IP address of the victim used to initiate the attack is faked to conceal the perpetrator's location