IJARIIT
International Journal Of Advance Research, Ideas And Innovations In Technology

ISSN: 2454-132X
Impact Factor: 6.078
(Volume 10, Issue 6 - V10I6-1277)
Available online at: https://www.ijariit.com

# A Review of Distributed Denial of Service Attack Techniques and Mitigation Strategies

Shantanu Gupta
shantanutks8@gmail.com
Vellore Institute of Technology, Vellore, Tamil Nadu

Sivakumar V
sivakumar.v@vit.ac.in
Vellore Institute of Technology, Vellore, Tamil Nadu

Anish Rout
anish.rout2022@vitstudent.ac.in
Vellore Institute of Technology, Vellore, Tamil Nadu

Devanshu Madnani
devanshu.madnani2022@vitstudent.ac.in
Vellore Institute of Technology, Vellore, Tamil Nadu

## ABSTRACT

***This report provides an extensive analysis of Distributed Denial of Service (DDoS) attacks, focusing on their motives, methodologies, and impacts across various sectors. It classifies different DDoS attack types, examining those targeting specific network layers and emphasizing unique attack patterns within cloud environments. The study also reviews trends highlighting the rising frequency of these attacks in sectors such as government, finance, and online gaming. To counteract these threats, the report outlines a range of preventive and mitigation strategies. It covers traditional methods like IP blacklisting, filtering, and firewalls, as well as advanced solutions involving real-time traffic monitoring and machine learning for dynamic anomaly detection. The effectiveness of cloud-based defenses, application- layer security practices, infrastructure resilience, and the integration of blockchain technologies is also explored. This comprehensive analysis ultimately aims to provide insights into the evolving landscape of DDoS attacks, advocating for a multi-layered approach to enhancing cybersecurity.***

**Keywords**: *Distributed Denial of Service, DDoS, Cybersecurity, Prevention Strategies, Machine Learning, Blockchain, Cloud Security, SDNs, Anomaly Detection.*

## INTRODUCTION

A Denial-of-Service (DoS) attack is a cyber-attack that aims to prevent a service or machine in a network from functioning normally by making it unavailable to legitimate users. This is done by flooding the target system with redundant or unnecessary requests, aiming to overload the systems, and preventing legitimate requests from being processed, thus disrupting the services of a host connected to a network. One frequently encountered type of DoS attack is the distributed denial-of-service attack (DDoS attack), which aims to overwhelm the victim machine with traffic originating from many different sources [1].
Distributed Denial of Service (DDoS) attacks are one of the most pressing threats in cybersecurity today. These attacks aim to disrupt the normal operation of a targeted network, service, or website by overwhelming it with an excessive amount of traffic. Unlike standard Denial of Service (DoS) attacks, which typically originate from a single source, DDoS attacks originate from multiple compromised systems which are taken over by the attacker, often forming a botnet, to amplify their impact. This distributed nature not only makes DDoS attacks more challenging to mitigate but also allows them to appear as legitimate traffic, complicating detection and response efforts.

Recent trends reveal that attackers are employing increasingly sophisticated techniques, exploiting cloud environments, IoT devices, and even software-defined networks (SDNs), making traditional defenses like firewalls and IP filtering less effective.

To combat these evolving threats, organizations need to adopt a multi-layered defense strategy. This report provides a detailed analysis of different types of DDoS attacks, examines their motives and patterns, and explores a range of mitigation strategies. By covering conventional methods like traffic filtering and rate limiting, along with advanced techniques involving machine learning, blockchain, and cloud-based protection, this study aims to shed light on how to enhance network resilience and maintain cybersecurity in the face of these complex threats.

## LITERATURE REVIEW

### Targets of DDoS Attacks

DDoS attacks have grown in scope and sophistication, targeting a wide range of industries, institutions, and users. The primary targets of these attacks include financial institutions, e-commerce platforms, ISPs, and cloud-based services.

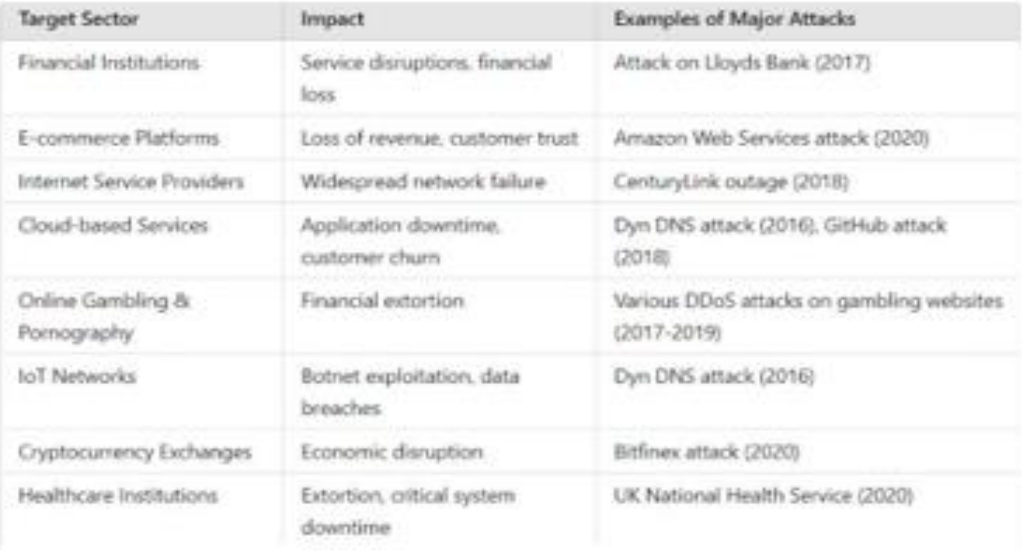
These entities are attractive targets because of their reliance on continuous service availability, and even brief service interruptions can result in significant financial losses and damage to the service's reputation [23].

Moreover, DDoS attacks are frequently launched against online gambling and pornography websites, primarily motivated by financial extortion. Governmental and political institutions are also key targets, as ideological and politically motivated attackers seek to disrupt services or silence voices they oppose. The IoT sector has also become increasingly vulnerable due to the widespread adoption of IoT devices, which are often inadequately secured. Attackers exploited this vulnerability in the 2016 Dyn DNS attack, which crippled major platforms like Netflix and Twitter [2].

In the past five years, the landscape of DDoS attack targets has expanded to include cryptocurrency exchanges and healthcare institutions, particularly during the COVID-19 pandemic. Cryptocurrency exchanges have been targeted due to the financial disruption a service interruption can cause, while healthcare organizations, which increasingly rely on telehealth and digital infrastructure, have been attacked with the goal of extortion [4].

Comparative analysis of traditional and emerging targets reveals that while industries like financial institutions and ISPs have fortified their defenses, sectors like IoT and healthcare are more vulnerable due to lack of security infrastructure [5].

*Table 1: Major Targets of DDoS Attacks (2016-2023)* [6]



| Target Sector | Impact | Examples of Major Attacks |
|---|---|---|
| Financial Institutions | Service disruptions, financial loss | Attack on Lloyds Bank (2017) |
| E-commerce Platforms | Loss of revenue, customer trust | Amazon Web Services attack (2020) |
| Internet Service Providers | Widespread network failure | CenturyLink outage (2018) |
| Cloud-based Services | Application downtime, customer churn | Dyn DNS attack (2016), GitHub attack (2018) |
| Online Gambling & Pornography | Financial extortion | Various DDoS attacks on gambling websites (2017-2019) |
| IoT Networks | Botnet exploitation, data breaches | Dyn DNS attack (2016) |
| Cryptocurrency Exchanges | Economic disruption | Bitfinex attack (2020) |
| Healthcare Institutions | Extortion, critical system downtime | UK National Health Service (2020) |

**Motivations behind DDoS Attacks**

The motivations driving DDoS attacks are varied and often interconnected. The primary motivations can be categorized as follows:

a. **Financial or Economic Benefit:** Attackers seeking financial gain are often highly skilled and well- organized. Extortion through ransom demands in exchange for halting a DDoS attack is a common technique. These attacks have become more sophisticated and are difficult to prevent due to attackers' extensive knowledge of system vulnerabilities [2].

b. **Revenge:** DDoS attacks motivated by revenge are typically carried out by individuals with personal grievances. These attackers are often less technically adept but can still cause significant disruption [2].

c. **Ideological Beliefs:** Politically and ideologically motivated attacks are typically aimed at governments and political organizations. The Estonia attack in 2007 is a prominent example. Ideological attacks have increased, particularly with the rise of hacktivist groups [2].

d. **Cyberwarfare:** State-sponsored or terrorist organizations may launch DDoS attacks as part of cyberwarfare efforts, aiming to paralyze critical infrastructure. The 2016 Mirai botnet attack is a notable example of this type of warfare, with the ability to incapacitate major services through botnets of IoT devices [2].

Financial gain continues to be the most prominent motivation for DDoS attacks. However, ideological attacks and cyberwarfare pose significant challenges due to their unpredictability and the large-scale disruption they can cause[2].

**Mechanism of DDoS Attacks**

A DDoS attack primarily consists of three phases. During these three phases, four primary components are present, namely the attacker, multiple control masters, multiple slaves and one victim.

DDoS attacks can be either manual, semi-automatic and automatic. However, in recent times, automatic DDoS attacks are the most popular, leading to DDoS attacks being more frequent and easier for the attacker to do.

i. **Phase 1 - Recruiting Attack Armies:** In this phase, the attacker uses viruses such as worms and self- propagating programs to infect the devices of users and take control of them by taking advantage of their security flaws.

These devices are known as slaves and are used by the attacker to overwhelm the victim system [2].

ii. **Phase 2 – Propagation:** This phase occurs after the acquiring of the attack army. In this phase, the attacker propagates commands known as the attack code to the slave devices. This attack code includes information of the victim, along with the time, date and duration of the attack [2]

iii. **Phase 3 – Attack:** After the attack code has been propagated, the attacker can begin to attempt a DDoS attack. There are several methods to perform a DDoS attack and most of the important ones have been classified below [2].

**Classification of DDoS Attacks**

i. **Bandwidth Depletion Attacks:** This type of attack is called bandwidth depletion one because it seeks to use up the bandwidth of the target system by the excessive amount of data that is being sent to it. The intent is to render the system incapable of processing any credible request owing to the sheer volume of requests. This sort of attack can also consist of either Protocol abuse or dig operational social engineering techniques to exploit the network Protocols and trigger huge data streams. For this type of attack, a practical UDP flood enhancement can be reasonably used. The internal system is bombarded with a flow of packets so that the denial of service to the valid users is also noticed at that point of time emulation of these architectural measures being performed is made [3].

ii. **UDP Flood Attack:** A UDP flood attack is executed when a target or a victim is forcefully brought to access a lot of ports available on the machine. In the TCP IP model/programming, applications listen to data directed to a particular port at a specified address. If a media destination address matches an advertisement on port x821165, the information appears in an open space in the device. This aggressive action is performed until there is no more Internet bandwidth left for the victims' systems. Many attackers use fake IP addresses to make more aggressive attacks and cause the target to become unreachable through the entire network [3].

iii. **ICMP Flood Attack:** An ICMP Flood attack is most commonly known as a ping flood attack. It solely uses ICMP echo requests (pings) against the system. During a ping flood attack, the attacker floods the target network with a large volume of ICMP echo request packets. ICMP echo replies are then sent by the target devices, utilizing the available bandwidth and CPU power of that system. The problem becomes quite serious if this form of attack is coupled with other networks and hence it is not surprising that this type of attack has brutal effects when carried out as illustrated in the smart attack [3].

iv. **Fraggle Attack:** Just as the ICMP flood, fraggle attacks also focus on saturating the victim with UDP packets but instead of ICMP packets. Large volumes of UDP echo packets termed as UDP flood water is also sent out. Normally, the UDP floods are aimed at network amplifiers like routers, DNS servers or other reflector services. Such reflectors send back the packets to the target and thus utilize excess bandwidth resulting in the system denying any further packets from genuine users [2].

v. **DNS Amplification Attack:** DNS amplification is carried out by sending a spoofed IP address, targeting DNS servers of organizations. This forwarding activity allows many DNS servers, when sent such requests, to return a DNS response (result) which is less than the amount of DNS queries made. This effectively enhances transmission and volume techniques because the basic purpose here is to circulate a bunch of queries and emote a horrid load of responses thereby saturating the network of the victim [2].

vi. **Ping of Death Attack:** In ping of death, ping packets with larger than anticipated packet size are used as a technique of assault. This is done, for example by adjusting the size of the data packet to exceed the limit allowed to the target system causing it to hang or crash. This last case is what used to happen a long time ago because all known systems now have ways of preventing this method of attack which tends to target the IP layer [3].

vii. **Teardrop Attack:** In a teardrop attack, the attackers take advantage of fragmentation by breaking messages into packets. For example, instead of waiting for a complete packet, with appropriately arranged offset values, the attackers force the system to have packets with the same offset values. Such an attack compromises the reassembly of packets which is a function under the transport layer making the system handle nonconforming packets poorly [3].

viii. **Infrastructure Attack:** Infrastructure attacks devastate to a higher magnitude as they target cardinal parts of the internet topography like the DNS root servers or major service providers. For instance, the Dyn DNS attack of October 2016 disabled some leading organizations such as Netflix, Twitter, and LinkedIn. These are the types of attacks that tend to cripple major services by targeting and flooding the main infrastructure of the internet, and as a result causing blackouts [2].

**Prevention of DDoS Attacks**

Distributed Denial of Service attacks pose a continuous threat to network infrastructures, as they involve overwhelming a networked system by sending significant amounts of requests. Various DDoS detection and mitigation techniques have been developed to identify and mitigate DDoS attacks using analysis of the traffic over the network and identifying abnormal behaviors. The following summarizes several modern techniques for DDoS prevention.

i. **Correlation analysis with K-Nearest Neighbors (KNN):** KNN is a machine learning technique leveraged to identify anomalies in network traffic behaviors. KNN evaluates specific features such as the rates of packets sent, or the frequency of requests sent and identifies abnormal clusters of connections. If a group of data points (representing active network connections) demonstrate similar anomalous actions, they are likely hosting a coordinated attack. KNN quickly computes the distance among features of the identified traffic for these types of irregularities [7].

ii. **One-Class Support Vector Machine (OC-SVM):** OC- SVM works similarly to KNN but with the goal of learning the normal patterns in the traffic on the network itself. Once the OC-SVM processes the normal actions for traffic, it can flag any behavior that deviates significantly from this model which could be a sign of a DDoS attack attempt [7].

iii. **FlowGuard:** A lightweight means of buffering DDoS attacks, FlowGuard is specifically designed for the constrained interface of Internet of Things (IoT) applications. FlowGuard studies the traffic flow on the network and identifies any unusual activity (such as an inordinate amount of traffic from a single source) which could be symptomatic of an impending DDoS attack [7].

iv. **Discrete Cosine Transform (DCT):** the DCT has been primarily applied in recognizing internal DDoS attacks by examining the CPU usage of virtual machines (VMs) in the cloud. The DCT simplifies finding abnormal relationships between CPU usages by transforming their CPU utilization into a transformed/intermediate domain [7].

v. **Host-based Intrusion Detection Systems (HIDS) and Network-based Intrusion Detection Systems (NIDS):** the HIDS and NIDS systems identify potential DDoS attacks by investigating network and host-level activities. The HIDS focuses on activities on a specific device,which includes identifying suspicious changes to files, while the NIDS examines traffic pattern behavior on the network from multiple devices by searching for expectedpatterns, prominently looking for surges of activity froma single IP address [7].

vi. **Intrusion Prevention Systems (IPS):** IPSs monitor traffic for evidence of DDoS attacks and provide protection to the server on a real-time basis by blocking or throttling traffic based on existing security policies and rules. The framework of the IPS enables it to detect behavior suggesting DDoS activity and to begin to block or limit exposure to traffic from a designated source of the attack [7].

vii. **SOA-Based Traceback Approach (SBTA):** SBTA is predicated on the ability to traceback attack traffic to its source through service requests across the network. The traceback function, once attained, can then be initiated to inhibit source traffic [7].

viii. **Deep Learning Techniques:** CNN and LSTM models have been utilized for DDoS detection. CNNs and LSTMs model rapidly analyze large volumes of network data, ultimately learning to differentiate between malicious and normal traffic patterns; CNN and LSTM models inherently recognize measurable changes across networks that indicate a distributed denial of service [7], [9].

ix. **Hybrid Approach for Low-Rate DDoS Detection (HA- LRDD):** The HA-LRDD examination is the first of its kind to combine deep learning and statistical analysis to detect low-rate DDoS attacks, which are considered harder to detect. This method includes identifying features, utilizing autoencoders to perform anomaly detection, and finally classifying the traffic with Convolutional Neural Networks (CNNs) to create a thorough approach to unveil the stealthier forms of DDoS attacks [8].

x. **Dynamic Low-Rate DDoS Attack Mitigation (DLDM):** In response to a low-rate DDoS attack the DLDM approach varies the network's configuration. This approach maintains critical services during a DDoS attack by rerouting traffic to a safer environment, such as avoiding a network or a region, or blocking traffic from suspicious sources [8].

xi. **Shannon's Entropy:** Entropy analysis of network traffic examines the knowledge content that ranges from order/organization to disorder, indicating randomness. During DDoS events, the request patterns are often perfectly predictable for extended periods, resulting from a large number of requests of the same types. In such cases, an attack may be identified when entropy levels, or values, deviate significantly from observed baseline data [8].

**Mitigation of DDoS Attacks**

While prevention techniques are the most desirable method to deal with DDoS attacks, due to the rapidly evolving environment of cyber-attacks, it cannot be the only defense. The next phase in defense against DDoS techniques can be broken down into three different mechanisms: **detection, response** and **tolerance mechanisms.**

### Detection Mechanisms

Identification of DDoS attacks is critical in the context of mitigation. There is a need to segregate normal and malicious traffic so that the victim can deal with the attack.

a. **Snort:** Snort is a lightweight NIDS that allows content pattern matching using rule-based logging, letting it identify a wide range of attacks and probes, including buffer overflows, stealth port scans, CGI-based exploits, and SMB probes. It is capable of detecting TCP SYN flood attacks by recognizing an unusually high volume of SYN packets without the corresponding ACK responses [10].

b. **Suricata:** Suricata is a high-performance engine that functions as a NIDS, Network Security Monitoring tool and an Intrusion Prevention System (IPS). It is open-source and maintained by the Open Information Security Foundation (OISF), a community-driven non-profit organization. Suricata can detect DDoS attacks by analyzing network traffic and matching it to known attack patterns, such as an unusually high number of HTTP requests or malformed packets [11].

c. **Arbor Networks TMS:** Arbor Networks TMS uses signature-based detection for mitigating DDoS attacks. It compares network traffic against a database of known DDoS attack signatures and flags traffic that matchesthese patterns. It can detect volumetric DDoS attacks likeDNS amplification by recognizing excessive DNS response traffic to specific IP addresses [12].

d. **Bro:** Bro is a real-time Network Intrusion Detection System that detects intruders by monitoring network traffic. It offers several advanced features, including a signature language based on regular expressions, a strong attack detection mechanism, and flexibility for extending capabilities to handle new events. However, Bro can be vulnerable to Denial-of-Service (DoS) attacks that exploit algorithmic complexity. Additionally, it requires the user to manually create attack signatures and event-handling scripts, making it essential to have an expert administrator manage and configure the system effectively [13].

e. **MULTOPS:** MULTOPS is a DDoS detection mechanism that monitors packet rates using a multi-level tree structure. It detects DDoS attacks by identifying significant imbalances in traffic, such as a high volume of incoming traffic to a server that is not matched by outgoing traffic. During a DDoS attack, the system expects the ratio of incoming to outgoing packets to deviate from normal levels because the victim server is overwhelmed with requests but cannot respond to them all [14].

f. **D-WARD:** D-WARD is a source-end defense mechanism deployed at the edge routers of an Internet Service Provider to monitor and control outgoing traffic from a network. It detects DDoS attacks by examining the flow of traffic leaving the network. It compares the traffic patterns of outgoing flows with predefined normal behavior models. If the system identifies a large discrepancy between the number of requests received and the number of responses sent, it assumes that the network is participating in an attack. It can also help in identifying attack sources [15].

g. **Threshold based detection:** Threshold based detection involves setting up predefined thresholds for network traffic metrics such as packet rate, connection rate and bandwidth usage. If any of these statistics exceed these thresholds, an alarm is triggered [16].

h. **Entropy based detection:** Entropy-based methods measure the randomness or uniformity of network traffic distributions, such as IP addresses, packet sizes, or port numbers. A drop in entropy implies an increase in uniformity of traffic, which could signify a DDoS attack [17].

i. **Machine learning based detection:** Machine learning models trained on normal network behavior can use unsupervised learning techniques to detect deviations. Algorithms such as clustering, decision trees, or neural networks can be used to detect DDoS attacks [18].

### Attack Source Identification

Identifying the source of DDoS attacks is the next step in mitigation. Several mechanisms and approaches have been developed to trace back and identify the origin of attack traffic.

a. **Packet marking:** This is a traceback method where the route of the packet is traced, and its origin can be retrieved by the victim. The route can be traced by gathering the identification information of each router that is attached to the packet, thus allowing the victim to reconstruct the path of the packet. Routers can either mark packets probabilistically with partial path information, or deterministically with the router's own identification information. This is especially useful in resolving spoofed addresses [19].

b. **Hop-by-Hop IP Traceback:** In this method, each router logs incoming and outgoing traffic. Upon request from the victim, the router can trace back the path of the packet hop by hop, reaching the attack source this way. This method is particularly useful for volumetric attacks like SYN floods [20].

### Response and Tolerance

a. **DDoS response mechanisms** aim to mitigate the impact of an attack by detecting malicious traffic, protecting resources, and restoring normal operations.Rate Limiting or Filtering is one of the most convenient ways to respond to DDoS attacks. Generally, if a detection mechanism is known to be more accurate, it is more efficient to filter the malicious traffic. However, if a detection mechanism is found to be partially successful or if it produces a lot of false negatives, it is reasonable to apply rate limiting rather than filtering [2].

b. **Tolerance mechanisms** are an alternative to when prevention and detection techniques fail. Since it is the final stage of defense, the purpose of this mechanism is to provide maximum quality of service by minimizing the impacts of the attacks. Tolerance can be achieved by introducing congestion policies, or by increasing the fault tolerance of the resource that is being attacked [2].

## COMPARATIVE STUDY AND ANALYSIS

### Survey Data of Previous Attacks

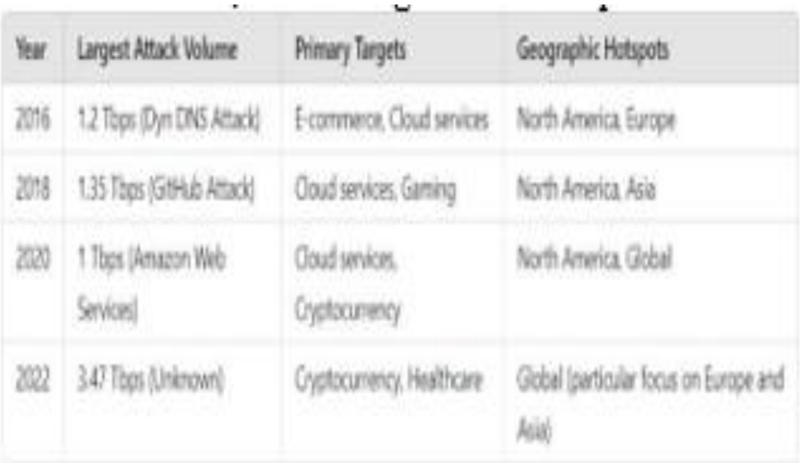
DDoS attacks have surged in both frequency and severity, with significant survey data illustrating these trends. Various surveys and reports offer insights into the scale and impact of these attacks.

i. **Attack Frequency and Volume:** According to Arbor Networks, there has been an exponential rise in DDoS attacks exceeding 1000 Gbps. The largest recorded attack occurred in October 2016 during the Dyn DNS attack, which reached 1.2 Tbps. More recently, GitHub experienced an even larger attack in 2018, with traffic volumes reaching 1.35 Tbps.

ii. **Geographic Distribution and Targets:** A report by Kaspersky Lab shows that e-commerce platforms, followed by cloud-based services, have been the primary targets of DDoS attacks. However, gaming platforms and cryptocurrency exchanges are increasingly becoming victims due to their reliance on real-time, high-availability services.

iii. **Financial Impact:** The Ponemon Institute's report estimates that the cost of a DDoS attack can range from $22,000 to $100,000 per minute for larger organizations. The financial toll extends beyond just immediate revenue loss, encompassing legal costs, customer churn, and damage to brand reputation.

***Table 3: DDoS Attack Trends by Year***



| Year | Largest Attack Volume | Primary Targets | Geographic Hotspots |
|---|---|---|---|
| 2016 | 1.2 Tbps (Dyn DNS Attack) | E-commerce, Cloud services | North America, Europe |
| 2018 | 1.35 Tbps (GitHub Attack) | Cloud services, Gaming | North America, Asia |
| 2020 | 1 Tbps (Amazon Web Services) | Cloud services, Cryptocurrency | North America, Global |
| 2022 | 3.47 Tbps (Unknown) | Cryptocurrency, Healthcare | Global (particular focus on Europe and Asia) |

### Analysis of Mitigation Techniques

This section provides an analysis of the mitigation techniques presented in the literature review section. It will include the most effective techniques used to combat every DDoS attack type.

**i.** **Snort:** Snort is the most effective at detecting flooding DDoS attacks, such as UDP floods, ICMP floods, Ping floods, SYN floods, HTTP floods and DNS Amplification attacks.

**Limitations:** Snort has limited effectiveness against zero-day DDoS attacks and attack vectors beyond the signatures it is configured for. Additionally, some volumetric attacks where the sheer volume overwhelms the bandwidth might be beyond Snort's capabilities. Performance of Snort also depends on the quality of the rules configured by the user, and thus may face problems regarding false positives due to user error. Snort involves analyzing all network traffic, which leads to poor scalability and high-performance costs.

**ii.** **Suricata:** Suricata is well versed in detecting and mitigating application layer attacks such as HTTP floods. Due to its high performance and muti- threading capabilities, it can handle large volumetric attacks effectively.

**Limitations:** Suricata is a complex rule-based system, thus requires careful configuration to avoid false positives and is not optimal for new users that cannot handle complexity. Despite it being designedfor high performance, scaling it to large or high- speed networks will present challenges, requiring careful tuning and optimization.

iii. **Arbor Networks TMS:** Arbor TMS has very advanced analysis and mitigation capabilities, allowing it to be highly effective in dealing with a wide range of attacks such as volumetric, protocol based and application layer attacks.

**Limitations:** Arbor TMS is a commercial product, which is a great limitation for companies with a limited budget and can lead to vendor lock-in due to its proprietary nature. It is also very complex in nature to configure and requires substantial infrastructure and hardware resources to set up.

iv. **Bro:** Bro integrates well with other security tools and systems, leading to better anomaly detection. Its detailed analysis capabilities make it very effective at identifying and mitigating application-layer attacks such as HTTP floods and DNS based attacks.

**Limitations:** Due to the in-depth nature of Bro's analysis, it can introduce a substantial performance overhead. It is also quite complex to set up, and while its detection abilities are significant, it is not a dedicated mitigation tool and works best when paired up with other solutions that can provide much needed features such as automated traffic filtering. It may also face challenges when scaled to large or high- speed networks.

v. **MULTOPS:** MULTOPS is well suited formitigating volumetric attacks due to its ability to apply appropriate filters. These adaptive filtering capabilities are also useful for handling protocol- based attacks.

**Limitations***:* MULTOPS is very complex to configure, and this complexity extends to scaling its system, requiring careful tuning and optimization. It is a very specialized solution, and thus may involve substantial costs for implementation and maintenance. MULTOPS is also very difficult to integrate with existing network infrastructure andwill require additional effort to ensure compatibility and efficiency.

vi. **D-WARD:** D-WARD is effective in dealing with web-based attacks such as HTTP floods and other application layer attacks. It is proficient at managing and controlling traffic, allowing it to be efficient at mitigating attacks aiming to deplete resources such as CPU, memory and bandwidth.

**Limitations:** D-WARD is focused on primarily dealing with web application protection and might not be suitable for defending against DDoS attacks targeting other parts of a network's infrastructure. D-WARD also requires expertise to configure properlyand can result in poor scalability and performance overheads if not properly optimized.

vii. **Threshold-based Detection:** Threshold-based detection is extremely straightforward to set up, only needing definition of traffic thresholds, that, when exceeded, indicate a potential attack. It is easy to scale up and is very convenient to integrate into existing security systems. It is good at detecting volumetric and flooding attacks.

**Limitations:** Threshold-based detection is very suspectable to false positives or negatives due to its simplicity. Due to the thresholds being static, it will not be able to adapt to varying network conditions, leading to either excessive alerts or missed attacks. It is challenging to use in dynamic scaled up environments due to its limited contextual awareness and requires continuous adjustment to maintain effectiveness in large or high-speed traffic conditions.

viii. **Entropy-based Detection:** Entropy-based detection is most useful in unpredictable environments, causing it to be very useful in detecting novel or unknown attacks such as zero-day DDoS attacks, as it focuses more on deviating traffic patterns rather than specific attack signatures. Certain attacks such as HTTP floods which cause traffic patterns to become more random can also be detected using this mechanism

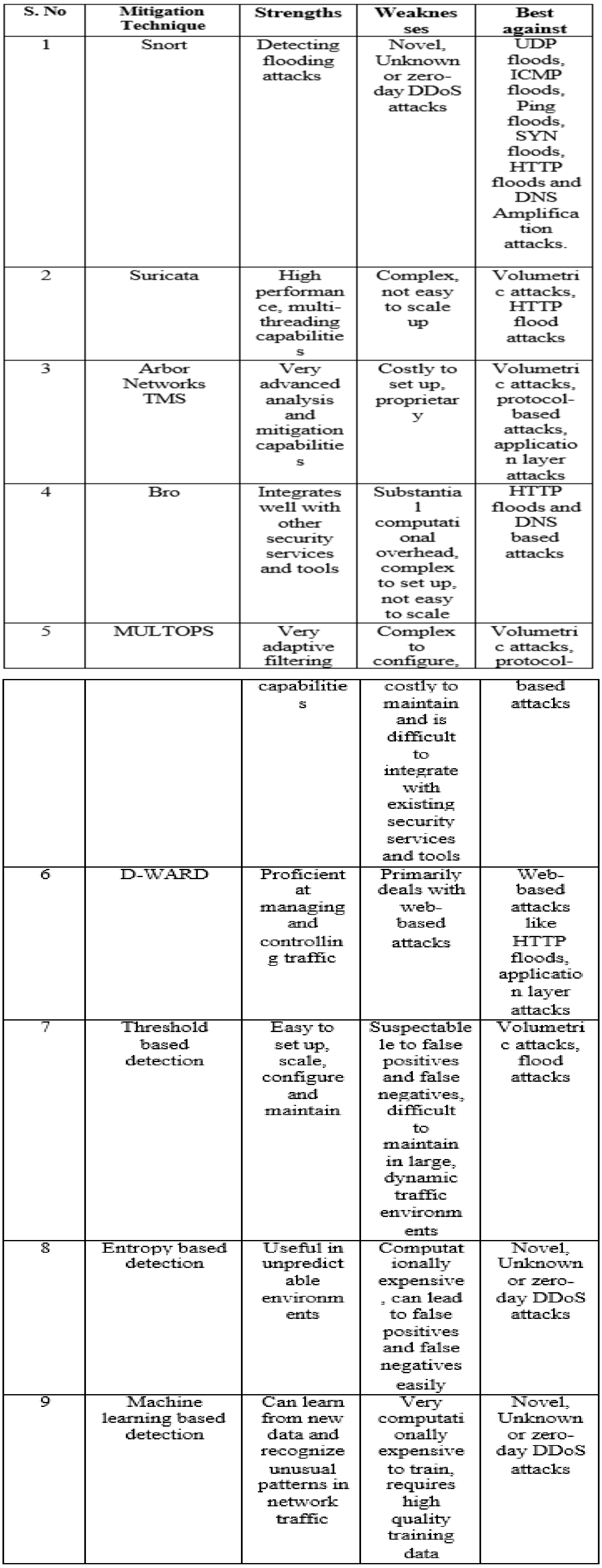
**Limitations:** Entropy-based detection is very complex to set up and using improper threshold sensitivities may lead to lack of accuracy of the detection. Normal traffic deviations may be misinterpreted as anomalies, leading to false positives and if attack traffic does not significantly deviate in terms of entropy, it may lead to false negatives. Calculating entropy is also a computationally expensive task which can consume a lot of system resources to do so.

ix. **Machine Learning based detection:** Machine learning based detection mechanisms are effective in dealing with sophisticated application layer attacks by analyzing complex traffic patterns. It also excels in identifying novel and unknown attacks by learning from new data and recognizing unusual patterns.

**Limitations:** A machine learning model heavily relies on the quality of its training data. Inadequate or biased data can lead to inaccurate detection and poor performance. Implementing and fine tuning such models is a complex and computationally expensive task, which can cost a lot of time and resources to properly set up.

Following is a table summarizing all above methods along with their strengths, weaknesses and the type of DDoS attacks they are most effective at countering.

*Table 4: Summary of DDoS mitigation techniques*



| S. No | Mitigation Technique | Strengths | Weaknesses | Best against |
|---|---|---|---|---|
| 1 | Snort | Detecting flooding attacks | Novel, Unknown or zero-day DDoS attacks | UDP floods, ICMP floods, Ping floods, SYN floods, HTTP floods and DNS Amplification attacks. |
| 2 | Suricata | High performance, multi-threading capabilities | Complex, not easy to scale up | Volumetric attacks, HTTP flood attacks |
| 3 | Arbor Networks TMS | Very advanced analysis and mitigation capabilities | Costly to set up, proprietary | Volumetric attacks, protocol-based attacks, application layer attacks |
| 4 | Bro | Integrates well with other security services and tools | Substantial computational overhead, complex to set up, not easy to scale | HTTP floods and DNS based attacks |
| 5 | MULTOPS | Very adaptive filtering capabilities | Complex to configure, costly to maintain and is difficult to integrate with existing security services and tools | Volumetric attacks, protocol-based attacks |
| 6 | D-WARD | Proficient at managing and controlling traffic | Primarily deals with web-based attacks | Web-based attacks like HTTP floods, application layer attacks |
| 7 | Threshold based detection | Easy to set up, scale, configure and maintain | Suspectable le to false positives and false negatives, difficult to maintain in large, dynamic traffic environments | Volumetric attacks, flood attacks |
| 8 | Entropy based detection | Useful in unpredictable environments | Computationally expensive, can lead to false positives and false negatives easily | Novel, Unknown or zero-day DDoS attacks |
| 9 | Machine learning based detection | Can learn from new data and recognize unusual patterns in network traffic | Very computationally expensive to train, requires high quality training data | Novel, Unknown or zero-day DDoS attacks |

## FUTURE DIRECTION OF RESEARCH

Future research in DDoS attack mitigation needs to focus on a multifaceted approach, encompassing advanced technologies like machine learning, blockchain, Software-Defined Networks (SDNs), cloud computing, and the Internet of Things (IoT). Enhancing current machine learning models for real-time detection and mitigation remains crucial. Integrating deep learning techniques with anomaly-based detection systems could improve the accuracy of differentiating between legitimate and malicious traffic. Further research into federated learning can foster collaborative defenses by training models across multiple organizations without compromising privacy.

Blockchain technology presents another promising direction, offering the potential to build decentralized and secure network architectures. Its features of immutability and transparency can be harnessed to protect against DDoS attacks by using distributed ledgers for secure communication between nodes, minimizing single points of failure. Exploring smart contracts for automated detection and mitigation could add an extra layer of security. However, the scalability and latency issues inherent in blockchain-based systems would need to be thoroughly addressed for practical implementation in real-time environments.

SDNs, with their centralized nature, remain vulnerable to targeted DDoS attacks, highlighting the need for new research on hardening SDN controllers. Lightweight in-switch defense mechanisms developed using languages like P4, and the implementation of adaptive, self-healing networks could enhance SDN resilience. A hybrid model that combines AI-driven traffic analysis with decentralized control mechanisms may further strengthen the defense against evolving threats.

Finally, research into cloud-based and IoT-specific defense mechanisms is vital. In cloud environments, dynamic, real-time resource allocation models using serverless computing and container orchestration can provide scalable responses to sudden surges in malicious traffic. For IoT ecosystems, lightweight security protocols and collaborative defense frameworks between devices are essential for enhancing detection and response capabilities. Future work should focus on developing adaptive, context-aware security models tailored for these diverse environments, creating a robust and proactive defense against complex DDoS attacks

## CONCLUSION

Distributed Denial of Service (DDoS) attacks remain a persistent and evolving threat to network security and online services. This article has provided a detailed analysis of the various types of DDoS attacks, their underlying motives, and their significant impacts on sectors like government, finance, and gaming. We examined multiple mitigation strategies, ranging from traditional methods to advanced technologies like machine learning, blockchain, and cloud-based defenses. Although these techniques offer promising solutions, attackers constantly adapt their methods,
challenging the efficacy of current defenses.

Given the evolving nature of DDoS threats, it is evident that a multi-layered, dynamic approach is necessary. Effective mitigation requires the integration of real-time monitoring, adaptive resource allocation, and proactive threat intelligence. Collaboration between stakeholders, continuous research, and innovation are also essential to develop more comprehensive strategies. As cyber attackers continue to evolve, the future of DDoS defense lies in flexible, adaptive solutions capable of responding promptly to emerging threats, ensuring the resilience and security of critical network infrastructures.

## ACKNOWLEDGMENT

The authors thank Dr. SIVAKUMAR V for their invaluable guidance and support throughout the preparation of this review article. Appreciation is further extended to the Vellore Institute of Technology for providing a platform for convenient access to essential resources and research materials that contributed greatly to the successful completion of this assignment.

## REFERENCES

[1] Denial-of-service attack – Wikipedia: https://en.wikipedia.org/wiki/Denial-of-service_attack

[2] Mahjabin T., Xiao Y., Sun G., Jiang W. A survey of distributed denial-of-service attack, prevention, andmitigation techniques Int. J. Distrib. Sens. Netw., 13 (12) (2017): https://journals.sagepub.com/doi/epub/10.1177/1550147717741463

[3] Distributed denial of service attack prediction: Challenges, open issues and Opportunities: https://doi-org.egateway.vit.ac.in/10.1016/j.comnet.2022.109553

[4] ENISA THREAT LANDSCAPE 2021 October 2021:https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

[5] Netscout Threat Intelligence report: https://www.netscout.com/threatreport

[6] AWS Shield is a managed threat protection: https://aws-shield-tlr.s3.amazonaws.com/2020-Q1_AWS_Shield_TLR.pdf

[7] S. Kumar, M. Dwivedi, M. Kumar, and S. S. Gill, "A comprehensive review of vulnerabilities and AI-enabled defense against DDoS attacks for securing cloud services," Compter Science Review, vol. 53, Aug. 2024. [Online]. Available: C. Modi, D. Patel, B. Borisaniya, A. Patel, and M. Rajarajan, "A survey of intrusion detection techniques in cloud," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 42-57, Jan. 2013.

[8] https://doi-org.egateway.vit.ac.in/10.1016/j.cosrev.2024.100661

[9] M. Jahir Pasha, K. Prasada Rao, A. Malla Reddy, and V. Bande, "LRDADF: An AI enabled framework for detecting low-rate DDoS attacks in cloud computing environments," *Measurement: Sensors*, vol. 28, p. 100828, Aug. 2023. Available: https://doi- org.egateway.vit.ac.in/10.1016/j.measen.2023.100828

[10] B.Bala, S.Behal, "AI techniques for IoT-based DDoS attack detection: Taxonomies, comprehensive review and research challenges", Computer Science Review, vol.52, Mar. 2024. [Online]. Available: https://doi-org.egateway.vit.ac.in/10.1016/j.cosrev.2024.100631

[11] M. Roesch, "Snort: Lightweight intrusion detection for networks," in Proceedings of the 13th USENIX Conference on

System Administration (LISA '99), Seattle, WA, USA, 1999, pp. 229-238.

[12] Suricata Project, "What is Suricata," *Suricata Documentation*, Suricata, accessed Sep. 16, 2024. [Online]. Available: https://docs.suricata.io/en/suricata-7.0.2/what-is-suricata.html.

[13] NETSCOUT, "Arbor Threat Mitigation System (TMS),"*NETSCOUT*, accessed Sep. 16, 2024. [Online]. Available: Paxson V. Bro: a system for detecting network intruders in real-time. Comput Netw 1999; 31(23): 2435–2463.

[14] https://www.netscout.com/sites/default/files/2018- 10/SECPDS_004_EN-1802-Arbor-Threat-Mitigation-System-%28TMS%29.pdf.

[15] M. Gil and M. Poletto, "MULTOPS: A data-structure for bandwidth attack detection," in *Proceedings of the 10th USENIX Security Symposium*, Washington, DC, USA, 2001.

[16] J. Mirkovic and P. Reiher, "D-WARD: A source-end defense against flooding denial-of-service attacks," *IEEE Transactions on Dependable and Secure Computing*, vol. 2, no. 3, pp. 216-232, July- Sept. 2005.

[17] L. Feinstein, D. Schnackenberg, R. Balupari, and D. Kindred, "Statistical approaches to DDoS attack detection and response," in*Proceedings of the DARPA Information Survivability Conference and Exposition*, Washington, DC, USA, 2003

[18] A. Lakhina, M. Crovella, and C. Diot, "Mining anomalies using traffic feature distributions," in *Proceedings of ACM SIGCOMM*, Philadelphia, PA, USA, 2005, pp. 217-228.

[19] S. Savage, D. Wetherall, A. Karlin, and T. Anderson, "Practical network support for IP traceback," in *Proceedings of ACM SIGCOMM*, Stockholm, Sweden, 2000, pp. 295-306.

[20] A. C. Snoeren, C. Partridge, L. A. Sanchez, C. E. Jones, F. Tchakountio, S. T. Kent, and W. T. Strayer, "Single-packet IP traceback," *IEEE/ACM Transactions on Networking*, vol. 10, no. 6, pp. 721-734, Dec. 2002.

[21] N. Jyoti and S. Behal, "A Meta-evaluation of Machine Learning Techniques for Detection of DDoS Attacks," *2021 8th International Conference on Computing for SustainableGlobal Development (INDIACom)*, New Delhi, India, 2021, pp. 522-526.

[22] T. -K. Luong, T. -D. Tran and G. -T. Le, "DDoS attack detection and defense in SDN based on machine learning," *2020 7th NAFOSTED Conference on Information and Computer Science (NICS)*, Ho Chi Minh City, Vietnam, 2020, pp. 31-35, doi: 10.1109/NICS51282.2020.9335867.

[23] A. Bendovschi, "Cyber-attacks – trends, patterns and security countermeasures," *Procedia Economics and Finance*, vol. 28, pp. 24-31, 2015. [Online]. Available: https://doi.org/10.1016/S2212-5671(15)01077-1.

[24] Hosam F. El-Sofany, “A New Cybersecurity Approach for Protecting Cloud Services against DDoS Attacks”, International Journal of Intelligent Engineering and Systems, Vol.13, No.2, 2020, DOI: 10.22266/ijies2020.0430.20

[25] N. Singh, H. P. Singh, A. Mishra, A. Khare, M. Swarnkar and S. K. Almas, "Blockchain Cloud Computing: Comparative study on DDoS, MITM and SQL Injection Attack," 2024 IEEE International Conference on Big Data & Machine Learning (ICBDML), Bhopal, India, 2024, pp. 73-78, doi: 10.1109/ICBDML60909.2024.10577412.

[26] Sivakumar V., Swathi R., Yuvaraj V. (2022). "Writing Machine for Blind People." Assistive Technologies for Differently Abled Students, edited by Sangeeta Dhamdhere and Frederic Andres, IGI Global, pp. 41-52. https://doi.org/10.4018/978-1-7998-4736-6.ch003

[27] S. Aravind and V. Sivakumar. (2023). "A Survey on Drug Suggestion Mechanisms using Machine Learning Algorithm," 2023 7th International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, 2023, pp. 187-191, doi: 10.1109/ICICCS56967.2023.10142523.

[28] Venu, S. ., Kumar, R. G. ., Kumar, M. K. ., Prasad, T. G. ., Suresh, B. ., & Neelima, P. (2023). An Intelligent and Service Based Smart Agriculture Recommendation System. International Journal of Intelligent Systems and Applications in Engineering, 12(7s), 153–158. https://www.ijisae.org/index.php/IJISAE/article/view/4051

[29] S. Venu and A. M. J. M. Z. Rahman. (2017). Effective routine analysis in MANET's over FAODV, 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI), Chennai, India, pp. 2016-2020, doi: 10.1109/ICPCSI.2017.8392068.

[30] Venu, S., Zubair Rahman, A.M.J.M. Energy and cluster based efficient routing for broadcasting in mobile ad hoc networks. Cluster Comput 22 (Suppl 1), 661–671 (2019). https://doi.org/10.1007/s10586-018-2255-3

[31] M. Zaki, V. Sivakumar, S. Shrivastava and K. Gaurav, "Cybersecurity Framework For Healthcare Industry Using NGFW," 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), Tirunelveli, India, 2021, pp. 196-200, doi: 10.1109/ICICV50876.2021.9388455.

[32] Abusaimeh, H., 2020. Distributed denial of service attacks in cloud computing. International Journal of Advanced Computer Science and Applications, 11(6), pp.163-168.

[33] MAHRACH, Safaa, and Abdelkrim HAQIQ. "DDoS flooding attack mitigation in software defined networks." International Journal of Advanced Computer Science and Applications 11, no. 1 (2020).