International Journal of Computer Trends and Technology
ISSN: 2231–2803 / https://doi.org/10.14445/22312803/IJCTT-V72I12P108

Volume 72 Issue 12, 69-77, December 2024
© 2024 Seventh Sense Research Group®

*Original Article*

# A Survey of Distributed Denial of Service (DDoS) Attack Mitigation Techniques

Rajender Pell Reddy

*Cybersecurity Advisor, Richmond, VA, USA*

*Corresponding Author : Rpellreddy@Gmail.Com*

Received: 30 October 2024 Revised: 24 November 2024 Accepted: 10 December 2024 Published: 29 December 2024

***Abstract*** *- One of the biggest and continuous challenges to the availability of online services currently is Distributed Denial of Service (DDoS) attacks. These attacks seek to deny users and/or network resources access to a specific server, service or network through its inundation with a large number and threatening traffic. Besides making the target system unusable, this leads to tremendous operational and financial losses for organizations. Botnets, amplification attacks, various evasion techniques, etc., are all piling on the pressure as attackers' sophistication increases, meaning traditional security measures are ineffective. Many techniques have been evolved to prevent or mitigate these attacks, such as the simple ones, like rate limiting and IP blacklisting, to the complex techniques, like anomaly-based detection and Machine Learning (ML) models. In this survey, we offer a comprehensive review of DDoS attack mitigation techniques, categorizing them into three key areas: prevention, detection, and actions after the emergence of occurrences. We look into contemporary approaches like real-time anomaly detection systems based on artificial intelligence and distributed defense framework, which seek to counter enormous system-level multi-vector DDoS attacks. Our examination also discusses the effectiveness and working issues related to technique and concentrates on high-level adaptive and scalable techniques for combating threats. Furthermore, we also provide a comparative analysis of these techniques in a tabular and graphical form with the help of figures so that an overall picture of the prevailing situation can be presented accurately. The paper concludes with directions for future research about the areas mentioned above, such as the application of decentralized security utilizing blockchain and the advancement of the integration of machine learning in order to enhance attack prediction and prevention.*

***Keywords*** *- Distributed Denial of Service (DDoS), Mitigation techniques, Detection systems, Anomaly detection, Rate limiting, Machine learning, Cybersecurity.*

## 1. Introduction

Distributed Denial of Service (DDoS) attacks have been recognized as among the most dangerous threats to the availability and integrity of online services. These attacks threaten the availability of network services through the over-flooding of traffic to the target, energy normally sourced from a large number of infected devices called a botnet. The main objective of a DDoS attack is to overwhelm the service capacity of the targeted Systems, including bandwidth, CPU, and memory, so the system is unavailable to the intended user. [1-3] Since the role of the internet expanded to manage the world's economy and communicate and provide public services, the consequences of these attacks have grown exponentially as they target not only ordinary users but also industries, states, and essential facilities.

As attackers adopted more advanced ways of presenting themselves, DDoS attacks have become multi-faceted, having multiple strings to their bow, as it were, to outsmart the traditional security measures that continue to be put in place. Therefore, making components of the CIA triad available is still a major concern cybersecurity specialists face.

### *1.1. Problem Statement*

It is noted that despite the increase in frequency and complexity of DDoS attacks, the current defense mechanisms are not efficient in handling such attacks. In the past, simple solutions like firewalls and rate limiting were enough, but in situations like the current ones, they are usually inadequate. Due to their distributed nature, it is very challenging to distinguish and eliminate malicious traffic while keeping valid users offline. Traditional security measures are overwhelmed by the vast number of these assaults. With this in mind, as the attackers practice better techniques like distributed botnets, traffic spoofing, and multi-vector attacks, the security solutions must also improve their ability to overcome the attackers. The dispersed nature of these attacks, combined with their ability to target different network stack layers, for instance, volumetric, protocol, and application layer, makes the need for advanced, dynamic and intelligent mitigations even more crucial. Today, traditional and unadaptable approaches still put organizations at risk of substantial financial loss, disruption, and, in some cases, even brand degradation.

### *1.2. Objectives*

To this end, this paper will further analyse the various methods available for addressing the menace of DDoS attacks. The first objective is to classify and discuss classic and novel measures against DDoS and to determine how these measures function in all phases of the attack life cycle, namely pre-attack, attack detection, and post-attack. We will compare traditional forms of solutions like rate limiting, IP blacklisting and load balancing with modern complex solutions based on machine learning for anomaly detection and defense based on distributed systems. In this research endeavor, several techniques are analyzed to provide information regarding their effectiveness and inefficiency under various attack conditions. Furthermore, this paper endeavors to discuss the shortcomings and threats of DDoS mitigation techniques in terms of their scalability, response time, and versatility in identifying new types of attacks. Finally, there are specific goals to introduce further research directions that might help to solve these problems and generate new intelligent defense systems.

## 2. Literature Survey

This section presents a brief literature survey on DDoS attack modeling and defense strategies with reference to traditional and novel approaches. [4-8] DDoS mitigation has changed with time due to the advancement in ways attackers use to launch their attacks. Early defense methodologies are quite simple to implement, and while the attack methods became more complex, the members of the cybersecurity community developed complex and composite defense approaches.

### *2.1. Historical Perspective*

As observed at the beginning of the DDoS mitigation, defensive measures were concerned with rudimentary approaches, including rate limiting and configuring firewalls. For example, rate limiting limits the number of requests that can be processed by the server within a given time, thus managing the traffic. Firewalls were used to restrict unauthorized access by using filters where incoming packets must pass through before being allowed to pass into other parts of the network. However, these simple solutions became ineffective as DDoS attacks became more complicated. In 2007, enhanced wit and dexterity were observed in attackers as they started using botnets that are distributed across the world and interconnected to deliver well-coordinated assaults. This distributed nature of attacks also caused problems for rate limiting and firewalls in distinguishing between legitimate and foul traffic. Moreover, traditional secure early detection systems heavily based on differential approaches involving traffic analysis concerning known attack signatures face difficulties in coping with new threats. It was only useful in subduing threats rooted in a previous list and failed to protect the networks from new invasions.

### *2.2. Current Techniques*

Modern mitigation strategies have been developed in response to the increasing complexity of DDoS attacks and can be broadly classified into three categories: proactive, identification and reactive.

#### *2.2.1. Prevention Techniques*

The prevention strategies ensure that improper traffic is prevented from getting into a system in the first instance.

- Rate Limiting has remained a powerful method in controlling the number of requests a server can handle in a given amount of time to avoid system overload.
- Another type of traffic block is source IP Blacklisting – the process of limiting traffic coming from certain dangerous IP addresses. However, this method is proactive, and it needs the recently collected information on the contaminated IPs and is prone to IP spoofing.
- Network Access Control (NAC) is applied to restrict or permit the connection of different networks by filtering the traffic from certain IP addresses to ensure invalid traffic never gets to the server. However, these techniques are less effective in DDoS attacks, especially those from a large group of Internet clients.

#### *2.2.2. Detection Techniques*

Detection strategies aim at detecting and setting up alerts each time suspicious traffic seeks to interfere with the services provided.

- The second one is called Signature-based Detection, which identifies the traffic patterns and checks them against a database of attack signatures. Although this method is rather effective for identifying well-known attacks, it cannot detect new and emerging threats.
- Moving further in consideration of the approaches, Anomaly-based Detection can be considered as searching for deviations from normal traffic behavior. This makes a profile of normal traffic used to raise alarms when variations from typical traffic happen, making it possible to uncover new attacking techniques. However, it can lead to several ‘false alarms’, making otherwise normal traffic appear malicious.
- The last approach is Machine Learning-based Detection, where the traffic is automatically classified as normal and malicious. These models are trained from large data sets and are capable of learning from new manifestations of attack in future. Thus, despite the fact that similar to anomaly-based systems, ML-based systems can generate higher false positive rates, we have to note that the further development of the given approach makes for the creation of highly adaptive and precise DDoS detection systems with fewer false positives as compared with anomaly-based systems because the given systems improve with new data.

#### *2.2.3. Response Techniques*

Response procedures are used to counter the detected attack, while containment procedures aim at minimizing the effects caused by the attack on the targeted network or system.

- Traffic Filtering is the process of blocking fake traffic while, on the other side authentic traffic is allowed to get through. This can be achieved through firewalls or Intrusion Prevention Systems (IPS), which analyze packets and make decisions based on prescribed rules or otherwise in real-time.
- Load balancing is the other method employed to ensure that the flow of traffic received by a certain server is demisted onto different servers to ensure maximum pressure is not applied on one server. This not only assists in dealing with the attacks based on volume but also checks that the services are running as they should during the attack.
- Redirection Techniques involve filtering out or redirecting to decoy servers or honeypots, as they are referred to, all the suspicious or malicious traffic with the intent to analyze them and neutralize them while allowing the real server to operate normally.

### *2.3. Emerging Trends*

Modern technological advances are characterized by new and sophisticated techniques of handling DDoS.

- Machine Learning (ML) and Artificial Intelligence (AI) are now the essential requirements for a contemporary approach to DDoS protection. As with the AI and ML algorithms demonstrated in the paper, they can always autonomously learn new types of attacks from the network traffic data. While doing so, they improve their capability to differentiate between normal and threatening traffic accurately, providing dynamics instead of the mostly rigid approaches. One of the biggest advantages of the AI-driven system is its capability to analyze and counter the attacks in real-time based on their dynamics; this makes such systems very useful in combating large-scale, dynamic DDoS attacks.
- Blockchain-based Defense is a new trend that uses blockchain technology's distributed character for traffic confirmation. Blockchain can be used to manage trust for nodes in a network as it makes it difficult for a third party to interfere while recording traffic sources. This approach provides a workable solution to central bottlenecks, usually targeted in DDoS. When the verification process is conducted across a huge network, the blockchain systems can enhance the level of security on a large-scale attack.
- The Collaborative Defense Mechanisms refer to a case whereby several nodes or systems are in harmony and complementary to counter DDoS. These distributed systems work coordinated, sharing intelligence and data and reducing the time needed to detect and respond. Cooperation between different network providers and other participating cybersecurity organizations can contribute to a better overall defense since all the participants are interested in detecting attack traffic and further analysis to improve mitigation strategies.

Altogether, the above points advance DDoS mitigation since they indicate the progressive path of DDoS technologies, which are more complex, scalable, and intelligent in overcoming the existing problems of modern DDoS attacks.

## 3. Methodology

This section captures the systematic method used in the survey and analyzes distributed denial of service (DDoS) mitigation techniques. [9-13] This paper sets out a systematic approach towards data collection and analysis to provide a systematic literature review of the various approaches and techniques used for DDoS attacks, emphasising their efficiency and feasibility for future development.

### *3.1. Distributed Denial of Service Attack*

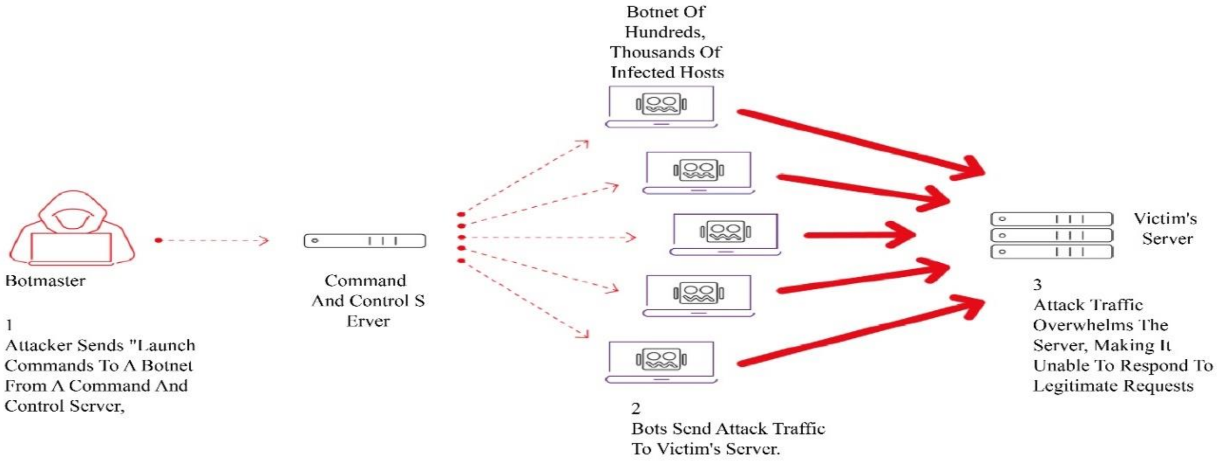

**Fig. 1 Distributed denial of service attack**

**Table 1. Summary of key papers on DDoS mitigation techniques**

| Technique Category | Number of Papers | Example Techniques |
|---|---|---|
| **Prevention** | 20 | Rate Limiting, IP Blacklisting |
| **Detection** | 25 | Anomaly Detection, Machine Learning Models |
| **Response** | 15 | Load Balancing, Traffic Filtering |

### *3.2. Research Approach*

In order to provide a comprehensive and fair analysis of the available DDoS mitigation methods, we organized our research process systematically. The applied method included the analysis of the paper's technical reports and white papers published between 2010 and 2024. This enabled us to capture basic techniques and recent developments within the selected time frame. We performed a cross-search on electronic databases such as IEEE Xplore, ACM Digital Library, and ScienceDirect to access the needed articles. Such platforms were selected because they contain large amounts of articles from peer-reviewed sources and technical studies on cybersecurity. The following keywords were used to search content: DDOS attack, mitigation techniques, DDoS detection by machine learning, distributed defense, and scalable security solutions; the chosen keywords were aimed to reduce the amount of irrelevant information and provide the focus on the topic of DDoS mitigation. Besides, for more grounded and empirically informed results, we included the analysis of industry whitepapers and technical reports of cybersecurity companies. Using academic and industrial sources of information offered DDoS mitigation techniques using a combination of theoretical and actual practice developments.

### *3.3. Data Collection*

In the spontaneous search, it was found that there was plenty of material, including over a hundred research articles, technical papers, and white papers that focused on numerous DDoS mitigation strategies. To filter our choice, we used relevance criteria to find articles that covered only prevention, detection, or response strategies. Experimental papers reporting their work in the form of quantitative results, new algorithms/techniques, and comparative studies of existing methods were deemed more valuable. Therefore, 60 papers were chosen for the analysis out of 141 papers concerning key findings. Table 1 summarises papers based on the type of mitigation technique presented in the papers. All these papers were assessed according to the authors' findings, their view on DDoS, and the techniques discussed. This structured review allowed us to categorize the techniques into three broad categories: promotion of prevention, early identification and effective response. Methods of prevention are to prevent or, to a certain extent, to filter out the incoming malicious traffic; methods of detection are to identify the incoming malicious traffic and to set the alarm bells ringing; response methods are to lessen or minimize the effects of the ongoing attacks.

### *3.4. Evaluation Metrics*

Since it was important for us to identify the effectiveness of different approaches to DDoS mitigation systematically, we defined the following key criteria for comparison. [17,18] These metrics are well defined in the literature in relation to the ability of any security system against DDoS attack performance measurements.

#### *3.4.1. Detection Accuracy*

It calculates the system's success rate and accuracy in identifying DDOS attacks. High detection accuracy implies the system will effectively detect unwanted traffic from normal traffic. For the same reason, any defensive action has to minimize the number of unnoticed attacks, which can lead to extended periods of system unavailability or drain all available resources.

#### *3.4.2. False Positives*

The raw traffic passing through the detection system falls within false positives but is not part of the malicious traffic. False positive results increase security threats and generate low effectiveness and utilization of the system since genuine users are locked out from services, they are legally authorized to access. A good mitigation strategy has the potential to reduce false positives while at the same time improving the level of detection accuracy.

#### *3.4.3. Scalability*

The third aspect is scalability, and this means that the system should have the capacity to support large-scale, distributive, distributed attack traffic. This is so because, as mentioned earlier, DDoS attacks use big botnets to generate huge traffic loads, and a highly scalable system is desirable for combating this type of attack. The system must be able to perform and carry out the detection tasks regardless of the number of incoming attacks.

#### *3.4.4. Response Time*

Availability refers to the time it takes for the mitigation system to identify the assault and the time taken to counter it. Response time is extremely critical as delays in recognizing the attack or even trying to remediate it could affect the availability of services, depletion of resources, and financial losses. This metric is critical in near real-time defense mechanisms, including traffic filtering or load balancing, where action needs to be taken to counter the attack. When using these estimates, we could judge some DDoS mitigation approaches as more effective than others and show the advantages and disadvantages of certain methods under various conditions. Therefore, in addition to concluding which techniques are currently employed to solve the problem most effectively, the process allowed us to determine what gaps in the current literature have not been filled yet.

The application of this methodological framework helps ensure that our survey yields a detailed and balanced assessment of the current practices in DDoS mitigation to pave the way for enhancements and different avenues for research in the future.

## 4. Results and Discussion

The following sub-sections highlight the results of the comparative assessment of DDoS countermeasures discussed earlier in this paper. Our performance metrics include attainable detection accuracy, false positives, scalability and response time. This analysis shows the advantages and limitations of each technique with the help of numerical values and information retrieved from scientific publications.

### *4.1. Comparison Between the Detection Methods*

In evaluating DDoS detection techniques, we compared three major approaches: Signature-based methods, anomaly-based methods, and Machine Learning (ML) based methods. All of these techniques function with different modalities, and in turn, each of them has its unique strengths and weaknesses.

#### *4.1.1. Signature-Based Detection*

The various detection techniques include the following: a) the use of the signature of attack, where the detection is based on the signature of the attack known ahead of time. These signatures are compared to the passing traffic in order to determine which of the threats are. Nevertheless, signature-based methods provide the advantages of a fast response time and good results against known attacks, but they have some disadvantages. The detection success rate for this approach is estimated to be approximately 85%, mainly because of the inability to detect new or zero-day threats. Moreover, when an attack is detected and signatures are used, much legitimate traffic will be flagged as malicious, thus having many false positives. This leads to interruptions with actual users, who, in turn, incur setbacks by testing the application.

Another weakness of signature-based detection is scalability because enhancing and maintaining a large set of attack signatures proves expensive, especially in large networks.

#### *4.1.2. Anomaly-Based Detection*

Anomaly detection systems are far superior to signature-based techniques because such systems analyse normal traffic and check for any variation from the norm, which may be an attack. While the detection accuracy of anomaly-based techniques is 90%, it is higher than that of signature-based methods. Nevertheless, they still have issues, such as a medium level of false positives. If an anomaly detection system is present, such network traffic is classified as malicious when it is not, and services get interrupted. Regarding scalability, these systems are moderately scalable because they are based on data mining of historical information and identifying outliers. If traffic volume scales, the vast amount of collected data requires more computational power to serve users’ requests. The response time for anomaly-based systems is relatively moderate because when a system develops an anomalous behavior, it takes some time to detect and confirm the same as that of signature-based techniques.

#### *4.1.3. Machine Learning-based Detection*

Machine Learning (ML) based techniques are the modern solution to DDoS detection. With huge data sets fed into it, it becomes possible for ML-based systems to be trained to recognize various forms of attacks and even forms of attacks that were hitherto unrecognized. These techniques give the highest detection or identification accuracy, about 95%, and thus can be considered more accurate than the other two techniques. It is also important to note that the presence of ML in systems ensures that the number of false positives is kept to a minimum since the systems can adequately discern the difference between genuine traffic anomalies and real threats.

**Table 2. Comparative Analysis of DDoS Detection Techniques**

| Technique | Detection Accuracy | False Positives | Scalability | Response Time |
|---|---|---|---|---|
| Signature-based | 85% | High | Low | Fast |
| Anomaly-based | 90% | Medium | Medium | Moderate |
| ML-based | 95% | Low | High | Moderate |

**Table 3. DDoS attack targets across different sectors**

| Category | Percentage |
|---|---|
| Online Shopping | 25% |
| Gaming Sites | 20% |
| Stock Exchange | 13% |
| Banks | 11% |
| Adult Content Sites | 8% |
| Blogs and Forums | 8% |
| Mass Media | 7% |
| Transport | 3% |
| Other Business-Related Sites | 3% |
| Government Sites | 1% |
| Other | 1% |

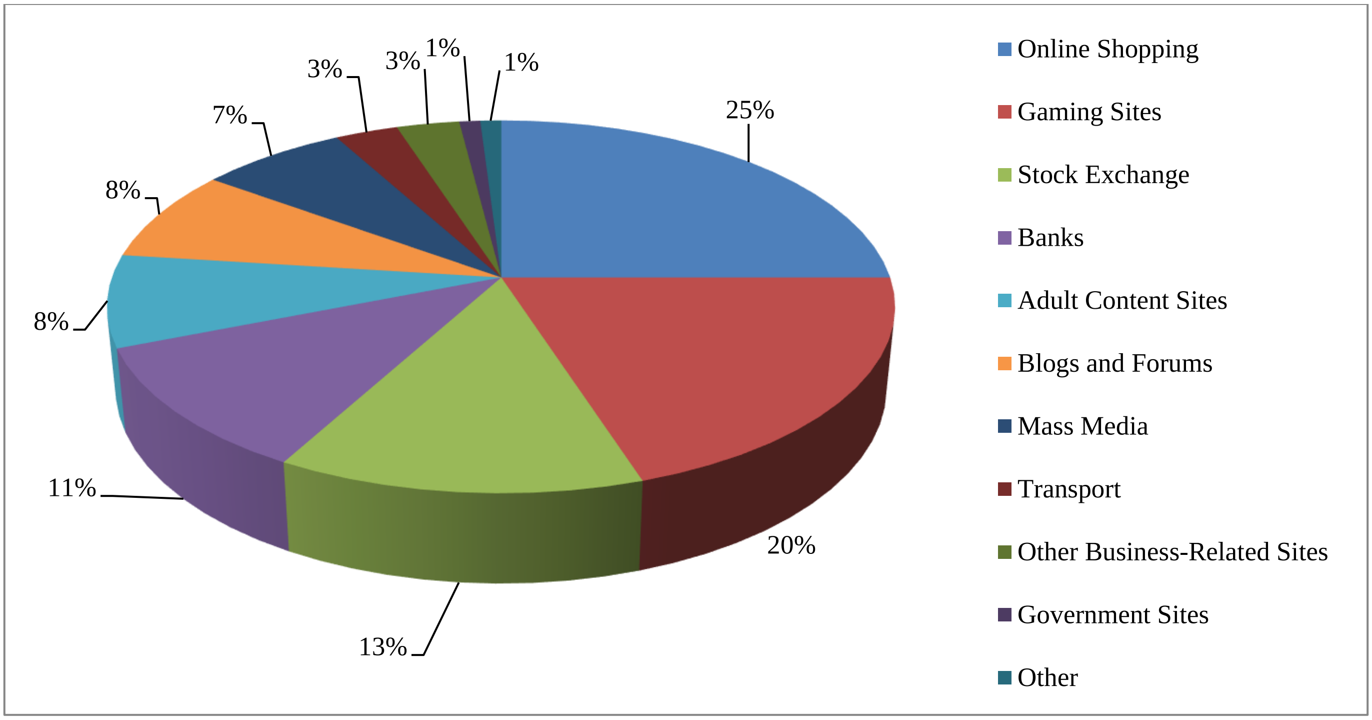

**Fig. 2 Graphical of DDoS attack targets by industry or category**

In terms of scalability, the proposed methods based on machine learning are fully scalable and may need more time and space to process the increasing traffic flow in the network. Despite this, their response time is fair and may be slow when classifying traffic through ML models; traffic takes processing power to be classified. However, they still can adapt to learning so they can refine themselves over time for better security provision. The pie chart in the graphic on the right gives the target industry or category distribution of DDoS attacks. It explains the impact of DDoS attacks on various sectors and the market share of target categories.

### *4.2. Breakdown of the Pie Chart*

#### *4.2.1. Online Shopping (25%)*

According to the frequency, the largest share of acts of illegal access are directed at Internet stores. These are popular platforms; as time lapses during an attack, the business will suffer greatly, and customer dissatisfaction will likely occur.

#### *4.2.2. Gaming Sites (20%)*

The second most targeted type of site is the gaming site, which makes up 20% of DDoS targets. This could be because of the heavy traffic these platforms freeze hence easily getting fixated by DDoS attacks that target to cripple services during such peak periods.

#### *4.2.3. Stock Exchange (13%)*

The most impacted industry is the stock exchange, with 13 percent of the chart prone to DDoS attacks. Bar on stock exchange pins results in severe financial consequences because of interferences in trade.

#### *4.2.4. Banks (11%)*

The targets include Banks with an 11% representation. This is because institutions that deal with financial aspects are targeted often.

After all, they play an important role in the specific country's economy. The attack leads to financial loss and damages the specific company's reputation.

#### *4.2.5. Adult Content Sites (8%)*

Adult content sites are also on the list, though they are attacked in 8% of cases. This sector as much as it is profitable for attackers within the context of anonymity and disruptive service intent for ransom and/or extortion.

#### *4.2.6. Blogs and Forums (8%)*

Blogs and forums are targeted most 8% of the time. Such sites may be specifically targeted to cause communication breakdown or political/ideological aggrandizement.

#### *4.2.7. Mass Media (7%)*

Another preferred target is mass media, with a rate of 7 percent of attacks. Media houses, particularly those with online newspapers, may be targeted to prevent the spread of information.

#### *4.2.8. Transport (3%)*

This makes up 3% of the DDoS targets with players in the transport services such as airlines, public transport, and logistics platforms, among others. Time loss in this industry is known to cause havoc with schedules and delivery of services.

*4.2.9. Other Business-Related Sites (3%)*

This has to do with other sites of business interest, which are also aimed at 3% of the time. This could be companies' websites, service providers, or commercial establishments.

*4.2.10. Government Sites (1%)*

DSPs Counter 1% of DDoS attacks on Government websites. Attacks on government websites with political subtexts are less frequent in occurrence but have the same effects.

*4.2.11. Other (1%)*

The Other category makes up only one percent of targets; it can encompass minor or specific markets not defined by the major options presented above.

Interpretation: The pie chart also shows that online shopping and gaming sites are the most common targets of DDoS attacks, making up 45% of the total. These sectors are vulnerable due to the necessity of real-time services and the many visitors they generate. The financial sector, media, and business-related sites are other considerable factors in the attack, proving that DDoS attacks are unbiased and affect everyone.

### *4.3. Discussion on the Issue of Mitigation Effectiveness*

From the study findings, it is clear that none of the detection mechanisms for DDoS is a complete solution. Both approaches have their advantages in certain scenarios; however, the underlying architecture of the network, as well as the scale of the attack, will play a critical role.

*4.3.1. Signature-based Detection*

This method suits small networks or environments with well-understood attack profiles. Due to this, it can be very useful when immediate action has to be taken. However, due to its high false positives and inability to scale to dynamic environments, it does not concretely fit such a setting. Further, it can only detect known attack types, which render it useless in the long run.

*4.3.2. Anomaly-based Detection*

Recent work has demonstrated that anomaly detection is a dependable method that is both accurate and sufficiently flexible. It is suitable for alerting new and emerging attack types owing to its flexibility in recognizing traffic that is not constant. However, its ability to give false positive results requires certain parameters to be tuned for the detection model, and it is not fully scalable for high-traffic environments.

*4.3.4. ML-based Detection*

The best solution is machine learning-based methods, especially for large-scale, distributed systems. These characteristics include high accuracy, low false positive ratios, and scalability, making them suitable for modern networks subjected to complex attacks. This is because, in most cases, the response time is moderate, and that must be timed against the advantages of deploying such an adaptive intelligent system that can enhance its capability and effectiveness as more threats emerge.

### *4.4. Future Research Directions*

Nevertheless, some challenges are worth discussing as they apply to ML-based systems that have numerous advantages. For instance, these models are characterized by high demand for labeled data, which is a critical challenge in the current machine learning models regularly. However, more studies are required to decrease response times when a cyberattack happens and enhance real-time countermeasures. Another area that can be further investigated includes applying blockchain techniques for decentralized traffic confirmation, which can complement the intricate defense collaborative mechanisms. Also, further integration of the proposed detection methods in a single hybrid system, which will use the best characteristics of the considered detection techniques, could provide a more effective and sufficient defense against DoS and DDoS attacks.

## 5. Conclusion

The problem of Distributed Denial of Service (DDoS) remains a critical issue for the dependability and accessibility of internet services in different fields. Another disadvantage of modern DDoS attacks is that they occur in large numbers and are complicated by the use of botnets and the multi-vector approach to attack. In this survey, we have addressed almost all types of mitigation strategies starting from the first-level approaches like rate limiting and IP blacklisting to the second-level of advanced techniques like machine learning and anomaly detection. While the fundamental methods of threat-level management are still effective for combating small or less complex invasions, they prove insufficient in the face of distributed, major attacks and thus require more efficient, adaptation-focused solutions. Traditional methods are not efficient since they depend on manual traffic analysis. Using anomaly-based or machine learning algorithms as a form of detection is a far more efficient means in that traffic patterns are analyzed rather than specific packets for signs of their abnormal behavior. Of the DS volumes, the highest potential probably belongs to the ML-based system due to its capability to learn as more data comes in, in this case, learning as more volume and variant of attacks come in. However, these systems have scalability issues and require big data sets to develop an accurate model. While their detection accuracy is quite high in most cases, the catch is that there remains considerable time consumption involved in its computational process, which in real-time DDoS mitigation scenarios is a significant problem. In the future, with the help of artificial intelligence mixed with decentralized systems such as blockchain, there is great potential for developing DDoS defense. Since the blockchain's core concept is decentralization, it could do away with the single point of failure, and AI could help create self-evolving systems capable of adapting to new attack forms. This integrated approach combines high-speed approaches inherited from conventional methods, the capability of learning algorithms, and decentralized structures, which appears promising in establishing a better protection mechanism. Future research should focus on creating such hybrid systems to adequately address the increasing complexity and magnitude of DDoS attacks.

## Future Work

Because DDoS attacks will become more sophisticated, it is essential to study the different characteristics of the hybrid attack detection and protection model. It is suggested that integrating signature-based, anomaly-based and machine learning methods could make defence mechanisms more effective in overcoming each approach's disadvantages. Due to the more complex tasks performed, the two together could serve to accomplish the known threats more rapidly and allow using the machine learning for new patterns to improve the defense systems' flexibility and completeness. Another potential area is the application of blockchain technology for distributed DDoS protection. An issue related to KG scalability is that traffic validation can be performed more robustly because traffic confirmation is conducted through a set of nodes based on the blockchain distributed ledger system, which does not involve a single point of presence. Smart contracts using blockchain technology could help confirm which traffic is legitimate, and the defense mechanisms deployed could also allow multiple networks in a system to share the threat intelligence data in real-time, making the system a hard nut to crack massive attacks. However, in a live environment, blockchain-based solutions require scalable and low-latency solutions that still remain an open issue. This paper also recommends that future studies address the social implications of decentralized defense, data protection, and legal responsibility across jurisdictions. Hence, with these barriers or issues being solved or avoided, we can develop tougher, more elastic and smarter mechanisms to fight the new generation of DDoS threats.

## References

[1] Jelena Mirkovic, and Peter Lawrence Reiher, "A Taxonomy of Ddos Attack and Ddos Defense Mechanisms," *ACM SIGCOMM Computer Communication Review*, vol. 34, no. 2, pp. 39-53, 2004. [CrossRef] [Google Scholar] [Publisher Link]

[2] Tao Peng, Christopher Leckie, and Kotagiri Ramamohanarao, "Survey of Network-Based Defense Mechanisms Countering the Dos and Ddos Problems," *ACM Computing Surveys (CSUR)*, vol. 39, no. 1, 2007. [CrossRef] [Google Scholar] [Publisher Link]

[3] G. Carl et al., "Denial-of-Service Attack-Detection Techniques" *IEEE Internet Computing*, vol. 10, no. 1, pp. 82-89, 2006. [CrossRef] [Google Scholar] [Publisher Link]

[4] Saman Taghavi Zargar, James Joshi, and David Tipper, "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks," *IEEE Communications Surveys and Tutorials*, vol. 15, no. 4, pp. 2046-2069, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[5] Haining Wang, Danlu Zhang, and Kang G. Shin, "Detecting SYN Flooding Attacks," *Proceedings Twenty-First Annual Joint Conferences of the IEEE Computer and Communications Societies*, New York, USA, vol. 3, pp. 1530-1539, 2002. [CrossRef] [Google Scholar] [Publisher Link]

[6] Shui Yu et al., "Traceback of DDoS Attacks Using Entropy Variations," *IEEE Transactions on Parallel and Distributed systems*, vol. 22, no. 3, pp. 412-425, 2010. [CrossRef] [Google Scholar] [Publisher Link]

[7] S. Asha Varma, and Karri Ganesh Reddy, "A Review of DDoS Attacks and its Countermeasures in Cloud Computing," *In 2021 5th International Conference on Information Systems and Computer Networks (ISCON)*, Mathura, India, pp. 1-6, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[8] Kriti Bhushan and B.B. Gupta, "Distributed Denial of Service (DDoS) Attack Mitigation in Software Defined Network (SDN)-Based Cloud Computing Environment," *Journal of Ambient Intelligence and Humanized Computing*, vol. 10, pp. 1985-1997, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[9] DDoS Mitigation, Arcane, 2025. [Online]. Available: https://www.arcanebt.com/solutions/network-security/ddos-mitigation

[10] Iman Sharafaldin et al., "Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy," *In 2019 International Carnahan Conference on Security Technology (ICCST)*, Chennai, India, pp. 1-8, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[11] Esraa Alomari et al., "Botnet-Based Distributed Denial of Service (DDoS) Attacks on Web Servers: Classification and Art," *International Journal of Computer Applications*, vol. 49, no. 7, 2012. [CrossRef] [Google Scholar] [Publisher Link]

[12] Shi Dong, Khushnood Abbas, and Raj Jain, "A Survey on Distributed Denial of Service (DDoS) Attacks in SDN and Cloud Computing Environments," *IEEE Access*, vol. 7, pp. 80813-80828, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[13] Saravanan kumarasamy, and R. Asokan, "Distributed Denial of Service (DDoS) Attacks Detection Mechanism," *International Journal of Computer Science, Engineering and Information Technology (IJCSEIT)*, vol. 1, no. 5, pp. 39-49, 2011. [CrossRef] [Google Scholar] [Publisher Link]

[14] Shweta Tripathi et al., "Hadoop Based Defense Solution to Handle Distributed Denial of Service (DDoS) Attacks," *Journal of Information Security*, vol. 4, no. 3, pp. 150-164, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[15] Shui Yu, *Distributed Denial of Service Attack and Defense*, Springer, New York, pp. 15-29, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[16] Sanjeev Kumar, "Smurf-Based Distributed Denial of Service (DDoS) Attack Amplification in Internet," *In Second International Conference on Internet Monitoring and Protection (ICIMP 2007)*, San Jose, CA, USA, pp. 25-25, 2007. [CrossRef] [Google Scholar] [Publisher Link]

[17] Firooz B. Saghezchi et al., "Machine Learning for DDoS Attack Detection in Industry 4.0 CPPSs," *Electronics*, vol. 11, no. 4, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[18] Tasnuva Mahjabin et al., "A Survey of Distributed Denial-of-Service Attack, Prevention, and Mitigation Techniques," *International Journal of Distributed Sensor Networks*, vol. 13, no. 12, 2017.[CrossRef] [Google Scholar] [Publisher Link]

[19] Shubhankar Chaudhary, and Pramod Kumar Mishra, "DDoS Attacks in Industrial IoT: A Survey," *Computer Networks*, vol. 236, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[20] Bryan Harris, Eli Konikoff, and Phillip Petersen, "Breaking the DDoS attack chain," *Institute for Software Research*, pp. 1-16, 2013. [Google Scholar] [Publisher Link]