

Retraction

Retracted: Prevention Techniques against Distributed Denial of Service Attacks in Heterogeneous Networks: A Systematic Review

Security and Communication Networks

Received 5 December 2023; Accepted 5 December 2023; Published 6 December 2023

Copyright © 2023 Security and Communication Networks. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

This article has been retracted by Hindawi, as publisher, following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of systematic manipulation of the publication and peer-review process. We cannot, therefore, vouch for the reliability or integrity of this article.

Please note that this notice is intended solely to alert readers that the peer-review process of this article has been compromised.

Wiley and Hindawi regret that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.






The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

- [1] A. Cheema, M. Tariq, A. Hafiz, M. M. Khan, F. Ahmad, and M. Anwar, "Prevention Techniques against Distributed Denial of Service Attacks in Heterogeneous Networks: A Systematic Review," *Security and Communication Networks*, vol. 2022, Article ID 8379532, 15 pages, 2022.

Review Article

Prevention Techniques against Distributed Denial of Service Attacks in Heterogeneous Networks: A Systematic Review

Ammarah Cheema ¹, Moenuddin Tariq ², Adnan Hafiz ¹, Muhammad Murad Khan,³
Fahad Ahmad ⁴ and Muhammad Anwar ⁵

¹Department of Computer Science & IT, Lahore Leads University, Lahore, Pakistan

²Department of Computer Science, National University of Modern Languages, Islamabad, Pakistan

³Department of Computer Science, Government College University, Faisalabad, Pakistan

⁴Department of Basic Sciences, Jouf University, Sakaka, Aljouf, Saudi Arabia

⁵Department of Information Science, Division of Science and Technology, University of Education, Lahore, Pakistan

Correspondence should be addressed to Muhammad Anwar; anwar.muhammad@ue.edu.pk

Received 22 February 2022; Revised 16 April 2022; Accepted 28 April 2022; Published 20 May 2022

Academic Editor: Muhammad Arif

Copyright © 2022 Ammarah Cheema et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

The Distributed Denial of Service (DDoS) attack is one of the most critical issues in network security. These sorts of attacks pose a noteworthy danger to the accessibility of network services for their legitimate users by flooding the bandwidth or network service using various infected computer systems. The targeted servers are overwhelmed with malicious packets or connection requests, causing them to slow down or even crash the server operations which results in preventing genuine users from accessing the service. In this paper, we discussed the detailed classification of DDoS attacks and identified attackers' motivations behind them and their consequences. Further, the DDoS attacks on IoT devices are elaborated based on applications and network layers. A comprehensive literature review has been conducted on cutting-edge defense techniques to defend against such attacks. An in-depth analysis of each mechanism has been carried out to find the optimal solutions. We fairly evaluated the existing defense techniques for DDoS attacks and presented key findings in comparison tables. Furthermore, this paper provides recommendations for future work for new researchers.

1. Introduction

A Distributed Denial of Service (DDoS) is a malevolent attempt to make an online service unavailable to genuine customers by simply stopping or delaying the host server's service. In DDOS attacks, hackers aim at specific servers, also called victims, and flood them with requests, effectively shutting down their services. The rush of arriving messages, connection requests, and falsified packets from these affected devices causes the victim server to become slower or even shut down altogether, preventing normal users and system access. A network of compromised devices with the controlled architecture is called botnet [1–4]. According to Kaspersky Lab research, the longest DDoS attack occurred in the second quarter of 2016 and lasted 291 hours due to

botnets used by many susceptible Internet of Things (IoT) devices [5–9]. The DDoS attacks have launched on DYN systems, which is a web application-based security firm and the world's largest DNS provider, to make unavailable its key web services such as PayPal, Twitter, Amazon, and Netflix. This DDoS attack was carried out using an interconnected device network that was linked to the Internet, as well as a unique malware named "Mirai botnet," which flooded the victim systems with traffic until they surrendered to the stress [10–16].

The DDoS attack is usually executed by a botnet, which is a group of compromised systems scattered worldwide. It is different from other denial of service (DoS) attacks, in that it overflows a victim server with malevolent traffic-utilizing one Internet-connected machine [17–21]. In other words, a

single attacker, at the simplest level, uses a single source to initiate a DoS attack against a target as depicted in Figure 1. The presence of these two, slightly different, definitions is due to this distinction.

A bot is a computer or networked device that is controlled by an attacker. Generally, a DDoS attack begins with a hacker manipulating the vulnerability in a computer system, which then becomes the DDoS master bot. The attacker master bot system finds other weak systems and takes control of them by infecting them with malware or bypassing verification measures. DDoS slave bots are the name of these systems. To command the botnet, the hackers generate a command-and-control system [22]. The attacker then inundates the target with traffic generated by the infected devices to take down its services. Figure 2 depicts a typical DDoS mechanism [23–25].

According to the current industry research, DDoS attacks are swiftly becoming a highly common sort of cyber threat which is expanding vividly in both frequency and volume over the last decade [26, 27].

The main objective of this study is to discuss the rising and serious danger to cybersecurity that has arisen because of such types of attacks. DDoS flooding attacks are the most difficult task facing security researchers and analysts today. These attacks are extremely destructive to the Internet. As a result, several techniques to detect and prevent DDoS flooding assaults have been proposed by using machine learning algorithms and other latest technologies. Some researchers proposed detection techniques in which they try to distinguish malicious traffic from regular traffic flows to stop DDoS attacks on time before creating destruction on the victim server. On the other hand, some of the authors presented not only detection techniques but also developed prevention systems to defend against DDoS attacks and minimize the destructive effects of these types of attacks on legitimate users of targeted systems. In this paper, we have performed an in-depth comparative analysis of several cutting-edge techniques and found out which technique is comparatively better to combat DDoS attacks on heterogeneous networks along with our personal findings and suggestions to improve existing techniques.

2. Common Types of DDoS Attacks

DoS and DDoS attacks are categorized into three broader types:

- (i) Volume-based attacks
- (ii) Protocol layer attacks
- (iii) Application-layer attacks
- (iv) Zero-day attacks

2.1. Volume-Based Attacks. The objective of this attack is to exceed the bandwidth of the attacked system, which is calculated in bits per second [28–30]. UDP flood, ICMP flood, and other spoofed packet floods are involved in this type of attack. Some common types of volumetric attacks are described below.

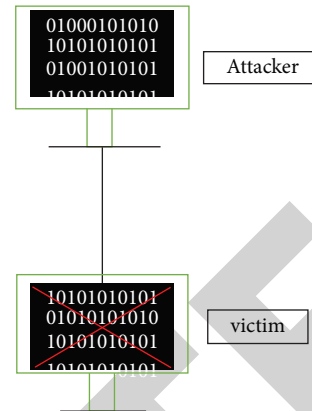


FIGURE 1: Simple DoS attack.

2.1.1. UDP Floods. A DDoS assault that overflows a victim with User Datagram Protocol (UDP) packets is known as a UDP flooding assault. This attack’s objective is to overwhelm arbitrary ports of a distant server with traffic flow. Therefore, it prompts the host to search for an application snooping on the specific port on a regular basis, and if none has been detected, it responds through an ICMP (Destination Unreachable) packet. Finally, this procedure reduces host resources, potentially resulting in unavailability [31].

2.1.2. ICMP Floods. The ICMP flooding attack, like the UDP flooding attack, floods the victim’s resources with “ICMP Echo Request”/ping packets in rapid succession without waiting for a response. Since the target’s computers will often challenge to react with “ICMP Echo Reply” packets, this kind of assault can use both outgoing and incoming bandwidth, subsequent in a huge inclusive system suspension [32]. The initial letter of each notional word in all headings has been capitalized.

2.2. Protocol Layer Attacks. This kind of attack utilizes server resources or middle communication infrastructures such as firewalls and packet filtering and is measured in packets per second (Pps). This type of attack contains SYN flood, and fragmented packet attacks, such as Smurf DDoS, ping of death, and others [33]. Some common types of protocol attacks are described below.

2.2.1. SYN Floods. SYN flood DDoS attacks take benefit of a recognized fault in the TCP connection process, in which an SYN request to create a TCP connection with a host must be met with an SYN-ACK response from the respective host, trailed by an ACK reaction from the applicant. In an SYN flooding condition, the applicant transmits several SYN queries but ignores the host server’s SYN-ACK response or sends the SYN queries from a forged IP address. On the other hand, the host server will continue to wait for approval of each query, tying up resources while no new connections can be formed, ending in a service denial [16].

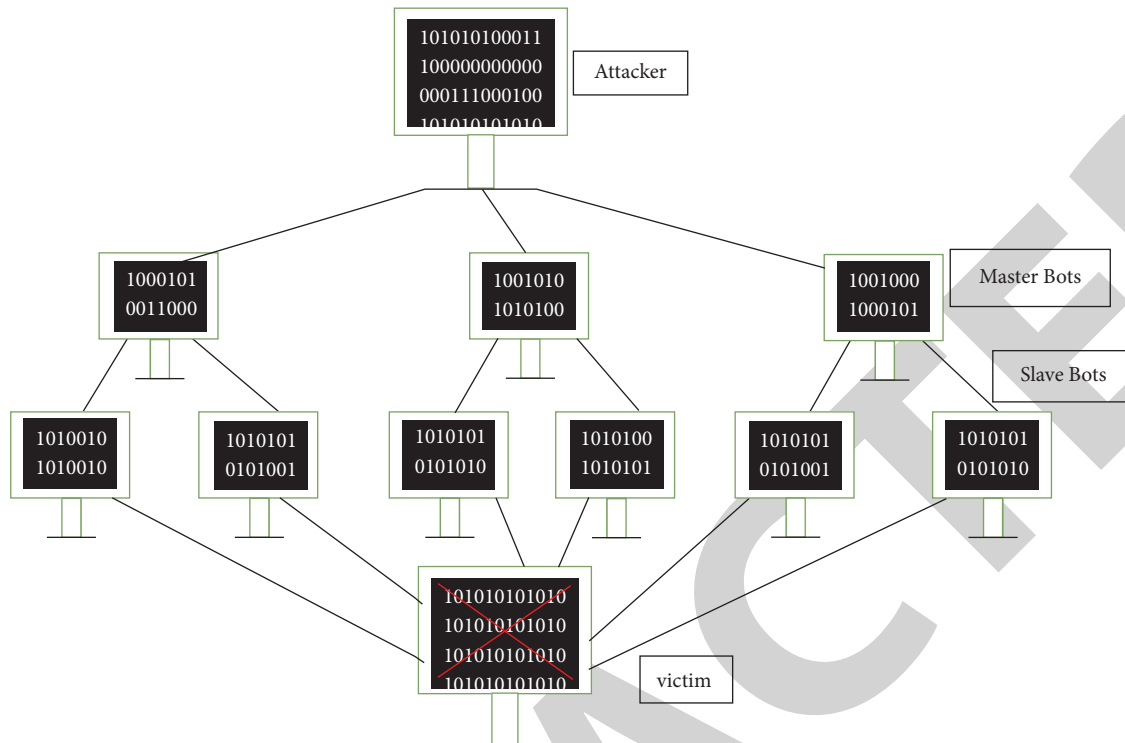


FIGURE 2: Typical DDoS attack architecture.

2.2.2. Ping of Death. The hacker transmits regular fake or malicious calls to a computer in a Ping of Death attack. The IP packet can have the largest duration of 65,535 bytes. On the other hand, a data link layer mostly sets a perimeter on the highest frame size, for instance, 1500 bytes on top of an Ethernet Network. In this situation, a bigger IP packet is distributed into several IP packets (described as fragments), and the destination server reconstructs the fragments into the full packet. In this attack scenario, the recipient receives an IP packet that is bigger than 65,535 bytes when restored because of malevolent fragment substance alteration. This can cause real packets to be denied service due to flooding memory barriers allotted for the packet [16, 33].

2.3. Application-Layer Attacks. The objective of this type of attack is to destroy the web server, created by apparently genuine and inoffensive requests, and the size measured in requests per second (Rps). This sort of attack includes truncated and sluggish attacks, GET or POST floods, attacks against Windows, Apache, or OpenBSD weaknesses. Some of the popular types of application-layer DDoS attacks are described below.

2.3.1. Slowloris. Slowloris attacks are a type of DDoS attack that permits one web server to shut down another while parting other services and ports on the victim's network unpretentious. They achieve this by keeping as various connections to the victim web server as possible. Slowloris does so by forming connections with the victim server but only sends a part of the query. The target's server keeps each

of these fraudulent connections open. The highest synchronized connection pool will almost certainly overflow, preventing valid customers from connecting [31].

2.3.2. NTP Amplification. The attacker of NTP amplification attacks uses openly nearby Network Time Protocol (NTP) servers to overflow the target system with UDP traffic. Because the request feedback ratio in such cases is usually between 1:19 and 1:190 or above, the attack has been categorized as an amplification attack. This ensures that every adversary who acquires a list of available NTP servers, i.e., utilizing Metasploit or data from the Open NTP Project, can simply launch a large bandwidth, highest level DDoS attack. [32].

2.3.3. HTTP Floods. The hacker utilizes apparently valid HTTP POST or GET queries to target a web server or an application in an HTTP flooding assault. HTTP flood does not include defective packets, fooling, or reflection methods and thus consumes a smaller amount of bandwidth to shut down the victim's system than other forms of attacks. When the server or application has been enforced to distribute the maximum number of resources viable in reaction to every query, the assault is most effective [16, 32].

2.4. Zero-Day Attacks. Zero-day attacks' description includes all strange or recent attacks, manipulating weaknesses for which no proper solution has been provided up to now. The word has become very famous among hackers' societies,

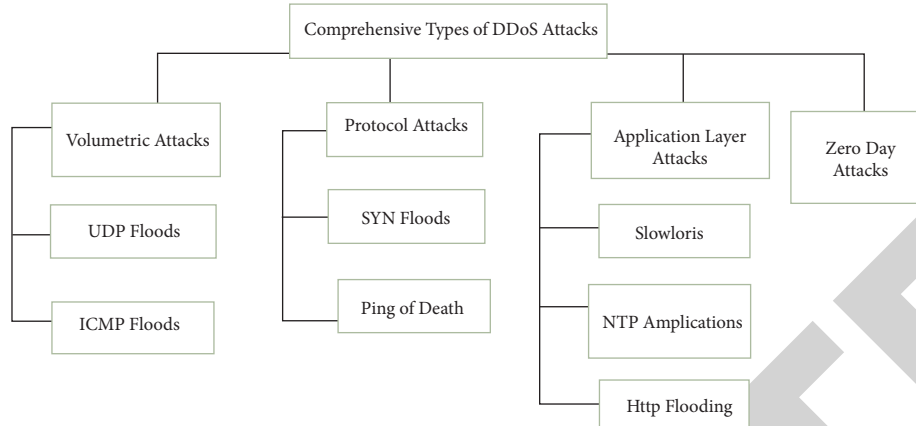


FIGURE 3: Common types of DDoS attacks.

where dealing with zero-day weaknesses has become a famous pastime.

We summarize the comprehensive types of DDoS attacks in Figure 3.

3. Survey Methodology

The literature was gathered using indexing databases and digital libraries like ACM, IEEE, and Google Scholar. In this study, we comprised various state-of-the-art defense techniques including detection, prevention, and mitigation methods against DDoS attacks for consideration. Firstly, we examined the collected literature's titles and abstracts. Secondly, we eliminated those papers that did not provide any detection or prevention techniques for DDoS attacks in their abstracts. In addition, we have selected only those papers published after 2017 because cyberattack rates and volumes have risen dramatically in recent years, rendering previous techniques for detecting and preventing the most recent DDoS attacks obsolete. Furthermore, due to the simplicity of the DoS attack defense structure, papers presenting the defense of only DoS attacks were omitted and included only those research studies which presented defense techniques for DDoS attacks. Similarly, studies that contained defense techniques that were improved upon in subsequent papers were eliminated, leaving only the most recent enhancements.

4. Classification of DDoS Attacks

Attacks on IoT device need verification information, for example, a pin and passcode. An intruder can use a brute-force approach to infect the device and seize control of it. An assault on the cloud layer, on the other hand, necessitates a huge volumetric attack to assure that the victim system has partly or entirely blackout. An assault from a sole machine or just a hundred devices would have little effect on the system or network. Current security measures are capable of withstanding attacks from a small number of devices. An adversary must conduct a big volumetric attack, such as the Mirai attack, which employed over 600,000 hacked IoT devices to target networks and servers with robust protection

defenses. An effective DDoS attack on the cloud layer must overwhelm the server or network with queries that are more than its capacity to process. The 2008 GitHub attack, with a capacity of 1.35 Tbps, totally knocked down the server for ten minutes. Attacks against IoT devices are easier to carry out and involve less exertion. To completely shut down a server or network, an assault on the cloud layer needs thousands of compromised IoT devices. The categorization of DDoS attacks describes the effect of DDoS on the target's bandwidth and network resources. The attacker's goal in such attacks is to exhaust the targets' few accessible resources. The best scenario would be to drop the malicious packets while allowing regular data to pass. When packets have dropped, a genuine user will stop attempting to connect, whereas an adversary will perceive this as a chance to increase their efforts in order to strengthen the attack. The victim's CPU resources would have drained, denying service to all consumers. Another possibility concerns network bandwidth depletion, in which an attack not only affects the target's resources but also all systems that rely on the target's server. Our categorization takes into account these two forms of network and bandwidth resource attacks. An attack might affect both network and bandwidth resources at around the same time.

4.1. Resource Depletion Attacks. The objective of a resource depletion assault is to exhaust the use of memory, CPU, and socket. This assault can be carried out by transmitting malicious packets, as in the PoD attack, or through abusing a flaw in the target's network, application, or physical layers protocol, as in the HTTP flood attack. The resource depletion attacks have been further classified into two categories:

- (i) Protocol exploit attacks
- (ii) Malformed packet attacks

We have covered both categories in depth below.

4.1.1. Protocol Exploit Attacks. The attacker makes use of flaws in network layer protocols, causing the target to

exhaust all of their CPU and memory resources. Several protocols, including the Hypertext Transfer Protocol (HTTP), Session Initiation Protocol (SIP), and Transmission Control Protocol (TCP), have been exploited in these types of attacks. Some common protocol exploit attacks have been discussed below:

(1) *TCP Push + ACK Attacks.* The header's PUSH and ACK bits are both adjusted to "1." The botnet of attacking computers will transmit repeated TCP packets, causing the victim server to try to remove its memory and respond to the user's affirmation. This allows the server to discard packets received by legitimate users.

(2) *Slow HTTP Attacks.* This slow attack seeks to slowly eat all of the victim's resources. Slowloris attacks originate by transmitting content slowly. It will make an incomplete HTTP request, followed by the header request at regular pauses, assuring that the sockets stay exposed. The server subsequently drops all genuine requests, resulting in a denial of service. It can be minimized by establishing a transfer rate limit from a customer. R.U. Dead Yet is another attack. This attack launches its attack using the form submission areas on the websites. Using several HTTP POST connections, the hacker will slowly add information in tiny packets. This action causes the computer to keep the link open for long term, eventually depleting all of its connections. The system will fail and deny service to legitimate users' packets.

(3) *HTTP Flood Attacks.* As part of a botnet, the attacker organizes a large number of compromised devices known as bots. The attacker will utilize bots to submit enormous amounts of requests, broadening the scope of the attack. An HTTP flood attack may have been carried out in two ways. The HTTP GET assault happens when the hacker utilizes the botnet to send many GET requests to the victim server for files, pictures, and so on. The server will remain busy responding to these requests from all victim PCs on the botnet, avoiding genuine requests from dropping. A GET request is significantly easier to carry out since any unknowing user may participate in the attack by just viewing a website. An adversary might insert an inline picture into the content of a web. Everybody who accesses the web may submit an unintentional GET request to the victim server.

The HTTP POST assault includes the adversary leveraging the botnet to input forms on a website. The website would be fully occupied with this computationally and bandwidth-intensive operation. When combined with the information that the requests are transmitting from a large number of infected computers, the server adds more resources. The server ultimately becomes overloaded, resulting in a denial of the service incident. POST assaults are riskier for the server since they contain parameters that cause intricate processing and dense processes on the system. As a result, POST request assaults are significantly more harmful than getting request floods.

(4) *SIP Flood Attacks.* This assault targets the SIP (Session Initiation Protocol) registration servers, and uses all of its capitals, along with the network bandwidth, CPU, and

memory. This assault will flood the system, preventing genuine users from connecting and causing an inconvenience. SIP attacks have been launched against services that provide voice-over IP. An attack can be launched by transmitting SIP INVITE, SIP INFO, SIP REQUEST, SIP RE-INVITE, and SIP NOTIFY.

(5) *TCP SYN Attacks.* This attack makes use of a flaw in the Transmission Control Protocol. To complete an effective handshake and establish a connection, the TCP handshake protocol needs a sequence of responses from both sides. The server directs the consumer to an SYN-ACK packet to complete the handshake. The hacker takes advantage of this protocol by delivering forged SYN packets to the server. After submitting the SYN-ACK request, the server waits for a response that does not ever come. The connection status is stored in the server's memory stack until a timeout occurs or the connection is recognized. The hacker overflows the server's memory, forcing it to ignore SYN requests submitted by legitimate users.

4.1.2. *Malformed Packet Attacks.* The core component of this attack is to deliver a distorted packet to the target, causing their system to crash. The Land attack, Ping of Death, IP packet option field, and Teardrop attack are among them.

(1) *Land Attacks.* This attack happens due to the formation of an infinite loop. The adversary customizes the packet's source address to be the target's IP address. When the target or system responds to the packet, it effectively responds to itself, creating an unlimited loop. Eventually, the system fails.

(2) *IP Packet Option Field Attacks.* The hacker generates random values for the IP packet's additional fields. The additional field, i.e., the service quality, is set to 1, forcing the algorithm to employ more time analyzing it. If an adversary transmits a flood of such packets, the system's processing capacity has depleted.

(3) *Ping of Death.* The assault causes the victim server to crash by delivering ICMP echo requests that are above the IP standard packet size limit. An IP packet can have a huge size of 65,535 bytes. Huge packet sizes have split into little segments before being sent as several packets. The adversary sends many large packets to the target, who reconstitutes them and exceeds the 65,536 bytes limit. Reaching the cutoff causes memory to overflow, which causes the system to fail. When a system collapses, it becomes more vulnerable to other attacks, for example, the Trojan horse attack.

(4) *UDP Fragmentation Attacks.* The hacker sends out fake packets that are greater than the network's broadcast range unit. The server seems not able to reconstruct the packets using its resources because they exceed the size limit. This attack eventually causes a denial of service to its clients.

(5) *Teardrop Attacks*. When the adversary delivers broken packets to the system, the attack happens. Because of a mistake in the TCP/IP segmentation assembly, the system delivers broken packets with overlapping offset values. When the packets overlap with one another, the target system crashes.

4.2. *Bandwidth Depletion Attacks*. The attack's goal is to use an attacking army to use all of the network's bandwidth. To intensify the attack, the attack packets might have been amplified or broadcasted. Until the attack is recognized and handled, genuine users experience a denial of service. Bandwidth depletion tracks are more categorized into two types:

- (i) Protocol exploit attacks
- (ii) Amplification Attacks

We discussed both types in detail below.

4.2.1. *Protocol Exploit Attacks*. The goal of the assault is to deplete the victim's resources by abusing an attribute as a flaw in their system. The attack has been carried out with a transport-layer protocol such as User Datagram Protocol (UDP) or a Network Layer Protocol like Internet Control Message Protocol. The assaults used the Protocol exploit approach discussed below:

(1) *UDP Flood Attacks*. The hacker provides directions, i.e., the target's address, the length of the assault, and the mechanism used to carry out the attack on several compromised machines called the Masters. The attacker may transmit it to a Master Control software first or connect straight with the Masters. The Master Control application will broadcast the assault directions to the Masters, causing them to transmit several UDP packets with a faked Internet Protocol (IP) as the basis to an arbitrary target port on the target's machine. In turn, the target will transmit Internet Control Message Protocol (ICMP) packets as the required answer to the faked address, but it will never get a response. Because of the enormous amount of packets received and the absence of response, the target's machine will continue to slow and eventually fail.

(2) *ICMP Flood Attacks*. The hacker sends several ICMP echo signals to an unsecured broadcast network, each with the faked source address of the target's computer. When targeting the target's server with different echo reply messages, the broadcast station will assist enhance the echo messages. The greater the number of broadcast stations engaged, the more enhanced messages the victim would get. The Smurf attack floods the target's computer with high-volume echo reply messages, causing the machine to slow down and finally become unusable.

(3) *Fraggle Attacks*. Fraggle attacks, usually termed amplification attacks, use UDP ECHO PACKETS to flood the target's bandwidth. As a launching mechanism, these attacks

use refactors. A refactor like a router or a DNS server will further disseminate the message to the target. The refactors will transmit the attack packet with a faked IP address that looks very similar to the targets. The hacker is difficult to discover due to the falsified IP address; meanwhile, the refactors are easily detected since they do not employ faked IP addresses.

4.2.2. *Amplification Attacks*. These attacks elicit a huge response since the hacker delivers minor packet sizes of fewer bytes, but by intensifying them; it sends a large number of packets to the target, using all of its available bandwidth. The DNS amplification attack and the Network Time Protocol (NTP) assault are two examples of such attacks.

(1) *DNS Amplification Attacks*. The hacker transmits a DNS search request to the DNS servers with a faked IP address, that is, the victim's address. The DNS server answers by sending the record to the target. The hacker will declare that every "ANY" request will send as much information to the target as possible. The DNS attack is an amplification attack since the amount of the request surpasses the size of the answer. Because the responses are legal server responses, it is impossible to identify whether the packets have been sent by an attacker or by authorized users.

(2) *NTP Amplification Attacks*. The main goal of the Network Time Protocol (NTP) is to coordinate the system clock with the server in order to establish the time. The hacker uses a faked IP address to deliver amplified data packets to the target over the NTP UDP protocol. The "monlist" command on the NTP server has been used to launch an NTP server attack. Because the MONLIST reply packet has amplified, the attacker's monlist request packet is considerably shorter at 64 bytes. The monlist or MON GET LIST command may be delivered to the NTP server, which responds with a list of 600 systems that are connected, demonstrating that NTP is excellent for use as an amplification attack.

(3) *CLDAP Amplification Attacks*. The connectionless light directory access, protocol amplification attack sends faked packets to the CLDAP server over UDP ports. Because it does not validate the user's address, UDP has frequently been used in DDoS attacks. The server returns the response to the faked address. One of the possible amplification attacks is a response that is 46–55 times the size of the genuine packet.

We summarize the classification of DDoS attacks in Figure 4.

5. Related Work

DDoS attacks happen at the network layer or the application layer of the malicious systems that are associated with the networks. On the other hand, some hackers take advantage of IoT devices' inadequate security implementation to capture them and utilize them to target the victim server or

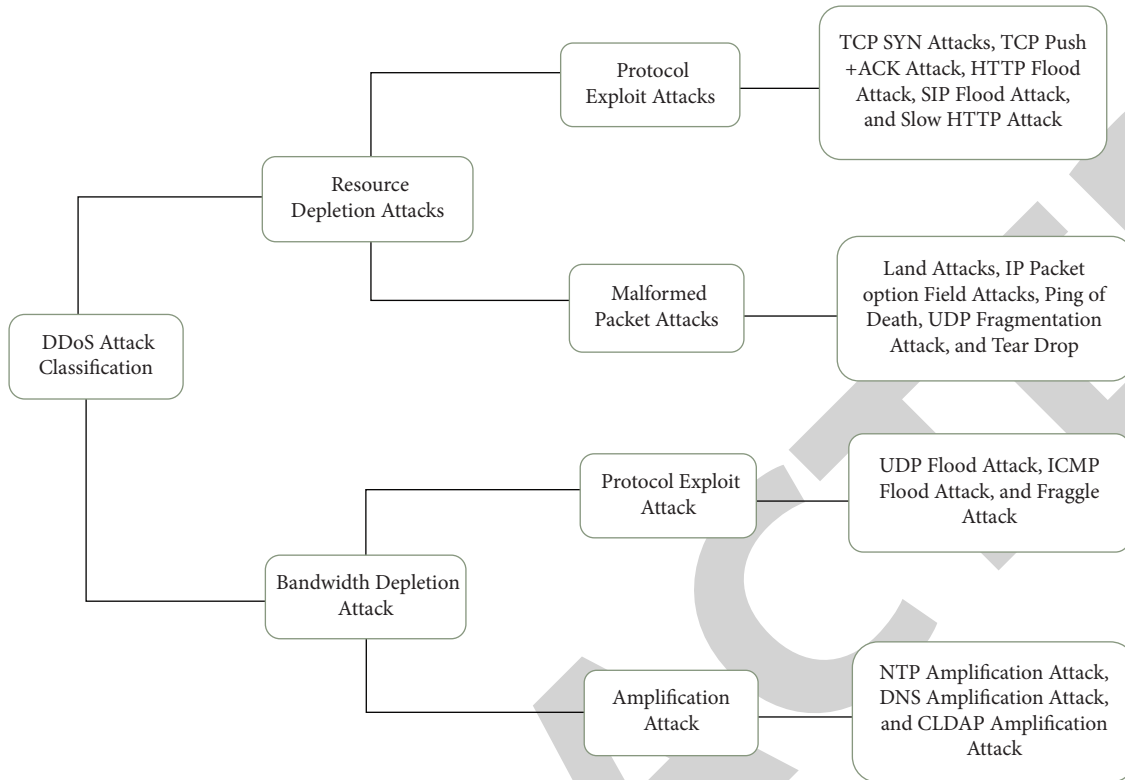


FIGURE 4: Classification of DDoS attacks.

network. Different researchers and analysts presented multiple technology-based solutions for the application layer, network layer, and IoT devices DDoS attacks and proposed various effective detection, prevention, and mitigation techniques. Some state-of-the-art approaches are discussed here.

5.1. DDoS Attacks Defense through Firewalls. Firewalls were once thought to be the first layer of protection against DDoS attacks. Each packet transmitted into and outside of a network is inspected by a firewall based on established filtering criteria such as specific IP (Internet protocol) addresses or routes. On the other hand, DDoS attacks overwhelm a firewall with superfluous packets, causing it to work inefficiently and significantly degrade its functionality. Worse yet, a hacker can create IP addresses and ports for packets to manipulate the firewall. Attacks like this compromise the target's network bandwidth and services, making it easier to prevent access to authorized users.

5.2. SDN-Based Defense Techniques against DDoS Attacks. Software-Defined Networking (SDN) is a revolutionary network management platform that presents numerous new chances for guarding against network threats because of its centralized control structural design. Switches in a Software-Defined Network context do not manage arriving packets in the same way that they do in a traditional network computation environment. They check the forwarding tables for incoming packets, and if none existed, the packets are passed

towards the controller for processing, which is the SDN's Operating System. The most serious risk to cyber security in an SDN network is a DDoS assault. The DDoS attacks arise on either the Network level or the Application level of the networked hacked systems. Furthermore, compared to traditional networks, SDN has numerous advantages. The physical separation of network control and forwarding devices is a major benefit of SDN.

Jia et al. [33] effectively detected two forms of flooding-based DDoS attacks through employing two essential attributes named Volumetric and Asymmetric. The proposed detection method can decrease both training and testing time. The purpose of this paper is to suggest a DDoS attack detection method based on SDN that will cause the least amount of disruption to valid user activities. In addition, they proposed the Advanced Support Vector Machine (ASVM) technique to enhance the current Support Vector Machine (SVM) algorithm to effectively detect DDoS flooding assaults.

Prakash and Priyadarshini [34] developed a machine learning-based adaptive technique for detecting whether incoming packets are infected or not. To detect unusual data traffic behavior, some machine learning techniques are used to complete the task, for example, K-Nearest Neighbor (KNN), Naive Bayes, and Support Vector Machine (SVM) machine learning algorithms. The entire project revolves around detecting DDoS attacks employing an SDN controller. Data are gathered from two entities in which the first set has been carried from the regular case while the other has been taken from the infected case.

By bombarding target servers with many requests, DDoS attacks force them to become unable to deliver services to real users. They would also have a substantial influence on the performance of SDN, as the controller would have to deal with several connections produced by the DDOS attacks. As a result, Y. C. Wang and Y. C. Wang [35] designed a lightweight but effective ELD method to protect against protocol-type DDoS attacks, with the goal of reducing the controller's operating cost in detecting and stopping attacks quickly. Due to limited memory space, the authors proposed an NRES data storage technique using ELD to assist the controller in recording current packets while saving a small number of older packets for references, which presents a more comprehensive and higher level picture of attacks. ELD distinguishes normal flows from DDoS flows by examining the signatures of flow size, IP irregularity, and length, thus preventing the packets of elephant and impulsive flows from being dropped. Furthermore, the suggested NRES method overwhelms conventional data storage methods in terms of memory usage, allowing the controller to store packet data and identify DDoS assaults more effectively.

However, the existing mechanisms of DDoS attacks are well recognized, but the issues have become more critical because of the resemblance between DDoS attacks and regular traffic. Nam et al. [36] developed a DDoS detection system by utilizing SDN along with two classification techniques based on Self-Organizing Map to categorize the existing network status as regular or malicious. The purpose system is lightweight, which can operate effectively with a variety of DDoS attacks since it uses five representative elements and is deployed using SDN technology. All the elements in the existing work are specified manually to effectively depict the network traffic. On the other hand, these properties can be distinct depending on the nature of the host which needs to be defended and the type of attack that can occur. When compared to typical detection algorithms, the presented methods have been shown to perform better when given alternative priorities.

Hu et al. [37] introduced FADM, a lightweight and economic framework for the detection and mitigation of DDoS flooding attacks using the SDN environment. Initially, they employed a CT-based and a flow-based technique based on distinct network environments to increase the reliability of information gathering. Furthermore, using the entropy-based approach, they evaluated variations in network characteristics and, by using the SVM classifiers, they determined whether the existing network state is regular or unusual. They presented an effective attack mitigation technique created on whitelisting and dynamically updating forwarding laws to safeguard the network and maintain regular operation while it is subjected to DDoS attacks. Thus, the attacked traffic can move on time and forward the mild traffic regularly by adding the mitigation agent into the network.

Giri et al. [38] suggested an architecture in which a smart contract is put on a confidential blockchain, allowing for collective DDoS mitigation through various network areas. The blockchain mechanism employed as an extra layer of

protection along with shared location, which enabled for all hosts. Rules are disseminated to all hosts via smart contracts. Furthermore, they used SDN to activate service and defense controls dynamically. This approach allows Autonomous Systems (ASES) to implement their own DDoS Prevention Service (DPS), eliminating the requirement to hand over network management to a third party. The difficulties of defending a hybridized enterprise against the impacts of a fast-growing DDoS attack are the focus of this study.

We comparatively analyzed some important properties of SDN-based defense techniques against DDoS attacks in Table 1.

After analyzing and comparing the above Software-Defined Network (SDN)-based defense techniques in Table 1, we conclude that Y. C. Wang and Y. C. Wang [35] and Hu et al. [37] proposed defense techniques against DDoS attacks are the best. They not only provide detection mechanisms to detect malicious traffic from regular traffic flow quickly but also provide lightweight, inexpensive prevention techniques to prevent DDoS attacks effectively. However, Giri et al. [38] proposed a groundbreaking approach by emerging two novel techniques, blockchain and SDN, to mitigate DDoS attacks.

5.3. Defense Techniques for Application-Layer DDoS Attacks.

Initially, DDoS attacks were aimed against the network and transport levels. However, attackers have transferred their violent techniques to the application layer over time. Due to the similar attacked traffic and the normal traffic flows, application-layer attacks can be more destructive and stealthier. These attacks are difficult to resist due to their distributed nature, as they can harm substantial computer resources in addition to network bandwidth usage. Furthermore, Internet-connected smart gadgets can be infective and exploited as botnets to execute DDoS attacks.

Rather than wasting network resources, application-layer DDoS attacks aim to damage application services. It has grown in importance as a threat to web services with time, surpassing traditional DoS attacks. DDoS attacks use a variety of flooding techniques, including HTTP POST flood, HTTP GET flood, DNS, and Slowloris, among others. As stated by Arbor, Inc. [39], Figure 5 characterizes the graphical distribution of DDoS attacks on the application layer.

Bhosale et al. [40] investigated the scope of the issue of the DDoS attack as well as several technical approaches to mitigate it. Application-level flooding, particularly on the web server, is the latest and most popular method of DDOS attacks. Rather than wasting network resources, application-layer DDoS attacks aim to impair application services. It has grown in importance as a threat to web services over time, surpassing traditional denial of service attacks. DDOS uses a variety of flooding techniques, including HTTP POST flood, Slowloris, HTTP GET flood, and DNS, among others. On the other hand, HTTP attacks account for a higher percentage of all attacks. HTTP has the highest rate of DDOS attacks, with up to 86 percent. This research focuses on the attributes of recently suggested application-layer DDOS

TABLE 1: Summary of SDN-based DDoS prevention techniques.

Reference	Main idea	Type	Strength	Future work	Results
Myint et al. [33]	Enhancing the functionalities of the existing SVM algorithm by purposing ASVM (advance vector machine) to detect DDOS assault	Detection	Minimize the disturbance of users' activities	In the future, an online detection DDoS attacks system on SDN networks and other SDN layer attack planes should be considered	Experimental outcomes show that the proposed detection technique has a 97 percent accuracy rate with the shortest training and testing times
Prakash and Priyadarshini [34]	A smart intrusion detection model can distinguish between malicious and normal arriving packets	Detection	The proposed method can successfully determine whether the incoming packet is malicious	After identifying the infected packets, extra actions would take to notify the target users and devices more quickly in the future	Experimental results show that KNN performed best out of the three algorithms trained on 75% of the data
Y. C. Wang and Y. C. Wang [35]	Purposing lightweight, effective ELD mechanism to fight against protocol-type DDoS attacks	Detection and prevention	Purposed method decreases the costs of the controller and quickly identifies and prevents DDOS attacks	This study is an initial step in this field of research. More research in the future can improve the accuracy of this technique	Findings prove that ELD enhances the true positive rate, dramatically reduces false alarms, and substantially decreases the cost of the controller
Nam et al. [36]	Utilizing self-organizing map to categorize the present network status as regular or malicious	Detection	As compared to traditional detection algorithms, the proposed techniques performed better	The attempted methods used to automate the selection of an attribute can be explored in the future	Outcomes show that proposed algorithms can shorten processing time while maintaining a high level of accuracy
Hu et al. [37]	Purposing FADM is an effective and lightweight framework for the detection and mitigation of DDoS attacks in an SDN context	Detection and mitigation	As compared to other existing detection techniques, running costs of FADM is quite low	In the future, application-layer DDoS attacks and botnets can be detected using the characteristics of SDN and machine learning technologies	Results reveal that several DDoS attacks can be efficiently identified and mitigated, and networks can recover quickly by using FADM
Giri et al. [38]	Blockchain and software-defined network is used to support a shared DDoS mitigation architecture across various network domains	Mitigation	The proposed technique helps to reduce the complexities of shielding a hybridized enterprise against the impacts of DDoS attacks	The proposed architecture would be evaluated with and without blockchain applications to determine the system's effectiveness in the future	Experimental results reveal that SDN's capacity made a network decentralized, while blockchain's distributed nature gave a viable approach to collaborative DDoS mitigation

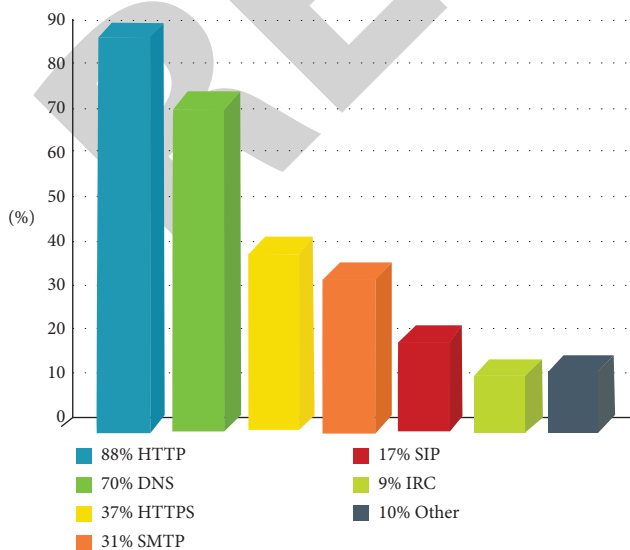


FIGURE 5: Common types of DDoS attacks on the application layer.

attacks as well as their special properties, defense mechanisms, and consequences.

Bojović et al. [41] anticipated a hybrid method for detecting DDoS attacks that merge both feature-based and volume-based detection. This study makes a two-fold contribution. The first step is to offer a hybrid technique for detecting DDoS attacks. Second, the proposed approach's performance was assessed and compared to two existing approaches. As a result, the data sets for evaluation were generated through a monitored Denial of Service experiment on a genuine network. An ICMP flood attack, which represented a high-level attack, a TCP SYN flooding attack, which represented a low-level attack, were used in the experiment. The technique depends on the additional parameter applied to two-time series, one of which contains information values and the other of which contains the number of packets. As a result, the purpose technique combined quantity-based and attribute-based detection. For both time series, the authors employed two EMA indicators,

TABLE 2: Important properties of defense techniques against application-layer DDoS attacks.

Ref	Main idea	Type	Strength	Future work	Results
Bhosale et al. [40]	Examined characteristics, security mechanisms of DDoS attacks, and their impact on web services	Prevention	Application-layer DDoS attacks and their impact on modern online services are presented very effectively	Due to the rapid increase in application-layer attacks, further research is needed	The characteristics of application-layer attacks and their effects were explored and investigated effectively
Bojović et al. [41]	Reduce the packet recognition time to understand the attack pattern	Detection	Presented a hybrid strategy for detecting DDOS attacks, also evaluated and compared them with two other methodologies	By adding a preprocessing module in the proposed technique, it would enable its application in overloaded links connecting huge networks	The technique attains the detection rate of an existing detection system, but it can detect numerous types of attacks better
Asad et al. [42]	Using deep learning techniques to discriminate between normal and malicious traffic flow	Detection	Used accuracy as a performance matrix to evaluate the proposed model on actual Internet traffic	The same strategy can be used to combat other types of DDoS attacks such as those based on UDP and ICMP in the future	Proposed technique correctly detected malicious behavior from packets when a completely new malicious pattern was used
Patani and Patel [43]	Detecting attacks on application and transport layer	Detection	This method uses CAPTCHA in a variety of ways to authenticate the source of genuine and malicious traffic	The suggested effort would simulate the results using data sets and technologies, as an addition to this paper in the future	This technique can detect strangely or faked IP addresses

one with a small duration and another with a large duration. On the other hand, numerous indicators were utilized to evaluate the performance, such as Precision, F1 Score, Recall, and Detection Rate. The operational curve of the receiver has been provided too. A traditional designed technique for detecting SYN flooding attacks is utilized for comparison, while the other utilized method is a common entropy-based irregularity detection technique.

Asad et al. [42] presented a new deep neural network for identifying network flows as normal or abnormal. The purpose technique uses a feedforward back-propagation design with seven secret layers. The authors tested this method for DDoS detection using the most up-to-date Canadian data set (CIC IDS 2017). The F1 Score at the test provided a value of 0.99, indicating that the experimental results were accurate in terms of Recall and Precision.

Among all the varieties of DDoS, a Flooding Attack poses the greatest threat to a network/Internet. DDoS attacks do not require a lot of computational effort to target destination servers and networks. The purpose of intrusion detection or intrusion and prevention system research is to develop a mechanism to counter undetected attacks on the application and transport layers. At the application and transport layers of TCP/IP, Patani and Patel [43] identified many vulnerabilities that explicitly aim to disrupt lawful users' access to services. The goal of this research is to offer a technique based on existing organizations for detecting and analyzing synchronous and nonsynchronous traffic flow while monitoring the network in time slots. Moreover, this method utilizes CAPTCHA in a variety of ways to authenticate the origins of genuine and malicious traffic.

We comparatively analyzed some important characteristics of defense techniques against application and network layer DDoS attacks in Table 2.

After analyzing and comparing defense techniques against application-layer DDoS attacks in Table 2, we conclude that Bojović et al., [41] and Patani and Patel's [43] detection techniques are the best. Bojović et al. [41] proposed method not only reduces the packet recognition time, which helps to detect attack patterns rapidly but also detects several types of DDoS attacks. Similarly, Patani and Patel's [43] purpose detection technique used a novel approach called CAPTCHA to authenticate the source of malicious and regular traffic flow and also can detect fake and suspicious IP addresses effectively.

5.4. Defense Techniques against DDoS Attacks on SMEs.

Organizations are becoming increasingly dependent on modern information and communication technologies, but they are also revealing themselves to a wide range of risks and weaknesses. Especially, Small and Medium Businesses are good targets for DDoS attacks because of their insufficient cybersecurity and lack of underlying competence. Due to the limited financial resources available to SMEs, it is critical to develop technological solutions that are not only effective but also cost-efficient.

Sharifi et al. [44] used the case of a current technology SME to develop a cloud-security strategy that might use at CloudPlus to enable rapid detection and prevention of DDoS attacks. The SME is a proposed technology that was launched in 2017. The goal of this study is to draw attention to the identification and prevention of DDoS attacks on Small and Medium Businesses. The SME specializes in cloud computing solutions such as Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS). This company offers low-cost, high-end cloud computing services and apps.

TABLE 3: Some important properties of DDoS attacks on SMEs.

Ref	Main idea	Type	Strength	Future work	Results
Sharifi et al. [44]	Developing an optimal anti-DDoS solution that ensures early detection and total prevention	Detection and prevention	Presented best measures for the cloud. Based security against DDoS attacks.	The presented technique is an initial step in this area of study. Therefore, constant research would reduce this research gap.	Results reveal that the proposed cybersecurity architecture enables cloud plus to identify and prevent DDoS attacks in the future

Furthermore, the organization was subjected to a series of cyberattacks due to a lack of suitable cybersecurity structure and skills. Until it recruited third-party cybersecurity specialists, the corporation was unable to detect DDoS attacks. As a result, CloudPlus realized it needed a cybersecurity architecture to help secure its cloud services from potential threats. The basic objective of this article is to develop and construct a cybersecurity infrastructure that will allow CloudPlus to defend against DDoS attacks in the future. As part of the investigation, an initial security audit was undertaken to identify the present holes in CloudPlus's cloud architecture. After that, a quick analysis of the literature on DDoS attacks and the best methods for detecting and preventing is presented. The proposed technical solution consists of three layers: cloud signaling, firewalling, and third-party cloud security through Akamai. The solution is created in such a way that it may be copied by any cloud-based small and medium enterprise.

We comparatively analyzed some important characteristics of defense techniques against DDoS attacks on small and medium enterprises in Table 3.

5.5. Defense Techniques against DDoS Attacks on IoT. The IoT is extremely susceptible to DDoS attacks as well as employed to initiate DDoS against other victims. The amount of DDoS attacks is expanding very rapidly with time. In 2013 and 2015, it was found to be functioning at a rate of 100 Gbps. In 2016, and 2017, there was a growth in attack levels of 800 Gbps and 1.35 Tbps, correspondingly [45]. DDoS attacks have become more deadly since the arrival of semi -IoT devices. Hackers can now take advantage of IoT devices' inadequate security implementation to capture them and utilize them to target the expected server or network. Organizations' investment in IoT security has been steadily increasing. It has been noticed that as the cost of deploying additional IoT devices rises, so does the number of assaults. According to a Gartner survey done in 2018, approximately 20% of firms reported having suffered at minimum one DDoS attack. Security investment on the Internet of Things was 1.5 billion dollars in 2018 and is expected to reach 3.1 billion dollars by 2021 as shown in Figure 6 [46]. Industry spending on IoT security is increasing, indicating the necessity for inventive protection methods for the Internet of Things environment to be considered.

DDoS protecting methods against IoT device attacks have become a hot topic, with a variety of approaches proposed and deployed. However, there have been no DDoS mitigation solutions for network side devices that are

inexpensive and low performance. As a result, Yaegashi et al. [47] presented a lightweight Distributed Denial of Service mitigation system on the network side that makes use of the restricted assets of low-cost devices like home gateways. The suggested scheme's purpose is to make it simple to identify and lessen flood attacks. It leveraged vacant queue resources to identify malevolent flows by rearranging queue distribution at random and discarding packets from the identified flows. It allows for the easy detection and adjustment of flooding attacks like the UDP flood. The suggested approach detected more than 100 flows by utilizing seven queues for queue transfer as proven by a computer model.

The greatest serious risk to the accessibility of Internet services is DDoS. A botnet having 0.01% of the IoT's 50 billion linked devices is sufficient to initiate a huge Distributed Denial flooding attack that could drain assets and disrupt any victim. Traditional anti-DDoS solutions, on the other hand, are limited in their detection capabilities due to the flexibility of user apparatus and the unique peculiarities of traffic flow in mobile networks. Nguyen et al. [48] presented MECPASS, a unique collaborative DDoS defensive architecture, to minimize attack traffic from mobile devices. Two sorting orders were used in the purpose design. Firstly, edge computation servers, for example, local nodes use filters to try to avoid spoofing attacks and unusual traffic as much as feasible. Moreover, by regularly combining data from the local nodes, worldwide analyzers are placed at cloud servers, for example, main nodes categorize the traffic of the completely examined network and reveal irregular activities. They tested the system's efficiency from the perspective of web servers against various sorts of application-layer DDoS attacks.

The study [49] presented a module for event detection that may have been installed in IoT devices. The suggested module focuses on system behavior during DDoS assaults and identifies it using information collected from NTP, which has been utilized in time synchronization services. They carried out demonstration experiments using the new module, simulating DDoS assaults. The module's benefit is that, unlike current ones, it does not need more expensive machines (i.e., monitoring server) or frequent maintenance requiring technical knowledge. The module was implemented into a compact board computer, and demonstration experiments were conducted. The result shows that the proposed module achieves high recall and precision values, indicating its usefulness in the real-time event. The module has been integrated onto a tiny board computer, and demonstration tests have been carried out. The results reveal that the suggested module has a high recall and precision value, showing its use in actual event detection on IoT. As

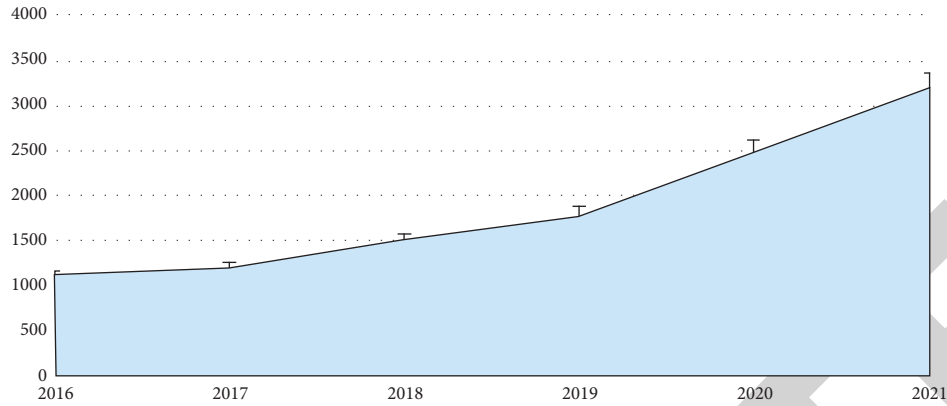


FIGURE 6: A rapid increase in organizations' spending (in billions of dollars) regarding IoT security in recent years [46].

TABLE 4: Summary of DDoS prevention techniques for IoT.

Ref	Main idea	Type	Strength	Future work	Results
Yaegashi et al. [47]	Proposing a lightweight DDoS mitigation system using low-cost devices and limited resources	Detection and mitigation	DDoS attacks are easily mitigated, especially in low-cost devices with limited resources	The proposed technique has sufficient flexibility for the network edge. Therefore, continual development in this research area is required	The proposed method detected illegal flows utilizing less budget devices with constrained resources, and the results match the theoretic predictions
Nguyen et al. [48]	Minimizing attack traffic from mobile devices, this study presents MECPASS, a unique collaborative DDoS protection architecture	Prevention	Proposed design can be implemented at any detection algorithm if the hardware permits	The proposed technique would be supported in the investigation under diverse network situations in the future	Results reveal MECPASS efficiently protected an Internet service provider's main network from compromised user equipment's trash traffic
	An event detection module has been proposed that focused on system behavior during DDoS assaults and detected it using information acquired from the NTP utilized in the synchronization service				

the result of different research, the accuracy value is 0.92 and the recall value is 1.0, indicating a desirable balance of strictness and completion. This implies that the built module is helpful in detecting actual events on IoT.

The authors in [50] derived the IoT environment's joint entropy characteristic and offer a DDoS detection approach based on the ELM algorithm. The proper excitation function and hidden layer nodes have been chosen as the input by experimental analysis and comparison. The suggested approach of identifying DDoS assaults based on ELM performed better than other machine learning methods in the testing, with a lower training period, a reduced false precision rate, and an improved detection rate.

We comparatively analyzed some important characteristics of defense techniques for DDoS attacks on IoT devices in Table 4.

After analyzing and comparing the above defense techniques against DDoS attacks using IoT devices in

Table 4, we conclude that Yaegashi et al.'s [47] and Nguyen et al.'s [48] purpose detection, prevention, and mitigation techniques performed best in their own ways. Yaegashi et al. [47] presented a lightweight DDoS detection and mitigation system that uses inexpensive devices with limited resources to detect and mitigate malicious traffic flow efficiently. Similarly, Nguyen et al. [48] proposed a prevention mechanism that efficiently protects ISP's main networks from malicious traffic and reduces attack traffic from mobile devices. The proposed technique can be adopted by any detection algorithm.

5.6. Defense Techniques against DDoS Attacks Using Path Identifiers. The Path Identifiers (PIDs) as interdomain routing objects are widely utilized to prevent flooding attacks. However, Path Identifiers are globally published, an end user identifies the PIDs for each node in the network,

TABLE 5: Summary of D-PID-based DDoS prevention techniques.

Ref	Main idea	Type	Strength	Future work	Results
Luo et al. [49]	Purposing a dynamic path identifier mechanism's design, implementation, and assessment	Prevention	Increases the expense of attacking and makes it easier to recognize the attacker swiftly	This research is the initial step towards adopting D-PIDs; more research in this area is required	D-PID successfully mitigated DDoS attacks, according to modeling and experiment data
Punidha et al. [50]	Introduces and implements a novel node blocking mechanism to prevent DDOS attacks	Prevention	Minimized the effects of the attacks and properly maintained by providing the conditions required to prevent DDoS attacks	Further research to use D-PID for reducing DDoS attacks can bring more improvement	When the unauthorized entrance and attack happened, these measures defended the traffic from a significant number of DDoS traffic

and hackers can initiate Distributed DDoS flooding attacks, just as they can on the current Internet. Therefore, path identifiers are converted to only being recognized by the network and are kept very hidden by end users; they can only transmit packets to the destination with certain content, and the route identifier is packed into the headers of the encrypted packets. With the help of a router, such packets are passed to another network; the router passes the encrypted packets to the designated network based on the headers. Although the PIDs used in current approaches are static, so attackers can easily execute DDOS attacks by creating new filters like PIDs built on current ones and even attain the link identifiers by using reverse engineering to execute DDoS flooding attacks. Similarly, attackers can use static path identifiers to initiate DDoS flooding attacks.

Luo et al. [49] described the architecture, execution, and assessment of a Dynamic PID (D-PID) technique to overcome this issue. In Dynamic PID, two nearby domains update their PIDs and establish the latest PIDs into the data plane for packet dispatching on a regular basis. However, if the hacker successfully acquires the PIDs from its victim system and transmits the malevolent packets, the PIDs will become worthless after a specific length of time, and the network will discard any additional attacking packets. Furthermore, attempting to obtain fresh PIDs while continuing a DDoS flooding attack increases not only the attacking cost but also makes it easier to discover the hacker. To prove Dynamic PIDs, they built a 42-node prototype with six domains and ran extensive simulations to assess its efficiency and costs.

Punidha et al. [50] proposed and implemented a new node blocking technique to prevent DDoS attacks. In this paper, the improved design of the dynamic path identifier is presented along with its implementation and evaluation. As a result, adjacent domains negotiate PIDs to explain how to keep communication continuing when path identifiers change. To demonstrate this procedure, a 42-node network with six domains was used to test the Dynamic-Path Identifiers' viability. This technique minimizes the consequences of attacks and ensures that they are perfectly maintained by establishing conditions that resist DDoS attacks. The suggested system includes a method for identifying client authentication if the user enters more than one condition. If the user enters more than one condition, the

user is saved as an attacker and added to the blocked list, and the service is provided to that identified user who entered incorrectly.

We comparatively analyzed some important characteristics of Dynamic-Path Identifiers (D-PID)-based defense techniques against DDoS attacks in Table 5.

After analyzing and comparing the above Dynamic-Path Identifier-based defense techniques in Table 5, we conclude that Punidha et al. [50] proposed prevention mechanism against DDoS attacks is the best. They utilized a novel node blocking technique to prevent unauthorized attempts and defend against many DDoS attacks.

6. Conclusion

In a DDoS attack, a single host is targeted by many computer systems from various locations using multiple IP addresses. Hackers can shut down the victim services for a specific period of time using a DDoS attack, which can last for a number of days, weeks, or months, reliant upon the type of DDoS attack. DDOS attacks are designed to make a computer or network resource inaccessible to their authorized users. Despite the years of researchers coping with DDoS attacks, they continue to exist even with more intensity and have an impact. We discussed the different types of DDoS attacks as well as the motivations behind them. We have discussed the detailed classification of DDoS attacks and their consequences of them. In addition, our literature evaluation covers the defense approaches for application- and transport-layer DDoS attacks as well. Additionally, after deeply analyzing the different researchers' work, we concluded that the attacker can cause the following damage to the target:

- (i) Economic loss to the victim since users will be unable to utilize services during the attack.
- (ii) Negative impact on the company's future: the target would appear to have security flaws, causing customers to lose faith.
- (iii) If user information has been breached or the target failed to satisfy service-level agreements because of the attack, there would be a legal prospect.

To avoid such things, we should implement proper countermeasures to combat DDoS attacks. In this survey

paper, we reviewed cutting-edge defense techniques which are currently being utilized to quickly defend against DDoS attacks to minimize the damage to the targeted system and its legitimate users. We performed an in-depth analysis of current defense techniques against DDoS attacks while comparing each technique in tabular form to find out the best one among them. Moreover, the specific prevention techniques for IoT and SDN devices are elaborated in detail. This review will be helpful for future researchers in getting domain knowledge of different types of DDoS attacks and various efficient defense techniques to detect, mitigate, and prevent them.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest to report regarding this research.

References

- [1] K. Singh, S. C. Guntuku, A. Thakur, and C. Hota, "Big data analytics framework for peer-to-peer botnet detection using random forests," *Information Sciences*, vol. 278, pp. 488–497, 2014.
- [2] J. Liu, Y. Lai, and S. Zhang, "A detection and defense system for DDoS attack in SDN," in *Proceedings of the 2017 International Conference on Cryptography, Security and Privacy*, pp. 107–111, Wuhan, China, March 2017.
- [3] V. Stanciu and A. Tinca, "Exploring cybercrime - realities and challenges," *Journal of Accounting and Management Information Systems*, vol. 16, no. 4, pp. 610–632, 2017.
- [4] N. Tariq, M. Asim, F. Al-Obeidat et al., "The security of big data in fog-enabled IoT applications including blockchain: a survey," *Sensors*, vol. 19, no. 8, pp. 1788–88, 2019.
- [5] N. Abbas, M. Asim, N. Tariq, T. Baker, and S. Abbas, "A mechanism for securing IoT-enabled applications at the fog layer," *Journal of Sensor and Actuator Networks*, vol. 8, 2018.
- [6] M. Faheem, S. B. H. Shah, R. A. Butt et al., "Smart grid communication and information technologies in the perspective of Industry 4.0: opportunities and challenges," *Computer Science Review*, vol. 30, pp. 1–30, 2018.
- [7] N. Perloth, "Hackers use new weapons to disrupt major websites across us," *The New York Times*, vol. 21, 2016.
- [8] C. Koliass, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: Mirai and other botnets," *Computer*, vol. 50, no. 7, pp. 80–84, 2017.
- [9] M. Anwar, A. Abdullah, A. Altameem et al., "Green communication for wireless body area networks: energy aware link efficient routing approach," *Sensors*, vol. 18, no. 10, 3237 pages, 2018.
- [10] J. Liu, Y. Xiao, K. Ghaboosi, H. Deng, and J. Zhang, "Botnet: classification, attacks, detection, tracing, and preventive measures," *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, no. 1, Article ID 692654, pp. 1–11, 2009.
- [11] K. N. Qureshi, E. Ahmad, M. Anwar, K. Z. Ghafoor, and G. Jeon, "Network Functions Virtualization for Mobile Core and Heterogeneous Cellular Networks," *Wireless Personal Communications*, vol. 2021, 2021.
- [12] A. Ahmed, K. Qureshi, M. Anwar, F. Masud, J. Imtiaz, and G. Jeon, "Link-based Penalized Trust Management Scheme for Preemptive Measures to Secure the Edge-Based Internet of Things Networks," *Wireless Networks*, vol. 2022, 2022.
- [13] S. Naseem, A. Alhudhaif, M. Anwar, K. N. Qureshi, and G. Jeon, "Artificial General Intelligence Based Rational Behavior Detection Using Cognitive Correlates for Tracking Online Harms," *Personal and Ubiquitous Computing*, vol. 2022, 2022.
- [14] M. Anwar, F. Masud, R. Aslam Butt, S. Mahdaliza Idrus, M. Nazir Ahmad, and M. Yazid Bajuri, "Traffic priority-aware medical data dissemination scheme for IoT based WBASN healthcare applications," *Computers, Materials & Continua*, vol. 71, no. 3, pp. 4443–4456, 2022.
- [15] Rizwan Aslam Butt, M. Faheem, M. Anwar, K. H. Mohammadani, and S. M. Idrus, "Traffic aware cyclic sleep based power consumption model for a passive optical network," *International Journal of Numerical Modelling: Electronic Networks, Devices and Fields*, 2022.
- [16] A. Sadiq, M. Anwar, R. A. Butt et al., "A review of phishing attacks and countermeasures for internet of things-based smart business applications in industry 4.0," *Human Behavior and Emerging Technologies*, vol. 3, no. 5, pp. 854–864, 2021.
- [17] M. Anwar, A. H. Abdullah, A. H. Abdullah, R. R. Masud, and F. Ullah, "CAMP: congestion avoidance and mitigation protocol for wireless body area networks," *International Journal of Integrated Engineering*, vol. 10, no. 6, pp. 59–65, 2018.
- [18] M. Anwar, A. H. Abdullah, R. A. Butt, M. W. Ashraf, and K. N. Qureshi, "Securing data communication in wireless body area networks using digital signatures," *Technical Journal*, vol. 23, no. 2, pp. 50–55, 2018.
- [19] M. Anwar, A. H. Abdullah, K. N. Qureshi, and A. H. Majid, "Wireless body area networks for healthcare applications: an overview," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 15, no. 3, pp. 1088–1095, 2017.
- [20] U. Shafiq, M. K. Shahzad, M. Anwar, Q. Shaheen, M. Shiraz, and A. Gani, "Transfer Learning Auto-Encoder Neural Networks for Anomaly Detection of DDoS Generating IoT Devices," *Security and Communication Networks*, vol. 2022, 2022.
- [21] S. Amjad, M. Younas, M. Anwar, Q. Shaheen, M. Shiraz, and A. Gani, "Data Mining Techniques to Analyze the Impact of Social Media on the Academic Performance of High School Students," *Wireless Communications and Mobile Computing*, vol. 2022, 2022.
- [22] M. Kamran, M. Malik, M. W. Iqbal, M. Anwar, and M. Aqeel, "Web Simplification Prototype for Cognitive Disable Users," *Human Behaviour and Emergency Technology*, vol. 2022, 2022.
- [23] A. H. Majid, M. Anwar, and M. W. Ashraf, "Classified structures and cryptanalysis of wg-7, wg-8 and wg-16 stream ciphers," *Technical Journal*, vol. 23, no. 2, pp. 50–55, 2018.
- [24] K. N. Qureshi, A. H. Abdullah, R. W. Anwar, M. Anwar, and K. M. Awan, "Aegrp: an enhanced geographical routing protocol for vanet," *Jurnal Teknologi*, vol. 78, no. 4-3, pp. 83–88, 2016.
- [25] K. N. Qureshi, A. Hanan Abdullah, A. Mirza, and R. W. Anwar, "Geographical forwarding methods in vehicular ad hoc networks," *International Journal of Electrical and Computer Engineering*, vol. 5, no. 6, pp. 1407–1416, 2015.
- [26] Abdul Qahar, K. Zen, M. Anwar, and A. Khan, "Energy Efficient Millimeter Wave Backhauling in 5G Heterogeneous

- Networks,” in *Proceedings of the 2021 International Conference on Innovative Computing (ICIC)*, IEEE, Lahore, November 2021.
- [27] Ammara Karim Noon, O. Aziz, I. Zahra, and M. Anwar, “Implementation of Blockchain in Healthcare: A Systematic Review,” in *Proceedings of the 2021 International Conference on Innovative Computing (ICIC)*, IEEE, Lahore, November 2021.
- [28] T. Kawamura, M. Fukushi, Y. Hirano, Y. Fujita, and Y. Hamamoto, “An NTP-based detection module for DDoS attacks on IoT,” in *Proceedings of the 2017 IEEE International Conference on Consumer Electronics - Taiwan (ICCE-TW)*, pp. 15–16, ICCE-TW, Taiwan, June 2017.
- [29] Z. Li, L. Wei, W. Li et al., “Research on DDoS attack detection based on ELM in IoT environment,” in *Proceedings of the 2019 IEEE 10th International Conference on Software Engineering and Service Science (ICSESS)*, pp. 144–148, China, October 2019.
- [30] A. Marques da Silva Cardoso, R. Fernandes Lopes, A. Soares Teles, and F. Benedito Veras Magalhaes, “Poster abstract: real-time DDoS detection based on complex event processing for IoT,” in *Proceedings of the 2018 IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation (IoTDI)*, pp. 273–274, Orlando, FL, USA, April 2018.
- [31] R. Yaegashi, D. Hisano, and Y. Nakayama, “Light-Weight DDoS mitigation at network edge with limited resources,” in *Proceedings of the 2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC)*, vol. 2021, Las Vegas, NV, USA, January 2021.
- [32] D. Yin, L. Zhang, and K. Yang, “A DDoS attack detection and mitigation with software-defined internet of things framework,” *IEEE Access*, vol. 6, Article ID 24694, Mcc, 2018.
- [33] Y. Jia, F. Zhong, A. Alrawais, B. Gong, and X. Cheng, “FlowGuard: an intelligent edge defense mechanism against IoT DDoS attacks,” *IEEE Internet of Things Journal*, vol. 7, no. 10, pp. 9552–9562, 2020.
- [34] A. Prakash and R. Priyadarshini, “An intelligent software defined network controller for preventing distributed denial of service attack,” in *Proceedings of the 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT)*, pp. 585–589, IEEE, Coimbatore, India, April 2018.
- [35] Y.-C. Wang and Y.-C. Wang, “Efficient and low-cost defense against distributed denial-of-service attacks in SDN-based networks,” *International Journal of Communication Systems*, vol. 33, no. 14, Article ID e4461, 2020.
- [36] T. M. Nam, P. H. Phong, T. D. Khoa et al., “Self-organizing map-based approaches in DDoS flooding detection using SDN,” in *Proceedings of the 2018 International Conference on Information Networking (ICOIN)*, pp. 249–254, IEEE, Chiang Mai, Thailand, January 2018.
- [37] D. Hu, P. Hong, and Y. Chen, “FADM: DDoS flooding attack detection and mitigation system in software-defined networking,” in *Proceedings of the 2017 IEEE Global Communications Conference (GLOBECOM)*, pp. 1–7, IEEE, Singapore, December 2017.
- [38] N. Giri, R. Jaisinghani, R. Kriplani, T. Ramrakhyani, and V. Bhatia, “Distributed denial of service (DDoS) mitigation in software defined network using blockchain,” in *Proceedings of the Third International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, pp. 673–678, IEEE, Palladam, India, December 2019.
- [39] D. McPherson, R. Dobbins, M. Hollyman, and C. Labovitz, “Worldwide infrastructure security report,” *Arbor Networks*, vol. 5, 2010.
- [40] K. S. Bhosale, M. Nenova, and G. Iliev, “The distributed denial of service attacks (DDoS) prevention mechanisms on application layer,” in *Proceedings of the 13th International Conference on Advanced Technologies, Systems and Services in Telecommunications (TELSIKS)*, pp. 136–139, IEEE, Niš, Serbia, October 2017.
- [41] P. D. Bojović, I. Bašičević, S. Ocovaj, and M. Popović, “A practical approach to detection of distributed denial-of-service attacks using a hybrid detection method,” *Computers & Electrical Engineering*, vol. 73, pp. 84–96, 2019.
- [42] M. Asad, M. Asim, T. Javed, M. O. Beg, H. Mujtaba, and S. Abbas, “Deepdetect: detection of distributed denial of service attacks using deep learning,” *The Computer Journal*, vol. 63, no. 7, pp. 983–994, 2020.
- [43] N. Patani and R. Patel, “A mechanism for prevention of flooding based ddos attack,” *International Journal of Computational Intelligence Research*, vol. 13, no. 1, pp. 101–111, 2017.
- [44] A. Z. Sharifi, H. Zaheer, M. F. Azizi, and J. Faizi, “Detection and prevention of distributed denial of service attacks in SMEs: the case of CloudPlus,” in *Proceedings of the 2019 Sixteenth International Conference on Wireless and Optical Communication Networks (WOCN)*, pp. 1–4, IEEE, Bhopal, India, December 2019.
- [45] S. Waterman, “DDoS Attacks Growing Faster in Size, complexity—Arbor Report,” 2018, <http://edscoop.com/>.
- [46] Gartner, “Worldwide IoT security spending will reach \$1.5 billion in 2018,” 2018, <https://www.gartner.com/>.
- [47] R. Yaegashi, D. Hisano, and Y. Nakayama, “Lightweight DDoS mitigation at network edge with limited resources,” in *Proceedings of the 2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC)*, pp. 1–6, IEEE, Las Vegas, NV, USA, January 2021.
- [48] V. L. Nguyen, P.-C. Lin, and R.-H. Hwang, “MECPASS: distributed denial of service defense architecture for mobile networks,” *IEEE Network*, vol. 32, no. 1, pp. 118–124, 2018.
- [49] H. Luo, Z. Chen, J. Li, and A. V. Vasilakos, “Preventing distributed denial-of-service flooding attacks with dynamic path identifiers,” *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 8, pp. 1801–1815, 2017.
- [50] R. Punidha, K. Pavithra, and R. Swathika, “Preserving DDoS attacks using node blocking algorithm,” *International Journal of Pure and Applied Mathematics*, vol. 119, no. 15, pp. 633–640, 2018.