# Machine Learning Approaches for Combating Distributed Denial of Service Attacks in Modern Networking Environments

## AHAMED ALJUHANI[ID]
Department of Computer Information Systems, University of Tabuk, Tabuk 71491, Saudi Arabia

e-mail: a_aljuhani@ut.edu.sa

**ABSTRACT** A distributed denial of service (DDoS) attack represents a major threat to service providers. More specifically, a DDoS attack aims to disrupt and deny services to legitimate users by overwhelming the target with a massive number of malicious requests. A cyberattack of this kind is likely to result in tremendous economic losses for businesses and service providers due to increasing both operating and financial costs. In recent years, machine learning (ML) techniques have been widely used to prevent DDoS attacks. Indeed, many defense systems have been transformed into smart and intelligent systems through the use of ML techniques, which allow them to defeat DDoS attacks. This paper analyzes recent studies concerning DDoS detection methods that have adapted single and hybrid ML approaches in modern networking environments. Additionally, the paper discusses different DDoS defense systems based on ML techniques that make use of a virtualized environment, including cloud computing, software-defined network, and network functions virtualization environments. As the development of the Internet of Things (IoT) has been the subject of significant research attention in recent years, the paper also discusses ML approaches as security solutions against DDoS attacks in IoT environments. Furthermore, the paper recommends a number of directions for future research. This paper is intended to assist the research community with the design and development of effective defense systems capable of overcoming different types of DDoS attacks.

**INDEX TERMS** DDoS attacks and detection, Internet of Things (IoT), machine learning (ML), network functions virtualization (NFV), software-defined network (SDN).

## I. INTRODUCTION

Distributed denial of service (DDoS) attacks have become increasingly sophisticated in recent years. In fact, a single DDoS attack is now able to infect a large group of devices. More specifically, zombies target the victim and deny services to legitimate users by inundating the network with requests [1]. Attackers install malicious software, which is known as the master DDoS, in an effort to gain control over a group of compromised machines located within the same network [2]. The attackers use these zombies as an army, remotely instructing them to simultaneously attack the victim, thereby rendering the service unavailable to valid users. A related new concept, namely DDoS as a service (DDoSaaS) [3], reduces the technical challenges associated with implementing an attack through the use of booters or stressers. A DDoSaaS attack utilizes a number of powerful

servers to transmit a massive amount of attack traffic to a specific target [4]. The owners of pre-staged botnets allow their clients to use the DDoSaaS approach to attack specific webservers. A client has to identify a webpage link or an Internet Protocol (IP) address in order for a specific location to be targeted. The costs associated with a DDoSaaS attack starts as little as six dollars, depending on the contracted duration of the attack [107]. For every hour that a system is down, businesses suffer significant losses of revenue and also incur additional operating expenses due to recovery efforts [5]. Fig. 1 presents the general architecture of a DDoS attack.

Machine learning (ML) techniques are considered to be a viable means of detecting DDoS attacks [6]. Such techniques learn the patterns behind attacks in order to detect them before network recourses become unavailable [7]. Modern defense systems make use of ML techniques alongside other detection models, including intrusion detection systems (IDS) and host-based intrusion detection systems (HIDS), in an effort

---

The associate editor coordinating the review of this manuscript and approving it for publication was Quansheng Guan[ID].
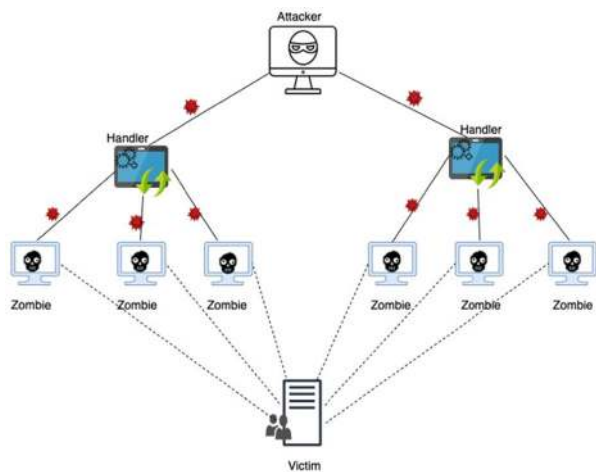
**FIGURE 1. Architecture of a DDoS attack.**

to effectively respond to complicated cyberattacks such as DDoS attacks [8].

The remainder of this paper is organized as follows. Section II discusses a number of recent DDoS attacks as well as their impacts on businesses. Section III sets out the aims and novel contributions of the present work, while section IV discusses the findings of previous studies relevant to this topic. Section V establishes a classification system for DDoS attacks and then describes each type of attack. Section VI details types of ML techniques. Section VII and VIII provide a broad overview of the potential uses of ML to combat DDoS attacks in traditional and modern networking environments, including cloud computing, software-defined network (SDN), network functions virtualization (NFV), and Internet of Things (IoT) environments. Section IX discusses a diverse range of DDoS mitigation techniques. Section X presents the discussion and research challenges. Finally, section XI concludes the paper.

## II. BACKGROUND AND MOTIVATION

Attackers continue to find new mechanisms and techniques for tricking defense systems, thereby exploiting the available software for illegal purposes and causing damage to service providers. Recently, emerging technologies, for example, the IoT, have been used to launch powerful and highly effective DDoS attacks [9].

The magnitudes of DDoS attacks have increased over the last decade. For example, in 2012, a botnet-based DDoS attack flooded a group of US banks with up to 75 Gbps of malicious traffic [10], while in 2013, a nonprofit organization named Spamhaus suffered a massive DDoS attack involving 300 Gbps of traffic [11]. In 2014, an unnamed Internet service provider was attacked by a network time protocol that generated traffic of up to 400 Gbps, which led to it becoming inaccessible to clients [12]. In October 2016, the Mirai botnet attacked Dyn, a web application security company, with up to 1.2 Tbps of malicious traffic [13]. Further, a remarkable DDoS attack occurred in 2018, when GitHub experienced an

immense flood of around 1.35 Tbps of generated traffic [14]. Amazon web services (AWS) was attacked by a reflection DDoS attack that make use of a third-party server to generate massive amount of traffic with up to 2.3 Tbps [112], which is considered to represent the largest DDoS attack to date [113]. Fig. 2 demonstrates the increasing magnitudes of DDoS attacks in recent years [10]– [15], [112].
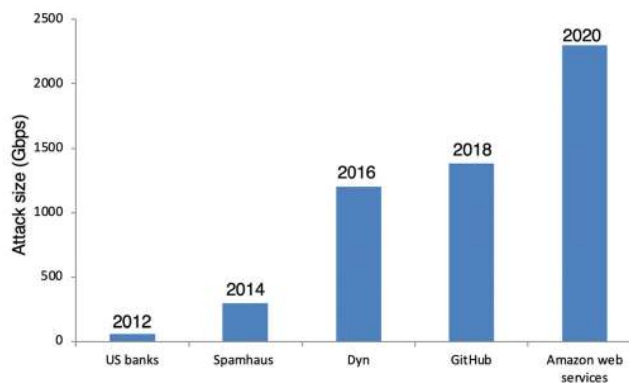


**FIGURE 2. Increasing magnitudes of DDoS attacks.**

DDoS attacks have a significant impact on businesses due to the associated operating and financial costs [16]. A business's sensitivity to the loss of its intended users intensifies after it experiences a cyberattack such as a DDoS attack. Fig. 3 shows the effectiveness of DDoS attacks, which are known to result in a 69% increase in operational expenses, a 33% decrease in revenue, a 31% increase in customer attrition, and a 14% increase in employee turnover [9].
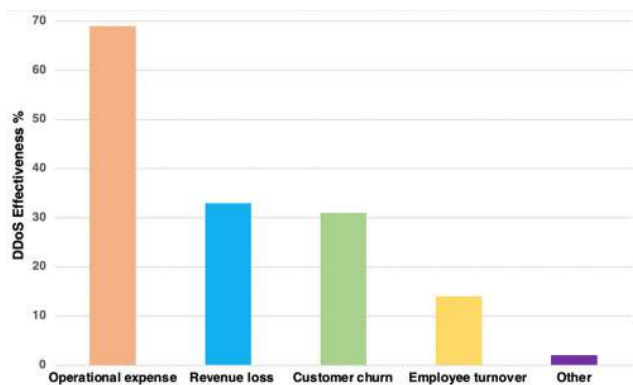


**FIGURE 3. The effectiveness of DDoS attacks.**

Prior studies have proposed various approaches for dealing with DDoS attacks. The majority of these approaches use several ML algorithms to defeat DDoS attacks. Additionally, hybrid solutions, which combine two or more different ML algorithms, have been proposed. The present study aims to assist the research community with the design and development of effective new solutions to DDoS attacks, as such solutions would help service providers to reduce their risk of falling victim to cyberattacks.

## III. AIMS AND CONTRIBUTIONS

A number of prior studies have investigated the use of ML techniques in different fields, although little research has been conducted to date with regard to DDoS attacks. Therefore, the present paper extends the scope of the existing research by focusing on ML approaches to combating DDoS attacks in modern networking environments. As a result, this paper makes several important contributions to the research in this area:

- It provides a broad overview of the various applications of ML/DL in terms of combatting different types of DDoS attacks.
- It offers an in-depth investigation of the most relevant DDoS defense systems based on the use of ML/DL techniques in different environments, including cloud computing, SDN, and NFV environments.
- It assesses defense systems that have recently employed ML/DL techniques in IoT environments.
- It classifies and analyzes the results of recent studies with regard to the type of DDoS attack, the type of ML, the dataset, and the evaluation metric(s).
- It highlights the research challenges facing the application of ML/DL approaches in modern networking environments that need to be investigated.

## IV. RELATED WORK

A number of prior studies have discussed the use of various ML approaches to combat DDoS attacks. However, the majority of such studies have discussed the matter in relation to only a traditional or specific network environment. In addition, some previous studies have focused on the use of ML techniques to combat outdated types of attacks, which are no longer of relevance to service providers. Moreover, several studies that have discussed DDoS attacks have focused solely on cloud computing environments [17]–[19] with only limited detail concerning the utilized ML approaches being provided and no other modern networking environments being considered.

Vishwakarma *et al.* [20] did discuss DDoS attacks in both IoT and SDN environments as well as the use of different ML algorithms. However, their study was limited to those two environments. Osanaiye *et al.* [108] reviewed DDoS defense systems in the context of cloud computing. The authors provided various anomaly detection techniques that were published between January 2010 and December 2015. The article also provided research challenges and directions for future work. However, the study was limited to the cloud environment, and the authors reviewed approaches that were published long ago. Salim *et al.* [110] reviewed DDoS defense systems in the context of the IoT environment. The authors provide a comprehensive review of DDoS defense systems in the IoT domain and detailed different attack methods and tools that have been used in this environment. In addition, the authors suggested criteria for implementing effective solutions to secure IoT devices from DDoS attacks.

However, this survey was limited to the IoT environment, and they did not discuss in detail the different uses of ML as mitigation solutions in the face of various DDoS attacks. Chaudhary *et al.* [111] reviewed DDoS defense systems in the context of cloud and fog computing. The authors discussed in depth the DDoS attack strategies, mitigation approaches, and security challenges facing cloud and fog computing. However, most of the reviewed papers that were presented in this article discussed old detection techniques. Another limitation of this work is that the authors did not discuss or mention the use of ML approaches to combat DDoS attacks.

The design and development of a solution for overcoming a DDoS attack should not be limited to a specific type of attack. Attackers have the ability to conduct different types of DDoS attacks and examine a defense system with each type of attack to perform a successful cyberattack. Today, many systems make use of modern technologies due to the advantages this environment offers, including flexibility, scalability, and cost reduction [54], [55]. However, modern networking environments remain vulnerable to a diverse range of DDoS attacks. As some technologies can be combined and integrated for CAPEX and OPEX, it is crucial to provide a comprehensive review of DDoS defense systems based on ML approaches in various modern networking environments. The present study will assist the research community with designing and developing effective and practical new solutions for overcoming DDoS attacks, as such solutions help service providers reduce their risk of falling victim to cyberattacks.

To the best of our knowledge, this is the first study to review, analyze, and classify the uses of ML against DDoS attacks in a diverse range of modern networking environments. Table 1 compares our study with related studies that have been conducted in relation to DDoS defense systems based on ML approaches.

## V. DDoS ATTACK CLASSIFICATION

This section details the state-of-the-art situation with regard to DDoS attacks and explains how they are initialized and conducted. Generally speaking, DDoS attacks represent a means of targeting a victim's network infrastructure and webserver in order to render services unavailable to legitimate clients. DDoS attacks become more complicated when they involve a botnet, that is, a large group of compromised devices that attack a specific target and thus cause its online services to be inaccessible [21]. The following subsections discuss the most common types of DDoS attacks.

### A. HTTP FLOOD ATTACKS

HTTP flood attacks are intended to overwhelm a webserver's resources using a massive number of HTTP requests generated by a botnet [22]. This type of attack has a significant impact on a webserver's resources, including its central processing unit (CPU) and memory [159]. To initiate an HTTP flood attack, a valid transmission control protocol

**TABLE 1.** Comparison of studies concerning DDoS defense systems based on ML approaches.

| Reference | Taxonomy of DDoS attacks | Taxonomy of ML approaches | DDoS defense system based on ML approaches in cloud computing environments | DDoS defense system based on ML approaches in SDN environments | DDoS defense system based on ML approaches in NFV environments | DDoS defense system based on ML approaches in IoT environments |
|---|---|---|---|---|---|---|
| [17] | ✗ | ✗ | ✓ | ✓ | ✗ | ✗ |
| [1] | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ |
| [18] | ✓ | ✗ | ✓ | ✗ | ✗ | ✗ |
| [19] | ✓ | ✗ | ✓ | ✗ | ✗ | ✗ |
| [20] | ✓ | ✓ | ✗ | ✓ | ✗ | ✓ |
| [108] | ✓ | ✓ | ✓ | ✗ | ✗ | ✗ |
| [110] | ✓ | ✗ | ✓ | ✓ | ✗ | ✓ |
| [111] | ✓ | ✗ | ✓ | ✗ | ✗ | ✗ |
| [Our paper] | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

✗ not covered; ✓ covered; ✓ partially covered

(TCP) connection has to be established with a real IP address (i.e., a non-spoofed IP). Once such a connection has been established, the attacker generates an enormous number of HTTP requests, with the aim of flooding the victim's server and depleting its available resources. HTTP flood attacks are difficult to detect [23] because the attacker is able to mimic legitimate users' behavior, making it appear as if the HTTP requests originated from legitimate sources [24]. To conduct this type of attack, attackers use either tools such as bonesi and goldeneye or a script written by professional hackers. To flood the webserver with malicious requests, attackers configure the tool and determine the IP target, number of machines, and number of requests that every machine is instructed to generate simultaneously, causing the webserver to respond very slowly to legitimate clients or even worse, not respond at all to users. Fig. 4 illustrates the process behind HTTP flood attacks [25].
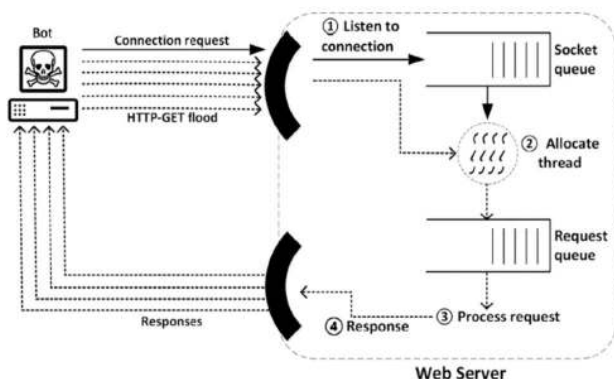


**FIGURE 4.** The HTTP flood attack process (adapted from [25]).

### B. SLOW- AND LOW-RATE DDoS ATTACKS
In the case of slow- and low-rate attacks, the attacker generates traffic toward the victim's webserver and then keeps the connection open (or active) without any reply until the server's resources are consumed [26]. The tools commonly used for conducting slow- and low-rate DDoS attacks include Slowloris, Sockstress, and RUDY (R-U-Dead-Yet) [27]. To accomplish this type of attack, an attacker must specify the target URL parameter, the number of sockets which will be run simultaneously from the source of the attack; the attacker will never complete the connection. As a result, the web server resources are consumed until the available resources run out making the services inaccessible to legitimate users.

### C. SESSION INITIATION PROTOCOL
The Session Initiation Protocol (SIP) is the most common protocol for managing signaling among communication parties in order to provide the necessary functionalities for registering users, checking statuses, and managing sessions [28]. The SIP is vulnerable to DDoS attacks [158], [161]. In fact, such attacks cause disruption to SIP services, or even worse, render such services unavailable to legitimate clients [29]. To launch a SIP DDoS attack, attackers use SIPp-DD, open source software, to generate malicious activity attacks on the SIP server. Some settings are needed to use the tool, such as the network range, the network target, port numbers, and the number of malformed IP packets.

### D. REFLECTOR ATTACKS
The main goal of a reflector attack is to mask the identity of the real attacker through the use of third-party "reflectors" and then to benefit from their resources [30]. The attacker

initiates an attack from zombie machines and instructs them to send traffic toward the target through third parties with the victim's IP address [31]. All the reflectors reply to the victim, while the original request comes from the attacking source, thus causing a huge amount of malicious traffic that consumes the target network resources [32]. Fig 5. illustrates the process behind a reflector DDoS attack.
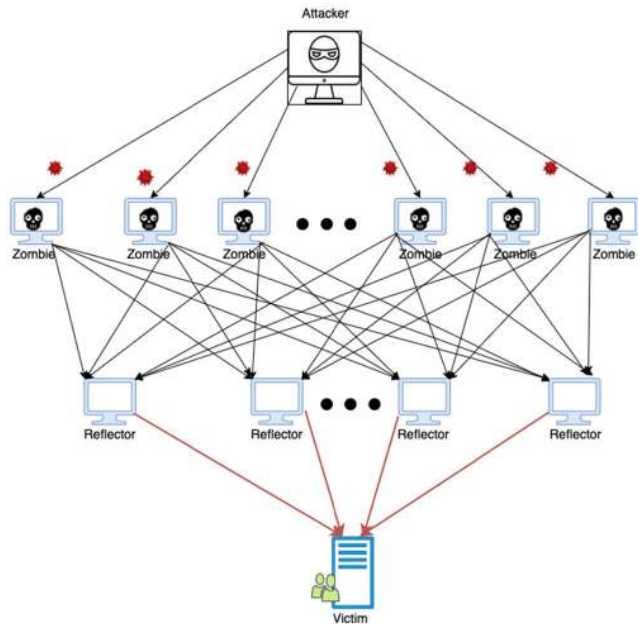


**FIGURE 5.** The reflector DDoS attack process.

### E. DOMAIN NAME SYSTEM AMPLIFICATION ATTACKS

In the case of this type of DDoS attack, the attacker aims to exploit vulnerabilities in the domain name system (DNS) in order to transform (i.e., amplify) the initially small messages sent by the attacker into much larger messages [33], [160]. The magnitudes of the messages deplete the victim's recourses, which renders its services unavailable to legitimate users. In this type of attack, attackers use a DNS flooder tool and specify needed parameters, such as the IP address and the port address, making the DNS server respond with a large amount of traffic directed to the target to paralyze the services and make them unavailable to legitimate users. Fig. 6 illiterates the process behind DNS amplification attacks [34].
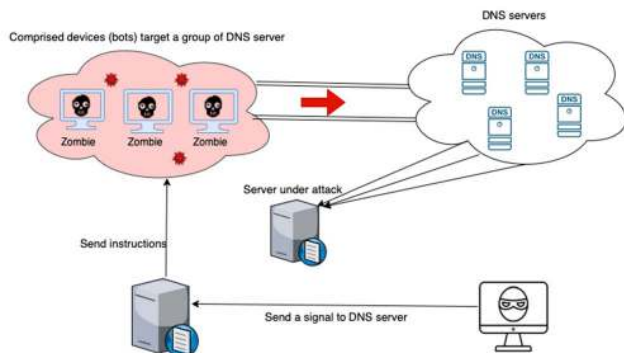


**FIGURE 6.** The DNS DDoS attack process.

### F. SYN FLOODING ATTACKS

A SYN flooding attack is the most common type of DDoS attack [35]. In the first quarter of 2019, this type ranked as the most frequently occurring type of DDoS attacks [109]. The attacker takes advantage of the TCP three-way handshake method to establish a connection with the server [36]. In a normal scenario, the client initiates the request to exchange data with the server by sending a SYN packet. The request is then allocated to a queue (i.e., stored in the memory). The server replies by sending a SYN/ACK packet to the client and then waits until the half-open connection is completed or the TCP connection has expired (i.e., timeout). In the case of a SYN flooding attack, the victim's server receives a massive number of SYN packets but never receives the final ACK required to finish the three-way handshake through the TCP protocol [37]. As a result, the server's queue is overwhelmed, which causes all incoming requests from legitimate clients to be dropped Hping3 is a commonly used tool for conducting a SYN flooding attack. An attacker configures the tool and specifies the IP address, port address, and data payload size. In addition, an attacker can hide the real source IP address and use the spoof hostname option to set a fake IP address, ensuring the target will never know the real address. Fig. 7 illustrates the process behind SYN flooding DDoS attacks.
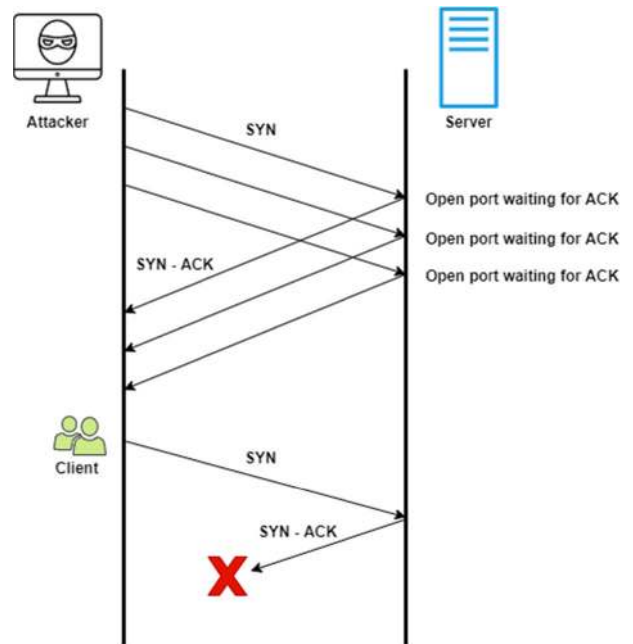


**FIGURE 7.** The SYN flooding DDoS attack process.

### G. UDP FLOODING ATTACKS

A user datagram protocol (UDP) flooding attack is a type of DDoS attack in which the attacker targets and overwhelms random ports on a targeted server with IP packets including UDP packets [115]. In this type of attack, the host checks for applications that are listening to a specific port. If the host does not find applications, it replies with ICMP messages
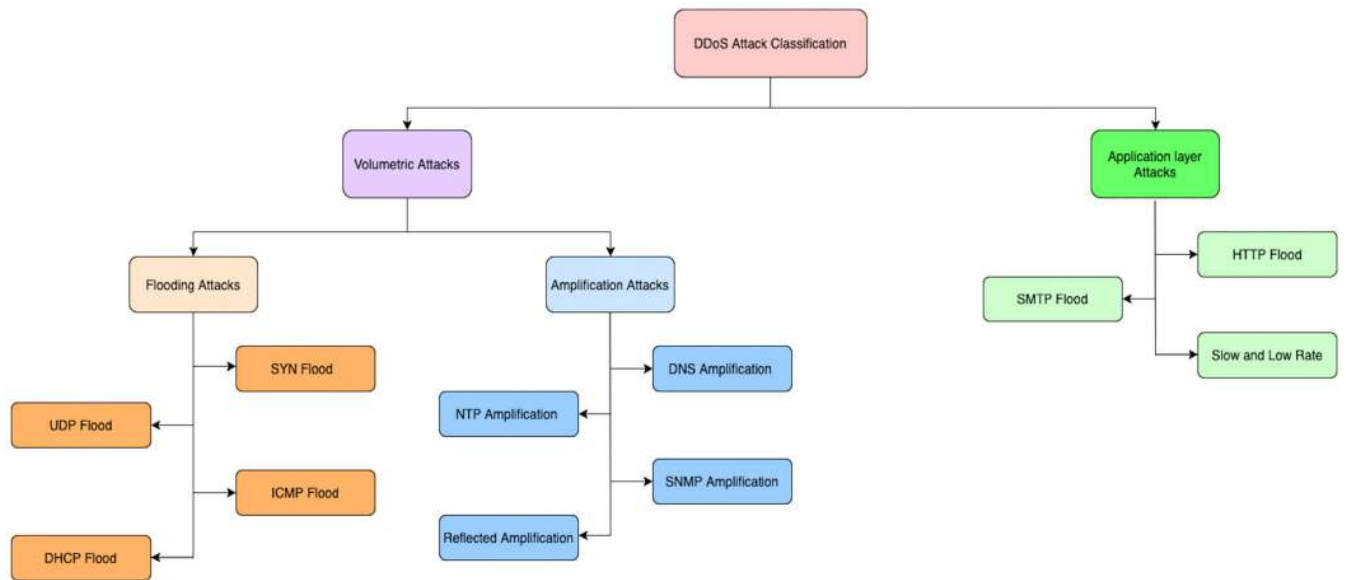
**FIGURE 8.** Taxonomy of DDoS attacks.

stating that the destination is unreachable. When a large number of UDP packets target the victim, the host is forced to send many ICMP destination unreachable packets [115]. As a result, the server' resources are consumed with these UPD packets, making the host unresponsive to legitimate clients.

### H. ICMP FLOODING ATTACKS

An ICMP flooding attack, also known as a ping attack, aims to target the victim's server with a huge number of echo requests. The targeted victim server has to send a response packet for each request received from the sender [116]. Each ICMP request requires the server use its resources to process the request and send the response to the sender. This type of attack overwhelms the server's resources with a large number of echo requests, making the server inaccessible to legitimate users. To conduct this type of attack, attackers use either tools such as Hping and Scapy or a script written by professional hackers.

### I. DHCP FLOODING ATTACKS

A dynamic host configuration protocol (DHCP) flooding attack, also known as a DHCP starvation attack, aims to consume all the IP addresses that can be assigned by the DHCP server [117]. An attacker broadcasts a large number of DHCP requests packets; the DHCP server begins to process each request and starts to respond to all the request packets. As a result, the available IP addresses on the DHCP server are consumed by the attacker, and legitimate users fail to connect to the DHCP server. Fig. 8 presents different types of DDoS attacks.

### VI. USE OF ML TO COMBAT DDoS ATTACKS

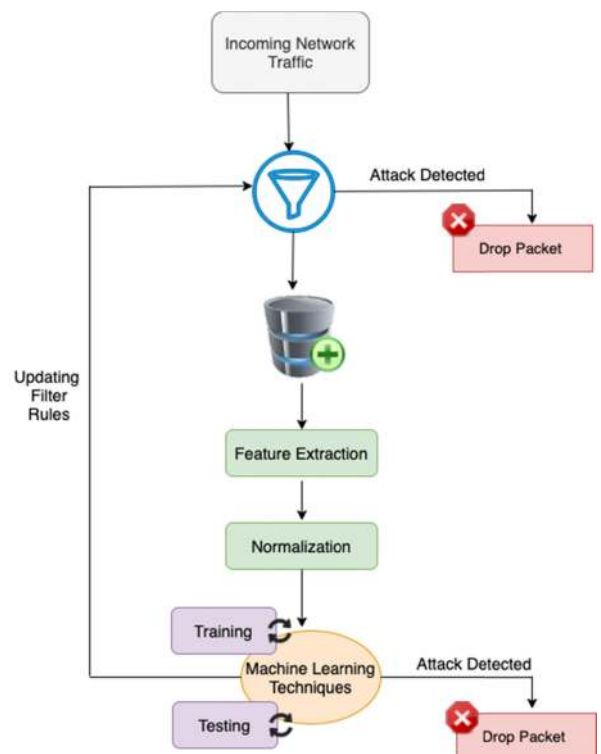In recent years, a number of ML techniques have been used for the detection of DDoS attacks [38]. The basic concept



**FIGURE 9.** General framework for DDoS detection based on ML.

behind ML is to automatically learn from a bank of data so as to identify certain patterns [39], for example, DDoS attacks.

ML techniques help defense systems to determine whether a given user is a regular user or an attacker. Fig. 9 presents an overview of the DDoS attack detection process based on ML [40]. In the first step, incoming network packets are examined with filtering policies and added to the database. In the feature extraction process, selected features from the database are extracted (e.g., source and destination addresses,
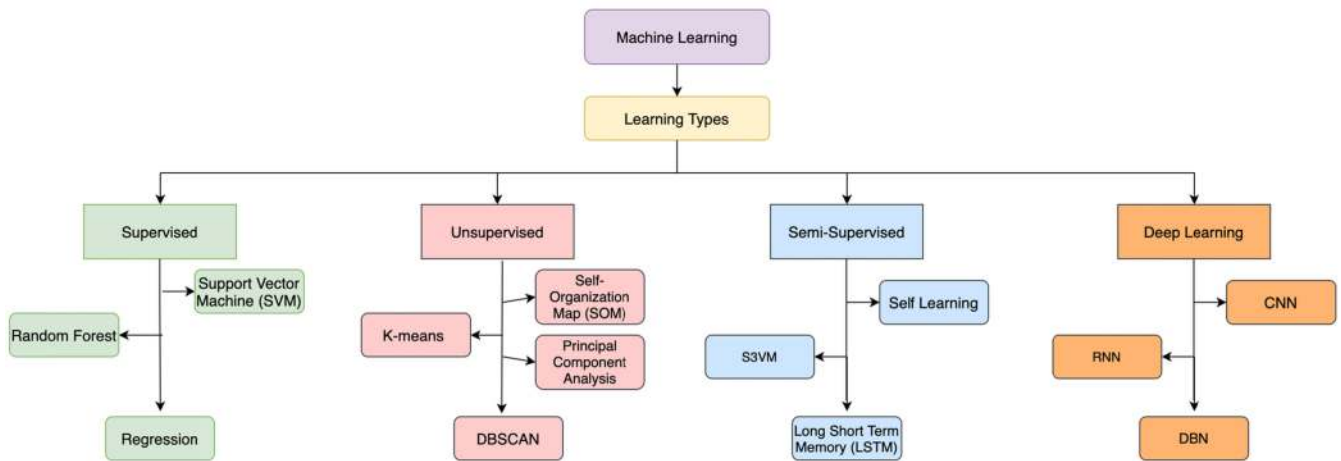
**FIGURE 10.** Overview of the ML techniques.

protocol name, port number). To improve the performance of the training process, selected features are normalized. The machine learning algorithms perform the training phase to learn patterns from the dataset. Based on the learning parameters, an incoming packet is distinguished as a DDoS attack or a legitimate user. In the final process, the system removes the detected DDoS packets and updates its filtering policy so that it will apply to the new incoming traffic.

The available ML techniques can be divided into supervised, unsupervised, and semi-supervised learning techniques [41]. Fig. 10 shows how the various ML techniques can be categorized based on the utilized learning methods. Further details concerning each category will be provided in the subsequent subsections.

### A. SUPERVISED LEARNING
Supervised learning is a category of ML in which algorithms learn from input variables (X), which serve as a kind of supervisor or teacher, in order to predict output variables (Y) [42]. This category is termed supervised learning because an algorithm can learn from a labeled training dataset, while the learning process stops when the algorithm reaches an appropriate level of performance. The most widely used supervised learning algorithms include the support vector machine (SVM), linear regression, logistic regression, naive Bayes, and k-nearest neighbor (KNN) algorithms. Further, there are two types of supervised learning:

**Classification**: The algorithm learns how to classify new observations from a labeled training dataset [43]. The output of the classification can be either bi-class (e.g., whether a given client is a regular user or an attacker, or whether an email is spam or non-spam) or multi-class, in which case it contains more than two classes.

**Regression**: The algorithm performs a regression task. It is trained to estimate the mapping function (f) based on a training dataset (x) in order to predict the numerical or continuous output (y). This type of algorithm can be used to predict, for example, a house price or a stock price.

### B. UNSUPERVISED LEARNING
Unsupervised learning is a ML approach whereby the model trains and learns based on its own information, without requiring guidance to discover patterns, similarities, and differences [44]. The various unsupervised techniques deal with unlabeled or unclassified data, and they allow the algorithms to learn and model on their own in order to uncover patterns [45]. The most widely used unsupervised learning algorithms include the hierarchical clustering, K-means clustering, mixture models, and density-based spatial clustering of applications with noise (DBSCAN) algorithms. The different types of unsupervised learning approaches can be divided into two groups:

**Clustering**: The data points are clustered into different groups. Data points with similar features or proprieties will be clustered into the same group, while data points that do not share similar features will be clustered into different groups.

**Association**: A rule-based ML technique designed to discover the relation or association across a large set of items.

### C. SEMI-SUPERVISED LEARNING
Semi-supervised learning relies on a combination of a labeled dataset for a large amount of data and an unlabeled dataset for a small amount of data during the training phase [46]. This type of ML falls somewhere between supervised learning, which involves a labeled dataset, and unsupervised learning, which involves an unlabeled dataset [47]. Some practical examples of semi-supervised learning include speech analysis, Internet content classification, and protein sequence classification.

### D. DEEP LEARNING
The deep learning (DL) technique is a type of ML that imitates the structure of the human brain in analyzing and processing data to observe patterns and perform different classification tasks [118]. DL utilizes a multi-layered structure of algorithms named neural networks; the design of the neural networks mimics the structure of the human brain to accomplish different tasks, including regression,

clustering, and classification. DL algorithms fall somewhere between supervised learning (which involves a labeled dataset) and unsupervised learning (which involves an unlabeled dataset) [119]. Some practical examples of DL include self-driving cars, speech recognition, natural language processing (NLP), fraud detection, language translation, and image classification.

## VII. DDoS DEFENSE SYSTEMS BASED ON ML APPROACHES IN TRADITIONAL NETWORKING ENVIRONMENTS

This section discusses recent studies concerning a diverse range of DDoS defense systems that make use of ML approaches in traditional networking environments.

Gu *et al.* [45] proposed a semi-supervised k-means algorithm for the DDoS attack classification process. In terms of the selected features, the authors used a hybrid feature selection algorithm to ensure the best detection results. The proposed approach was applied to different known datasets, including the DARPA, CAIDA, CICIDS, and real-world datasets. However, the authors created real-world datasets by using tools to stimulate normal and attacker traffic; and no accuracy measurement was provided in the proposed work for a comparison with other related work. Zhang *et al.* [48] proposed a DDoS detection model that uses two algorithms, namely the power spectral density (PSD) and SVM algorithms, for low-rate DDoS attack classifications. The PSD algorithm calculates the entropy and then compares it with two predefined thresholds. To distinguish traffic patterns, the SVM algorithm is applied to investigate suspicious traffic and recognize similar patterns for the classifications. The experimental results showed that the proposed approach detected 99.19% of all low-rate DDoS attack traffic within a low-complexity timeframe. The proposed work must be validated with recent datasets. Filho *et al.* [49] proposed a smart detection system, that is, an online approach to DDoS attack detection. The proposed technique uses the random forest tree algorithm to perform the DDoS classification. Their article also presented a new signature database consisting of normal and attack network traffic. The database is used by the online smart detection system. In terms of the system evaluation and validation, the authors used both a customized dataset and existing datasets, including the CIC-DoS, CICIDS2017, and CSE-CIC-IDS2018 datasets. The performance metric results concerning the smart detection system indicated an improvement in the detection rate (DR), the false alarm rate (FAR), and the precision rate (PREC).

Yuan *et al.* [40] proposed a deep learning detection approach known as DeepDefense. They designed a recurrent deep neural network to learn behavior from a large-scale network traffic dataset. The DeepDefense mechanism adapts a number of ML techniques, and the approach used various types of recurrent neural networks (RNNs) to detect DDoS attacks. The evaluation results revealed that the proposed method reduced the error rate and exhibited a higher accuracy rate. However, the dataset used in the proposed work

is old and did not contain recent DDoS attack techniques. Sofi *et al.* [50] proposed a new dataset that contains modern classes of DDoS attacks, with a focus on HTTP flood and SIDDoS attacks. For the DDoS detection and classification, various ML methods were applied to distinguish between normal and DDoS attack traffic. Among the different classification methods described in the article, the multilayer perceptron (MLP) provided the highest accuracy rate. However, the proposed work used a synthetic dataset, which affected the quality of the performance, and did not provide a comparison with other related work. Devi *et al.* [51] proposed a detection model consisting of an online monitoring system and a spoofed traffic detection module. The online monitoring system aims to construct baseline profiles for normal and attack traffic. The spoofed traffic detection module combines two algorithms, namely the hop-count inspection (HCI) and SVM algorithms, to perform the classification. The experimental results demonstrated 98.99% accuracy and a reduced false positive rate. However, the proposed work did not provide enough details about the dataset used. In addition, no comparison with previous work in terms of performance metrics was provided. Das *et al.* [52] proposed a network intrusion detection system (NIDS) to detect both predefined and modern types of DDoS attacks. The proposed NIDS is based on the integration of various classifiers using ensemble models. Each classifier is specified for a certain type of intrusion in order to achieve a solid detection mechanism in the face of DDoS attacks. The experimental results showed that the proposed NIDS detected 99.1% of all DDoS attack traffic. However, the proposed approach is limited to specific types of DDoS attacks, and only one dataset was used to test the model. Liu *et al.* [53] proposed a novel mitigation approach in the edge environment to detect large-scale, low-rate DDoS attacks. A deep convolution neural network (DCNN) is used to automatically learn the optimal features of the dataset. For the attack classifications, the authors used a deep reinforcement learning Q-network. They also used an enhanced Mirai botnet to conduct a powerful and sophisticated attack. The experimental results demonstrated that the proposed approach could differentiate between attacks with an increased detection accuracy rate as well as more quickly with regard to the response time than the SVM, K-means, and surface learning neural network approaches. However, the article did not compare the performance metrics with other related work. Jia *et al.* [131] proposed a detection method based on hybrid multi-classifier learning techniques. The detection approach utilized singular value decomposition (SVD) for traffic classification. The authors used a known public dataset called the KDD Cup 1999 dataset to perform the training and testing for the proposed detection system. The experimental results demonstrated that the proposed detection approach achieved a higher accuracy and precision rate. However, it would be interesting to evaluate the proposed detection method with recent real traffic datasets. Diverse use of ML approaches in traditional networking environments can appear in Table 2.

**TABLE 2.** Comparison of DDoS defense system based on ML approaches in traditional networking environments.

| Reference | Types of DDoS attacks | ML techniques used | Dataset | Evaluation metrics | Best accuracy, precision, TPR, and FPR |
|---|---|---|---|---|---|
| [45] | Network layer DDoS attacks | k-means | DARPA, CAIDA, CICIDS, and real-world dataset | True positive rate (TPR), false positive rate (FPR), and detection time | Accuracy: not available<br>Precision: not available<br>TPR: 99.75<br>FPR: 0.20 |
| [48] | Low rate DDoS attacks | SVM | KDD99 dataset | Detection rate (DR) and the percentage of detection amount (DA) | Accuracy: 99.19<br>Precision: not available<br>TRP: not available<br>FPR: not available |
| [49] | Volumetric attacks: TCP flood, UDP flood, HTTP flood, HTTP slow headers, HTTP slow body, and HTTP slow read | Random forest tree | CIC-DoS, CICIDS2017, CSE-CIC-IDS2018, and customized dataset | Detection rate (DR), precision (PREC), false alarm rate (FAR), and sampling rate (SR) | Accuracy: 0.99<br>Precision: 0.99<br>TPR: not available<br>FPR: 0.00 |
| [40] | HTTP, TCP, IRC, DNS, and SMTP | Convolutional neural network (CNN), RNN, long short-term memory neural network (LSTM), and gated recurrent unit (GRU) | ISCX2012 dataset | Error rate, accuracy rate, precision, recall, f-measure, accuracy rate, and area under the curve (AUC) | Accuracy: 98.41<br>Precision: 98.4<br>TPR: 98.40<br>FPR: 1.59 |
| [50] | HTTP flood, SIDDoS, UDP flood, and Smurf attack | Naive Bayes, MLP, SVM, and decision trees | Synthetic dataset | Accuracy rate, precision, and recall | Accuracy: 98.91<br>Precision: 0.98<br>TPR: 0.98<br>FPR: not available |
| [51] | TCP SYN, Smurf, UDP, and ICMP | HCI and SVM | Synthetic dataset | CPU usage, memory usage, packet loss, throughput, link utilization, true positive, false positive, precision, recall, f-measure, and accuracy rate | Accuracy: 98.99<br>Precision: 0.984<br>TPR: 0.974<br>FPR: 0.026 |
| [52] | Network layer DDoS attacks | C4.5, KNN, MLP, and SVM | NSL-KDD dataset | Accuracy rate, TPR, FPR, precision, recall, f-measure, and ROC area | Accuracy: 97.89<br>Precision: 0.979<br>TPR: 0.979<br>FPR: 0.022 |
| [53] | Low-rate DDoS attacks | DCNN and deep reinforcement learning Q-network | Mirai Bots | Detection rate, FPR, training time, network speed, and packet loss rate | Accuracy: 95.22<br>Precision: not available<br>TPR: not available<br>FPR: 0.40 |
| [131] | TCP. UDP, and ICMP | Multi Classifier | KDD99 dataset | Accuracy, precision, and TNR | Accuracy: 99.8<br>Precision: 99.84<br>TPR: not available<br>FPR: not available |

## VIII. DDoS DEFENSE SYSTEMS USING MODERN NETWORKING ENVIRONMENTS BASED ON ML TECHNIQUES

A number of different approaches have been proposed with regard to DDoS attack detection based on ML techniques in modern networking environments. Today, many systems make use of modern networking technologies due to the advantages that such an environment offers, including flexibility, scalability, and cost reduction [54], [55]. This section discusses DDoS defense systems based on ML techniques using a diverse range of modern networking environments.

### A. DDoS DEFENSE SYSTEMS BASED ON ML TECHNIQUES IN CLOUD COMPUTING ENVIRONMENTS

The term "cloud computing" refers to the way in which computer recourses and network services are delivered over the Internet (i.e., the cloud) [56]. The invention of cloud computing shifted the focus of network infrastructure adaptation
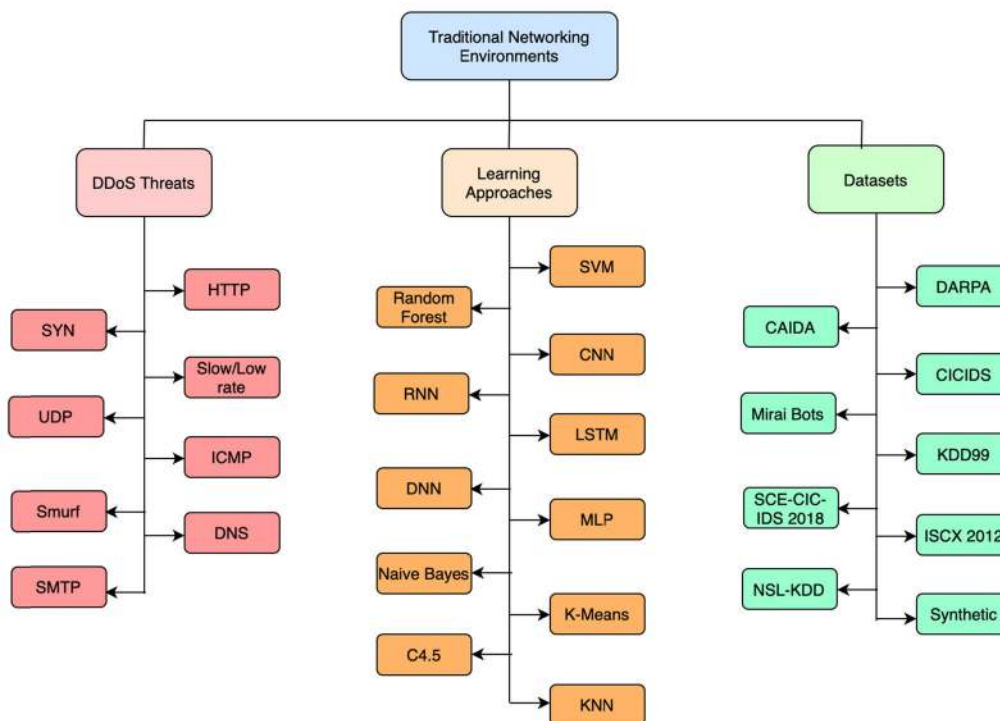
**FIGURE 11.** Summary of DDoS threats with the used learning approaches and datasets in traditional networking environments.

from enterprises' premises to cloud services. The number of enterprises that have chosen to move their IT infrastructure to the cloud is increasing day by day due to the significant benefits associated with the use of cloud services, including cost reduction and the ability to scale network services [57].

As many clients now use cloud services, it is important to recognize that DDoS attacks represent a major threat to such services [58]. This subsection discusses the different DDoS defense approaches based on ML techniques in the context of cloud computing.

Gurulakshmi and Nesarani [59] used different ML algorithms, including the SVM, naive Bayes, and random forest algorithms, to perform the DDoS attack classifications. A new dataset with nine features and four classes was created to be used with various ML techniques. The experimental results showed that the SVM algorithm achieved high performance when compared with the other ML methods used in the paper. However, the proposed approach must be tested with recent real-world datasets that contain new DDoS attack techniques. Zekri *et al.* [60] proposed a DDoS detection system based on the C.4.5 algorithm. The algorithm was designed in such a way that it coupled with signature detection methods to achieve better DDoS classifications. The proposed approach involves a processing module, a detection module, and storage. The detection module consists of the signature-based detection and C.4.5 algorithms working together to perform better DDoS detection. The evaluation results showed that the

system was able to mitigate DDoS attacks with high detection and efficiency rates. However, the proposed work must be validated with recent real traffic datasets. Alsirhani *et al.* [114] proposed a dynamic DDoS attack detection system consisting of a classification algorithm, a distributed system, and a fuzzy logic system. The proposed system uses fuzzy logic to choose the most suitable algorithm from among a list of existing classification algorithms capable of identifying various DDoS attack patterns. The available algorithms are the naive Bayes, decision tree (entropy), decision tree (Gini), and random forest algorithms. When dataset1 was used, the experimental results showed that the proposed approach exhibited higher performance rates and lower delays. However, the proposed system exhibited lower performance rates and delays when dataset2 was used.He *et al.* [62] proposed a DDoS attack detection approach based on the source side of the cloud environment. The proposed method utilizes statistical techniques to gather the required data from the hypervisor of the cloud server and the virtual machine, thereby preventing traffic from being sent outside the network. The authors used nine different ML approaches so as to draw a comparison between the available algorithms. The evaluation of the proposed approach showed it to exhibit 99.7% accuracy in relation to preventing four types of DDoS attacks. In future work, the authors intend to combine various ML algorithms to achieve better performance in the face of DDoS attacks. However, the proposed work used an unknown dataset which affected the performance results. Rivas and Lafalce [63] proposed a DDoS

attack detection approach that relies on a new application of ML. To learn from an attacker's behavior, they used a honeypot to produce a training dataset. The dataset contains the source IP address, country name, and attack duration. The authors used two ML algorithms for the classification, namely the SVM and CNN algorithms. The experimental evaluation showed that both the utilized ML algorithms have the ability to detect DDoS attacks with a high degree of accuracy. However, the proposed approach is limited to certain types of DDoS attacks. Rukavitsyn *et al.* [64] proposed a self-learning approach that can be performed in two steps: capturing the network traffic and retraining the detection method using updated data. The authors used a relearning algorithm to dynamically adapt to any changes in traffic in the cloud and to implement a new detection model. The experimental environment was rendered via OpenStack, with the results showing that the proposed relearning algorithm was able to increase the accuracy of the DDoS attack detection within the cloud environment. However, the proposed method must use a real traffic dataset to test and validate their approach. Priyadarshini and Barik [120] proposed a deep learning intelligent mechanism to mitigate DDoS attacks in fog and cloud environments. The proposed methodology used long short-term memory (LSTM) as the deep learning algorithm to classify the DDoS attacks. The authors used the Hogzilla dataset to train and test the proposed work and using the Hping3 tool, created another dataset to stimulate DDoS attack traffic and normal user traffic. The attack traffic was conducted on three types of DDoS attacks: TCP, UDP, and ICMP. The experimental evaluation showed the proposed method is effective in terms of detecting DDoS traffic within cloud and fog environments. However, the dataset used in the proposed model is old, and the authors need to validate their approach in a large-scale real environment. Çakmakçı*et al.* [121] proposed a novel DDoS detection method in which the proposed algorithm is improved based on a kernel-based online anomaly detection approach. The proposed work used an unsupervised machine learning algorithm and the CICIDS2017 dataset. The authors verified and compared their work with other related works in terms of the accuracy rate, precision, and recall. The performance results showed that the proposed approach is effective in the face of DDoS attacks. However, the proposed work is limited to certain types of DDoS attacks. Virupakshar *et al.* [122] proposed a DDoS mitigation system for the OpenStack platform within the private cloud environment. The proposed work utilized different ML approaches for DDoS classification. To train and test the dataset for DDoS classification, the authors created a dataset within the cloud environment and used a simulation tool called low orbit ion cannon (LOIC) to generate various types of DDoS attack traffic. The performance results showed that the KNN, naïve Bayes, and the DNN exhibited a high accuracy rate in the face of different types of DDoS attacks. However, it would be more appropriate to use a real traffic dataset rather than a synthetic dataset. Gumaste *et al.* [123] proposed a detection approach on the OpenStack platform within the
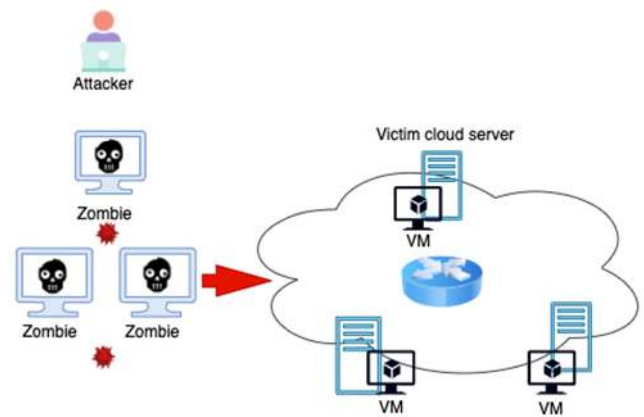


**FIGURE 12.** DDoS attacks in cloud computing environments.

private cloud environment. The authors designed Spark as a service for on-demand provisioning of clusters. For the detection part, the proposed method employed three different ML algorithms, including random forest, decision tree, and logistic regression. The performance results showed that the random forest technique achieved a higher accuracy rate in contrast to the other ML algorithms. However, the proposed work is limited to certain types of DDoS attacks. Diverse use of ML approaches in cloud computing environments can appear in Table 3.

### B. DDoS DEFENSE SYSTEMS BASED ON ML TECHNIQUES IN SDN ENVIRONMENTS

An SDN is a new network paradigm that enables the network topology to be controlled or programmed via various software applications [65]. An SDN provides a centralized controller to manage the entire network. Although the controller represents one of the most significant advantages of an SDN, it might become inaccessible or unavailable as a result of DDoS attacks [66], [157].

Dong and Sarem [67] proposed a DDoS detection method for use in an SDN environment based on a ML approach. The proposed method can be performed in two ways. First, by identifying DDoS attacks based on the degree of the attacks. Second, by employing ML techniques to perform the classifications. The authors used an improved KNN algorithm to identify DDoS patterns with four selected features, namely the flow length, flow duration, flow size, and flow ratio. The experimental evaluation demonstrated that the proposed method could successfully identify DDoS attacks. However, the authors used an unknown dataset and did not provide any details about it. Sun *et al.* [68] proposed a real-time detection method for an SDN controller. The detection method first determines the abnormality in the network traffic through the use of entropy. Then, a warning alarm is generated and important features are extracted. To identify the DDoS patterns, the authors used the BiLSTM-RNN neural network algorithm. The proposed defense system involves four modules, namely the anomaly detection module, the flow table collection module, the feature extraction module, and the attack detec-

**TABLE 3.** Comparison of DDoS defense system based on ML approaches in cloud computing.

| Reference | Types of DDoS attacks | ML techniques used | Dataset | Evaluation metrics | Best accuracy, precision, TPR, and FPR |
|---|---|---|---|---|---|
| [59] | HTTP, TCP, UDP, and ICMP | SVM, naive Bayes, and random forest | Synthetic dataset | Accuracy rate, precision, recall, specificity, and f-measure | Accuracy: 0.997 Precision: 0.998 TPR 0.99 FPR: not available |
| [60] | TCP SYN attack, UDP attack, and ICMP attack | C.4.5 algorithm | Synthetic dataset | Accuracy rate, TPR, FPR, true negative rate, f-measure, correct classification rate, detection time, and ROC area | Accuracy: 99.05 Precision: 0.99 TPR: 100 FPR: 2 |
| [114] | Network layer DDoS attacks | Naive Bayes, decision tree (entropy), decision tree (Gini), and random forest as candidate algorithms. | CAIDA | Accuracy rate, precision, recall, f-measure, FPR, and true negative rate | Accuracy: 0.98 Precision: 0.98 TPR: 0.98 FPR: 0.02 |
| [62] | SSH brute-force attacks, ICMP flooding attacks, DNS reflection attacks, and TCP SYN attacks | Linear regression (LR), SVM, decision tree, naive Bayes, random forest algorithm, k-means, and Gaussian- mixture model for expectation maximization (GMM-EM) | Unknown dataset | Accuracy rate, precision, recall, f-measure, FPR, and false negative rate | Accuracy: 99.73 Precision: 100.0 TPR: 99.76 FPR: < 0.07% |
| [63] | HTTP request | SVM and a CNN | Hive plot dataset | Accuracy rate, precision, recall, and AUC | Accuracy: 100.0 Precision: 1.00 TPR: 1.00 FPR: not available |
| [64] | Not specified | Self-learning algorithm | Synthetic dataset | Accuracy rate, precision, recall, and F1-score | Accuracy: 1.0 Precision: 1.0 TPR: not available FPR: not available |
| [120] | TCP, UDP, and ICMP | long short-term memory (LSTM) | Hogzilla and synthetic dataset | Accuracy rate | Accuracy: 98.88 Precision: not available TPR: not available FPR: not specified |
| [121] | UDP, TCP, and HTTP | Improved KOAD | CICIDS2017 dataset | Accuracy rate, precision, and recall | Accuracy: 99.55 Precision: 95.24 TPR: 95.23 FPR: 0.23 |
| [122] | ICMP, TCP, and HTTP flooding | Decision Trees, K-nearest neighbor (KNN), Naive Bayes, and Deep Neural Network (DNN) | Synthetic dataset | Accuracy rate, precision, recall, F1-score | Accuracy: 99.55 Precision: around 98.0 TPR: 0.99 FPR: not specified |
| [123] | ICMP flooding attacks | Random forest, decision tree, and logistic regression | KDD Cup and Synthetic dataset | Accuracy rate, precision, false positive rate, and detection time | Accuracy: 99.21 Precision: 99.91 TPR: not available FPR: 0.003 |

tion module. The experimental results showed that the proposed system can be effectively used to detect DDoS attacks as well as to minimize the overhead on the SDN controller. However, the proposed method is limited to specific types of DDoS attacks. In addition, the proposed approach must

be validated with recent datasets. Abou El Houda *et al.* [69] proposed a blockchain-based approach known as Cochain-SC for DDoS mitigation in the context of an SDN. The proposed mitigation system consists of two stages, namely the intra-domain and inter-domain DDoS mitigation stages.
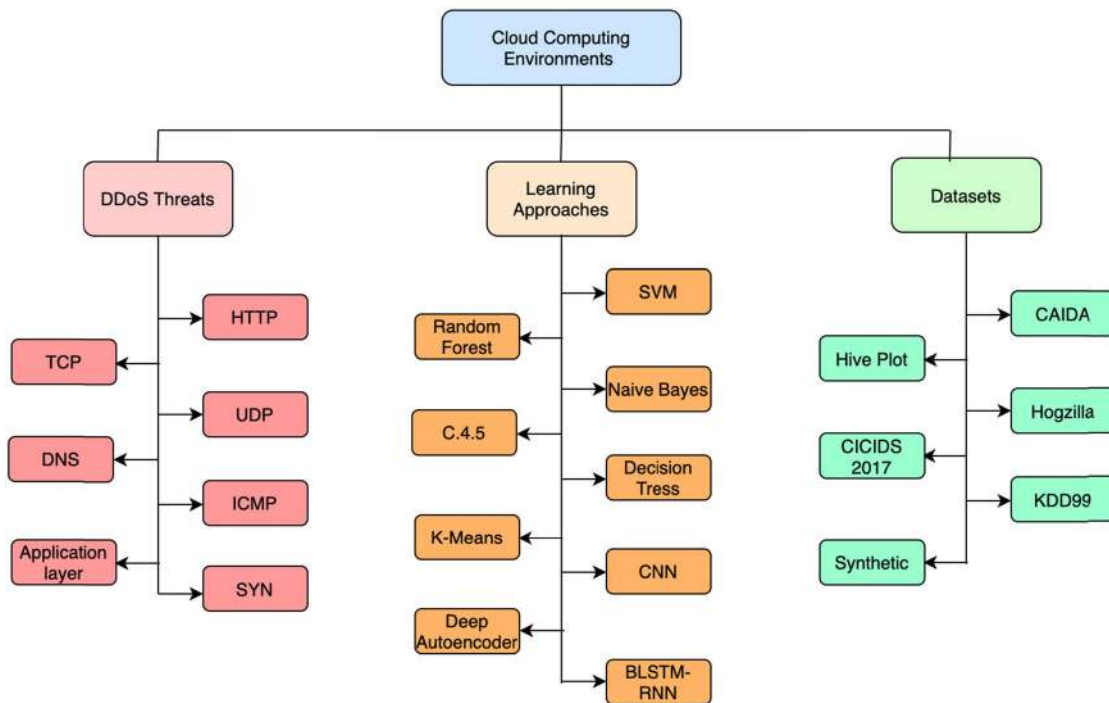
**FIGURE 13.** Summary of DDoS threats with the used learning approaches and datasets in cloud computing environments.

The intra-domain mitigation stage involves three primary methods: (1) an intra-entropy-based method for data randomness, (2) an intra-Bayes-based method for classifications; and (3) an intra-domain method for mitigating illegal traffic. The inter-domain DDoS mitigation stage uses a blockchain to route malicious traffic in a decentralized fashion. The experimental results showed that the proposed approach could effectively mitigate DDoS attacks in the context of an SDN. However, the authors must validate the proposed approach with recent real traffic datasets and improve the detection method to identify different types of DDoS attacks. Liu *et al.* [70] also proposed a DDoS detection method in the context of an SDN. The proposed method deploys an entropy approach on the switch, which results in a distinction being made between normal and abnormal traffic. When the traffic is abnormal, the anomaly detection module collects the flow table and extracts the features required for the classifications. The attack detection module determines whether a client is normal or an attacker through the use of a PSO-BP neural network. The experimental evaluation demonstrated that the proposed method can reduce the SDN controller's overhead, improve the detection accuracy, and enhance the detection speed. However, the article did not provide any details about the dataset used. In addition, the evaluation metrics should be compared with other related works. Lingfeng and Hui [71] proposed a detection framework for mitigating DDoS attacks in the context of an SDN. The proposed approach comprises three main parts: (1) a traffic collection module, (2) a DDoS attack identification module, and (3) a flow table delivery module. The proposed detection approach uses the SVM algorithm to determine whether the collected traffic is normal or attack traffic. After attacks are detected, the forwarding policy is adjusted according to the flow table delivery module. The experimental results demonstrated that the proposed approach is effective in terms of detecting DDoS attacks. However, the dataset used is old and did not contain recent types of DDoS attacks. Rahman *et al.* [72] proposed a framework for detecting and mitigating DDoS attacks in an SDN environment. The proposed framework uses four ML techniques (J48, random forest, SVM, and KNN) to perform the classifications. After the evaluation process used to select the ML algorithms, the authors used the best model in the SDN network topology to perform the DDoS detection and mitigation. The experimental evaluation showed the J48 algorithm to be the most accurate model for the proposed network. However, the authors used a synthetic dataset which affected the evaluation metrics. In addition, the dataset used contained only two types of DDoS attacks. Deepa *et al.* [73] proposed an ensemble approach that combines various ML algorithms to perform DDoS classifications in the context of an SDN environment. The selected ML classifiers are the KNN, naive Bayes, SVM, and self-organizing map (SOM) algorithms. The performance metrics showed that the SVM-SOM combination delivered higher accuracy, a better detection rate, and a reduced false positive rate. Moreover, Deepa *et al.* [74] proposed a hybrid technique that combines two ML algorithms for attack classifications in the context of the SDN controller. The performance evaluation
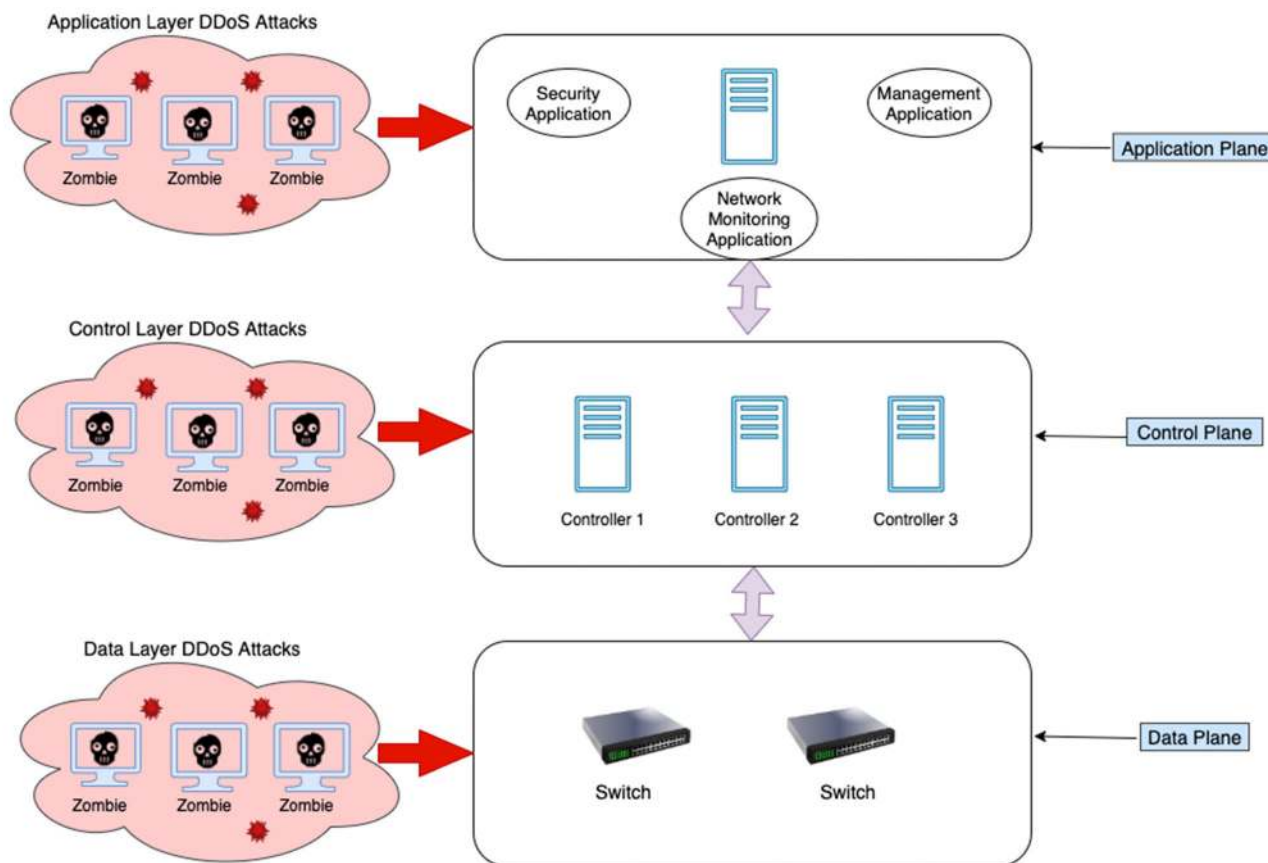
**FIGURE 14.** DDoS attacks in the context of SDN environments.

metrics demonstrated that the proposed hybrid ML model (SVM-SOM) achieved better accuracy, a high detection rate, and a reduced false positive rate when compared with the use of a simple ML algorithm. However, the proposed detection method must be validated with recent real traffic datasets. Zhijun *et al.* [75] proposed a detection method for low-rate DDoS attacks. The factorization machine (FM) ML algorithm is used for the DDoS classifications. The proposed approach trains the selected features sample (six tuple) in order to construct the FM prediction model for low-rate DDoS attack classifications. The experimental evaluation demonstrated that the proposed detection approach is able to detect low-rate DDoS attacks with higher detection accuracy, a higher recall rate, a higher precision rate, and a higher AUC rate. Haider *et al.* [15] proposed a deep learning framework for DDoS attack detection in the context of an SDN. To improve the detection rate in relation to flow-based data, the proposed approach utilizes ensemble CNN models. The CICIDS2017 dataset was used to provide flow-based attributes and features for the SDN. The authors verified and compared their work with other related works in terms of the accuracy rate, precision, recall, F1-measure, test time, train time, and CPU usage. The performance results showed that the proposed approach is effective in the face of DDoS attacks on the

SDN controller. Although the authors provided a comparison of different benchmark datasets, they did not compare the proposed method with other related work. Oo *et al.* [124] proposed an advanced support vector machine (ASVM) for DDoS attack classification. The learning algorithm is able to perform a multiclass output, comprising three different classes. The proposed mechanism classified two types of DDoS attacks, including UDP and SYN flooding attacks. The authors used a generated traffic tool named Scapy to perform DDoS flooding attacks and created a new dataset called SDNTrafficDS. The experimental evaluation showed the proposed method is effective in terms of detecting UDP and SYN flooding attacks within the SDN environment. However, the authors must validate their approach on a real traffic dataset. In addition, after DDoS attacks are detected, a mitigation method should be performed to eliminate malicious traffic. The authors did not provide any details about the mitigation strategy. Tuan *et al.* [125] proposed a novel DDoS attack mitigation scheme in Internet service provider (ISP) networks within the SDN environment. The implemented approach was designed to mitigate TCP-SYN and ICMP flooding attacks by using ML techniques. The authors used a KNN to distinguish whether a given data set is normal or an attack. To implement the mitigation algorithm, the authors

used two datasets. The first dataset was the 2007 CAIDA dataset, and the second one was created by using the Bonesi tool to stimulate DDoS botnet traffic. The experimental evaluation showed the proposed mitigation method is effective in terms of detecting TCP-SYN and ICMP flooding attacks within the SDN environment. However, the authors must validate their approach in a recent real traffic dataset rather than old or synthetic datasets. Diaz *et al.* [26] proposed a flexible modular framework for detecting and mitigating low-rate DDoS attacks in the SDN environment. The proposed model includes two modules: an intrusion prevention system (IPS) and an intrusion detection system (IDS). The authors used a diverse range of ML and DL techniques for DDoS classification implemented within the IDS. The proposed mechanism used the 2017 CIC DoS dataset to train and test ML algorithms. The performance results showed that the proposed approach is effective in the face of slow- and low-rate DDoS attacks in the SDN setting. However, the authors did not compare the performance results with other related works. Dehkordi *et al.* [126] proposed a detection method that makes use of statistical and ML approaches for DDoS detection. The implemented model aimed to detect HTTP application layer DDoS whether high- or low-volume attacks. The proposed framework comprised three main sections: collector, entropy-based, and classification modules. To validate the model, the detection approach used three datasets: the UNB-ISCX, CTU-13, and ISOT datasets. The evaluation results showed that the proposed mechanism performed better than the other approaches mentioned in the article. However, the authors must validate their approach with recent real traffic datasets. Sahoo *et al.* [127] proposed a detection mechanism that employs SVM as the learning algorithm for malicious traffic classification. The model used kernel principal component analysis (KPCA) during the feature extraction phase and utilized a genetic algorithm (GA) for optimizing different settings of the SVM classifier. To evaluate, train, and test the proposed model, the authors used two different datasets which contained normal traffic and different DDoS attacks, including UDP flooding, HTTP flooding, Smurf, and SiDDoS. The evaluation results revealed that the proposed method reduced the false alarm rate and exhibited a higher accuracy rate. However, the authors did not compare the performance results with other related works. Virupakshar *et al.* [128] proposed a detection mechanism for DDoS attacks with two levels of security. In the first process, the DDoS attack signature is identified by using an open source intrusion detection system called Snort. In the second security phase, the proposed method employed two ML techniques named the DNN and SVM to predict DDoS attacks. For the training and testing stages, the KDD Cup 1999 dataset was applied to ML algorithms for DDoS classification. The evaluation results demonstrated that the DNN gave higher accuracy in contrast with SVM. However, a recent dataset would be more appropriate to use and produce the performance results. Various use of ML approaches in SDN environments can appear in Table 4.

## C. DDoS DEFENSE SYSTEMS BASED ON ML TECHNIQUES IN NFV ENVIRONMENTS

The NFV process has attracted significant research attention in recent years [76]. The main concept behind NFV concerns decoupling network functions and network services (i.e., load balancers, routers, and firewalls) from dedicated hardware to instead run on high-volume servers (x86 server) as software [77]. NFV provides various features that serve to reduce the capital expenditures (CAPEX) and operating expenses (OPEX) [78]. Another significant feature of NFV is automation, as it shifts the mission of network functions from administration to technology [79]. Fig. 12 presents the NFV architectural framework [79].

The SDN/NFV combination has recently been used to mitigate DDoS attacks. Fig. 13 illustrates how an SDN and NFV can be integrated to mitigate such attacks [80]. Many related works have proposed different methods relying on ML approaches that can use an NFV environment to help beat DDoS attacks. This subsection discusses the different available approaches that utilize an NFV environment and ML techniques to combat DDoS attacks.

Abdulqadder *et al.* [81] proposedan attack-aware security provisioning approach for DDoS attack mitigation in the context of the SDN/NFV combination with a 5G network. The proposed approach has the following features: (1) an access point (AP), (2) trusted authority (TA), (3) an open virtual switch (OVS), (4) an SDN controller, (5) a user, and (6) virtual network functions (VNF). The proposed approach uses a genetic algorithm to perform the best feature selection for the classifications. The traffic is classified using the radial basis function with extreme learning machine (RBF-ELM) so that malicious packets can be distinguished from legitimate traffic. The malicious traffic is dropped at the VNF, while the legitimate traffic is rerouted to the controller. The experimental evaluation showed that the proposed approach achieved a higher accuracy rate, a higher packet transmission rate, a lower delay, and a lower packet loss ratio. However, there are not enough details about the dataset used. Kalliola *et al.* [82] proposed a flexible mitigation testbed environment to develop and evaluate security orchestration in the context of NFV. The proposed method employed ML techniques to classify normal and attack traffic. The results of the ML classifiers are provided to the orchestrator so as to prevent the VNFs from being compromised. Further action is then taken, such as filtering and rerouting the captured packets for additional investigation. The experimental results showed that the proposed approach is effective in terms of mitigating different types of attacks. However, the proposed work should be validated with a real traffic dataset. Aljuhani *et al.* [83] designed and developed an App-DDoS attack detection and mitigation model to protect webservers against App-DDoS attacks. They first developed a holistic DDoS mitigation model to detect and mitigate a diverse range of DDoS attacks [54]. Based on this defense framework, the authors derived a novel scheme for mitigating App-DDoS cyberattacks. The defense system utilizes three modes: normal, screening, and

**TABLE 4.** Comparison of DDoS defense system based on ML approaches in SDN environments.

| Reference | Types of DDoS attacks | ML techniques used | Dataset | Evaluation metrics | Best accuracy, precision, TPR, and FPR |
|---|---|---|---|---|---|
| [67] | TCP, UDP, and ICMP | Improved KNN algorithm | Synthetic dataset | TPR, FPR, precision, recall, AUC, and f-measure | Accuracy: 0.91<br>Precision: 0.993<br>TPR: 0.994<br>FPR: 0.009 |
| [68] | Network layer DDoS attacks | BiLSTM-RNN neural network algorithm | Synthetic dataset | Accuracy rate and CPU utilization | Accuracy: 98.88<br>Precision: not available<br>TPR: not available<br>FPR: not available |
| [69] | Network layer DDoS attacks | I-BS | Synthetic dataset | Detection rate, FPR, attack mitigation (packet/second), and ROC area | Accuracy: 100.0<br>Precision: not available<br>TPR: not available<br>FPR: 26.0 |
| [70] | TCP_SYN flood, UDP flood, and ICMP flood | PSO-BP neural network | Synthetic dataset | Detection rate, accuracy rate, and FPR | Accuracy: 98.02<br>Precision: not available<br>TPR: not available<br>FPR: 1.43 |
| [71] | HTTP flood attacks | SVM | KDD99 dataset | TPR, FPR, false negative rate, and true negative rate | Accuracy: 0.998<br>Precision: not available<br>TPR: number of 191598<br>FPR: number of 553 |
| [72] | ICMP and TCP flood attacks | J48, random forest, SVM, and KNN | Synthetic dataset | Accuracy rate, precision, recall, F1-score, sensitivity, and specificity | Accuracy: 1.00<br>Precision: 1.00<br>TPR: 1.00<br>FPR: not available |
| [73] | TCP, UDP, and ICMP | KNN, naive Bayes, SVM and SOM | CAIDA 2016 | TPR, FPR, false negative rate, and true negative rate | Accuracy: 98.12<br>Precision: not available<br>TPR: 85.49<br>FPR: 2.51 |
| [74] | TCP, UDP, ICMP | SVM-SOM | Synthetic dataset | Accuracy rate, detection rate, false alarm rate, false negative rate, and true negative rate | Accuracy: 98.12<br>Precision: not available<br>TPR: 85.49<br>FPR: 2.51 |
| [75] | Low-rate DDoS attacks | FM | NSL-KDD, DARPA 98, and CAIDA dataset | Accuracy rate, precision, recall, AUC, ROC area, and forwarding success rate under different attack rates | Accuracy: 0.958<br>Precision: 0.950<br>TPR: 0.946<br>FPR: not available |
| [15] | Slowloris, slow http, and http flood | RNN, LSTM, and CNN | CICIDS2017 | Accuracy rate, precision, recall, F1-measure, test time, train time, and CPU usage | Accuracy: 99.45<br>Precision: 99.57<br>TPR: 99.64<br>FPR: 0.0 |
| [124] | UDP, and SYN flooding attacks | Advanced support vector machine (ASVM) | Synthetic dataset | Training data time, testing data time, false alarm rate, detection rate, and accuracy | Accuracy: 0.97<br>Precision: not available<br>TPR: 0.97<br>FPR: 0.02 |
| [125] | TCP-SYN and ICMP flood attacks | K-Nearest Neighbors (KNN) | CAIDA 2007 and Synthetic dataset | Accuracy rate, precision, recall, and F1-score. | Accuracy: 0.9910<br>Precision: 0.991<br>TPR: 0.991<br>FPR: not available |
| [26] | Slow and low rate DDoS attacks | J48, Random Tree, REP Tree, Random Forest, Multi-Layer Perceptron (MLP), and SVM | CICIDS2017 dataset | Accuracy rate, precision, recall, false alarm rate, and F1-score | Accuracy: 0.95<br>Precision: 0.954<br>TPR: 0.50<br>FPR: 0.005 |
| [126] | HTTP attacks | K-fold | UNB-ISCX, CTU-13 and ISOT datasets | Accuracy rate, precision, recall, false alarm rate, true positive rate, and F1-score | Accuracy: 99.85<br>Precision: 99.64<br>TPR: 98.60<br>FPR: 0.1 |
| [127] | UDP flood, HTTP flood, Smurf, and SiDDoS | SVM | NSL-KDD, and DDoS datasets | Accuracy, recall, precision, and total training time | Accuracy: 98.90<br>Precision: around 99.00<br>TPR: 98.60<br>FPR: not available |
| [128] | Network layer DDoS attacks | DNN and SVM | KDD Cup'99 dataset | Accuracy rate, precision, and recall | Accuracy: 0.923<br>Precision: around 0.9<br>TPR: approximate 1<br>FPR: not available |
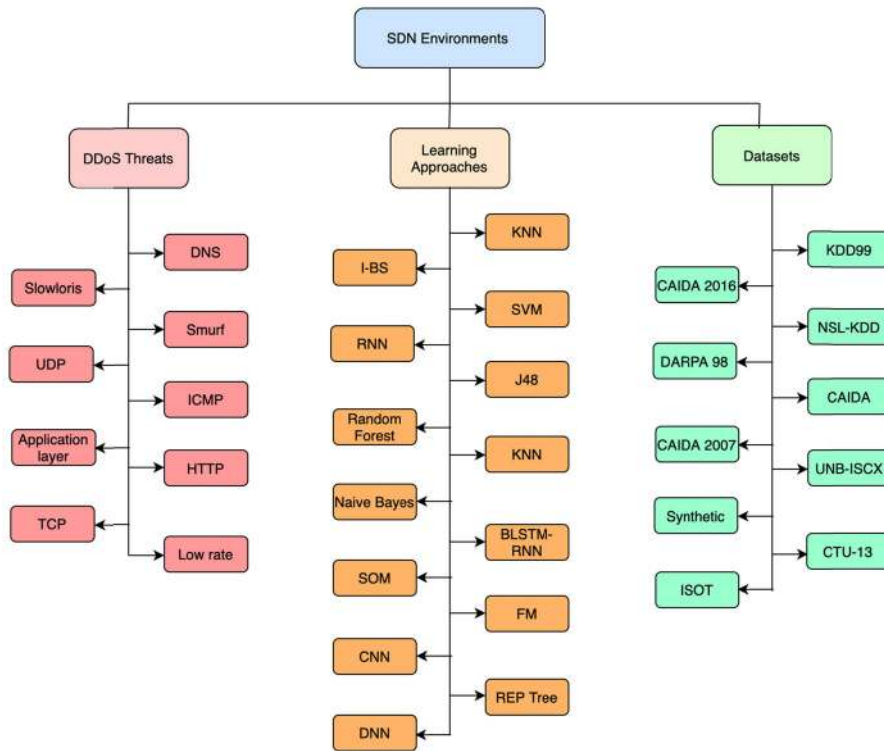
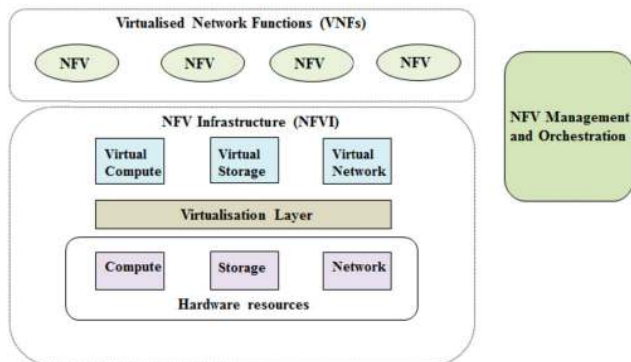**FIGURE 15.** Summary of DDoS threats with the used learning approaches and datasets in SDN environments.



**FIGURE 16.** NFV architectural framework (adapted from [79]).



**FIGURE 17.** Enabling SDN/NFV to mitigate DDoS attacks (adapted from [80]).

suspicious. The defense system switches between the modes according to the server load. The detection method employs ML techniques in the screening mode. The experimental evaluation showed that the proposed approach could successfully mitigate App-DDoS attacks. However, the proposed scheme is limited to App-DDoS attacks. Alharbi *et al.* [84] presented a collaborative SYN flooding mitigation approach using NFV. The proposed approach can detect and mitigate attacks without any involvement from the administrator. The approach involves two modes, namely the stand-by and deep screening modes. In the stand-by mode, agents calculate the network traffic and listen for any start/stop request messages from the controller. When a message is flagged with a start request, it calls up the deep screening mode for further
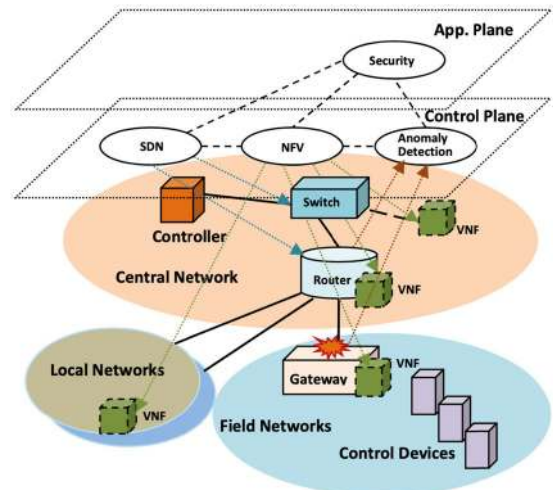
investigation. In the deep screening mode, agents collect a sample of the SYN packets. The important features are then extracted. Based on the extracted features, a classification process is performed using the DBSCAN algorithm. After attempted attacks are identified, the proposed defense system generates policy rules to prevent the attacks. Further, the XFirewall [85] is instantiated and configured with the new ruleset to block any detected attacks. The experimental results demonstrated that the proposed defense approach is effective

**TABLE 5.** Comparison of DDoS defense system based on ML approaches in NFV environments.

| Reference | Types of DDoS attacks | ML techniques used | Dataset | Evaluation metrics | Best accuracy, precision, TPR, and FPR |
|---|---|---|---|---|---|
| [81] | Network Time Protocol (NTP), Hyper Text Transfer Protocol (HTTP), and Simple Mail Transfer Protocol (SMTP) | RBF-ELM | Not specified | Detection accuracy rate, the number of packets redirected, packet transmission rate, average delay, and packet loss ratio | Accuracy: 95.3 Precision: not available TPR: not available FPR: not available |
| [82] | Volumetric attack | Not specified | Synthetic dataset | Packet drops and QoS | Accuracy: not available Precision: not available TPR: not available FPR: not available |
| [83] | HTTP flooding attacks | Logistic regression | ClarkNet-HTTP and customized dataset | CPU usage, memory usage, traffic rate, transmission rate, and response time | Accuracy: not available Precision: not available TPR: not available FPR: not available |
| [84] | SYN flooding attack | DBSCAN | Synthetic dataset | Transmission rate, traffic rate, response time, normal traffic, and malicious traffic | Accuracy: not available Precision: not available TPR: not available FPR: not available |
| [86] | ICMP, IGMP, Smurf attack, TCP-SYN, UDP flooding attack, PUSH-ACK attack, and low-slow rate attack | SVM and SOM | CAIDA and customized datasets | Accuracy rate, detection rate, false alarm rate, detection performance rate, and CPU utilization rate | Accuracy: 99.30 Precision: 0.993 TPR: not available FPR: 0.67 |
| [87] | Network and application DDoS attacks | ALM | Synthetic dataset | Accuracy rate, false alarm rate, precision, and exposure rate | Accuracy: 0.91 Precision: 1.0 TPR: not available FPR: 0.00 |
| [50] | SYN flooding attacks | Single SVM and multiple SVMs model | Synthetic dataset | Detection accuracy rate, TPR, and FPR | Accuracy: 0.91 Precision: 1.0 TPR: 0.994 FPR: 0.009 |

with regard to mitigating SYN flooding attacks in the context of NFV.However, the proposed approach is limited to SYN flooding attacks. Phan *et al.* [86] proposed a novel hybrid ML model for attack classifications. Their hybrid model combines two machine learning algorithms, namely the SVM and SOM algorithms. Additionally, the authors proposed an enhanced history-based IP filtering approach to achieve a better detection rate and to improve the speed of detecting attackers' IP. The performance metrics demonstrated that the proposed approach is effective and practical in relation to beating DDoS attacks in the context of an SDN and NFV environments. However, the proposed approach must be tested with recent real traffic datasets. Janarthanam *et al.* [87] proposed a detection framework that adapts ML techniques to combat DDoS attacks. The framework involves traffic data collection, feature extraction, and the classification of the collected traffic in an effort to distinguish normal users from attackers. The authors used the adaptive learning method (ALM) to recognize DDoS attacks. The experimental results revealed the accuracy of the proposed method to be 97%. However, the proposed method should be tested with a real traffic dataset to validate the proposed detection method.

Diverse use of ML approaches in NFV environments can appear in Table 5.

### D. DDoS DEFENSE SYSTEMS BASED ON ML TECHNIQUES IN IoT ENVIRONMENTS

The IoT has been the subject of significant research interest in recent years [88]. It connects a tremendous number of physical devices (or "things") around the world that are capable of collecting and sharing data over the Internet [89]. The IoT facilitates people's daily life by connecting various objects (e.g., cars, homes, kitchen appliances, etc.) to smart devices that can receive and send data via wireless networks without the need for human interaction [90], [91]. The IoT offers numerous advantages, which is why this technology has grown rapidly and been widely adopted around the world. As a result, both the industrial and research domains have had to make significant changes to adapt to the demands of IoT-related technology [89]. Yet, despite the attention that has been paid to the IoT, related security issues remain a key concern [92]. One major security issue concerning IoT environments is their vulnerability to DDoS attacks, which can cause service disruption and so affect the quality of
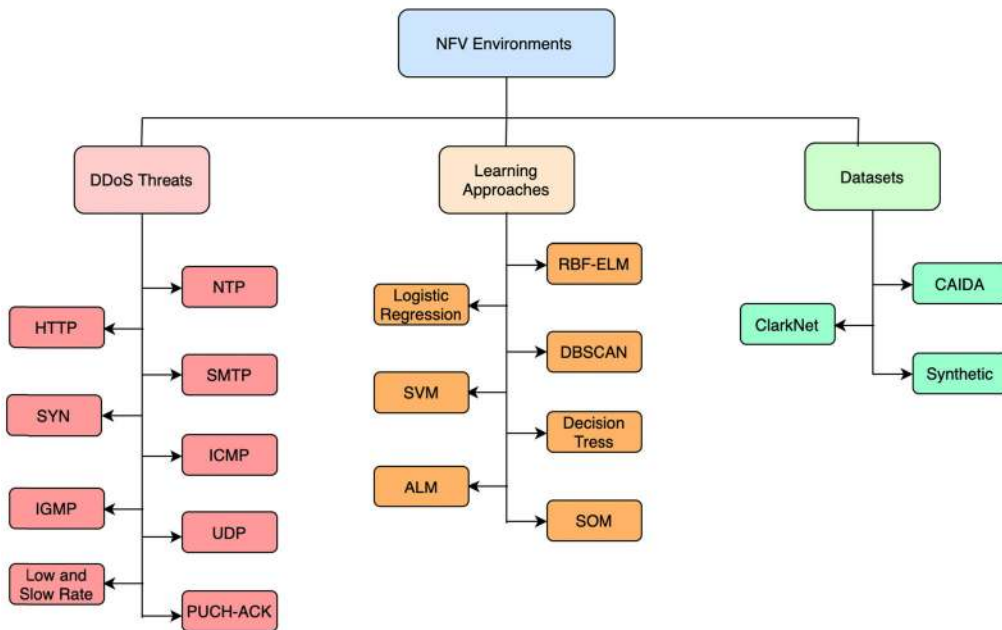
**FIGURE 18.** Summary of DDoS threats with the used learning approaches and datasets in NFV environments.

service (QoS). Even worse, attackers can exploit security weaknesses within IoT devices in order to turn them into zombie machines capable of attacking another target [93]. This subsection discusses the various approaches that make use of ML techniques in IoT environments to combat DDoS attacks.

Roopak *et al.* [94] proposed a deep learning approach for tackling cyber threats within IoT networks, including DDoS attacks, and then evaluated the proposed algorithm using a recent dataset known as CICIDS2017. The authors used four different learning algorithms for the attack classifications, namely the 1d-CNN, LSTM, CNN, and LSTM algorithms. The authors also compared the proposed approach with other ML algorithms and observed the differences in terms of accuracy, precision, and recall. However, the proposed method is limited to specific types of DDoS attacks, and only one dataset was used to test the model. To conclude, the authors set out some open research challenges when using deep learning within the cyber security domain. Soe *et al.* [95] proposed a detection approach that uses ANN for the DDoS attack classifications in IoT environments. The authors used a modern public attack dataset (Bot-IoT) to achieve a better detection rate. As the utilized dataset featured a small amount of legitimate data and a large amount of attack data, the authors used the synthetic minority over-sampling technique (SMOTE) to resolve the data variation issue and develop a ML detection system in the face of DDoS attacks. The detection results showed the proposed system to be effective in terms of defending IoT environments from DDoS attacks. However, the proposed mechanism is limited to specific types of DDoS attacks. Ravi *et al.* [96] proposed

a novel approach known as learning-driven detection mitigation (LEDEM) for the DDoS attack classifications. The authors used the semi-supervised deep extreme learning machine (SDELM) approach for the DDoS detection. With regard to the mitigation stage, the authors provided a novel mitigation algorithm that falls within the class of approximation algorithms, and they demonstrated it to be a two-approximation algorithm. The proposed model was tested in a testbed, and the experimental results demonstrated the effectiveness of the solution in relation to preventing DDoS attacks in IoT environments. However, the proposed approach is limited to UDP flooding attack, and only one dataset was used to test the model. Roopak *et al.* [97] proposed an IDS that made use of feature selection and a deep learning model for the categorization of DDoS attacks. They used the jumping gene-adapted NSGA-II algorithm to perform the feature selection. For the deep learning model, they used a convolutional neural network (CNN) integrated with long short-term memory (LSTM). The evaluation results showed the proposed approach to be effective against DDoS attacks. Additionally, it exhibited a high accuracy rate when compared with state-of-the-art techniques. However, it would be interesting to evaluate the proposed approach with more real traffic datasets.

Li *et al.* [98] proposed an approach for the classification of DDoS attacks in IoT environments involving an extreme learning machine (ELM). The authors used the joint entropy method at the feature extraction stage. The size of the dataset used in the experiment ranged from 1000 to 20,000, and it contained protocols such as the ICMP, UDP, and TCP. The evaluation results showed that the proposed mechanism

IoT Network
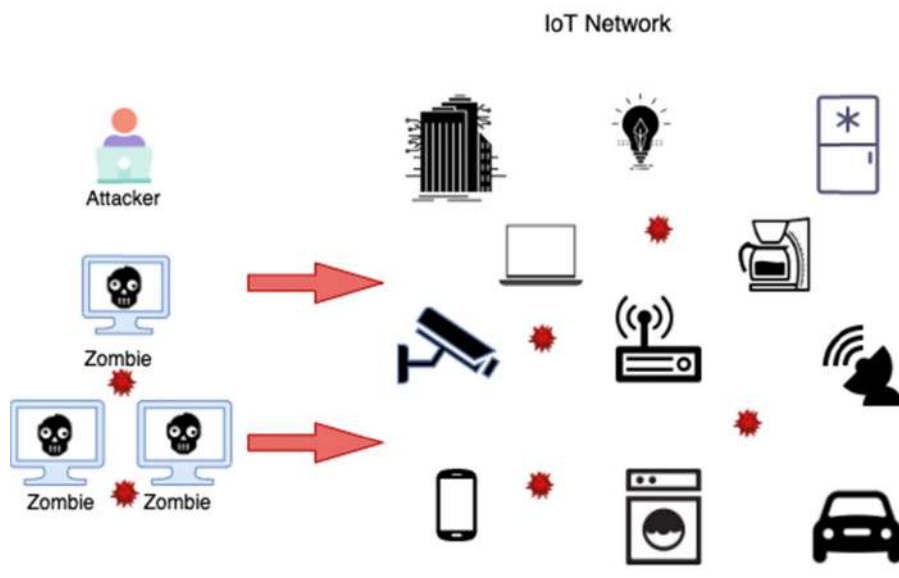


FIGURE 19. DDoS attacks in the context of IoT environments.

performed better than the other approaches mentioned in the article. However, the authors need to evaluate the proposed detection method with recent real traffic datasets.

Meidan *et al.* [99] proposed a novel approach for anomaly detection known as N-BaIoT, which made use of deep autoencoders in IoT environments. The proposed approach acted as a fully automated detector, unlike other proposed approaches. The authors used real traffic data collected from nine different IoT devices that were infected by botnets. The experimental evaluation showed the proposed method to be effective in terms of detecting malicious traffic within IoT environments. However, no accuracy measurement was provided in the proposed work for a comparison with other related work.

Su *et al.* [100] proposed a lightweight mechanism for the classification of DDoS attacks using the CNN technique. The proposed method used an IoT DDoS dataset containing 500 malware samples gathered by IoTPOT. The experimental results demonstrated the proposed detection method to be effective with regard to the classification of DDoS attacks generated by botnets. However, the proposed approach is limited to specific type of DDoS attacks.

McDermott *et al.* [101] proposed a detection method that used a bidirectional long short-term memory-based recurrent neural network (BLSTM-RNN) for the classification of DDoS attacks. Four different attacks were selected from the Mirai botnet, including the UDP flood, ACK flood, SYN flood, and DNS flood. The evaluation results showed that the implemented detection method exhibited a high accuracy rate in the face of botnet malware attacks. However, no TPR and FPR measurements were provided in the proposed work for a comparison with other related work. Doshi *et al.* [162] proposed an anomaly detection pipeline consisting of four major categories: traffic network capture, grouping of

packets by device and time, feature extraction, and binary classification. The IoT detection pipeline captures the network packets after collecting the network traffic. It then splits the packets by device, before generating feature vectors based on the packets for the classification algorithm. The proposed approach relies on five different ML algorithms, all of which were found to provide higher accuracy (greater than 0.99). The proposed approach gave rise to higher performance results when compared with the results of related studies mentioned in the article. However, the proposed work used a synthetic dataset, which affected the quality of the performance. Parra *et al.* [129] proposed a novel distributed deep learning approach to detect attacks in IoT environments. The proposed approach is composed of two main security methods: 1) a DCNN for identifying phishing and App-DDoS attacks 2) the LSTM model deployed at back-end servers for detecting botnet attacks. To train and test the proposed model, the authors used the N_BaIoT dataset for IoT attack detection. The evaluation results showed that the proposed mechanism achieved higher detection accuracy and a higher F-1 score. However, the comparison of the different proposed methods did not use the same datasets. Ma *et al.* [130] proposed a deep learning framework for DDoS attack detection in the context of the IoT. The detection method employed a CNN for data classification. In the training and testing phase, the authors used the benchmark NSL-KDD datasets to perform the experiment and evaluate the proposed detection approach. The proposed detection approach was implemented in TensorFlow, and the experimental results demonstrated the effectiveness of the solution in relation to preventing DDoS attacks in IoT environments. In future work, the authors intend to improve the detection performance results. Various use of ML approaches in IoT environments can appear in Table 6.

**TABLE 6.** Comparison of DDoS defense system based on ML approaches in IoT environments.

| Reference | Types of DDoS attacks | ML techniques used | Dataset | Evaluation metrics | Best accuracy, precision, TPR, and FPR |
|---|---|---|---|---|---|
| [94] | Network DDoS attacks | CNN, LSTM, CNN+LSTM | CICIDS2017 | Accuracy, precision, and recall | Accuracy: 97.16 Precision: 98.44 TPR: 9.20 FPR: not available |
| [95] | Network DDoS attacks | ANN | Bot-IoT | Detection response time, throughput, and detection time | Accuracy: 100 Precision: not available TPR: 1.0 FPR: 0.0 |
| [96] | UDP flooding attacks | Semi supervised deep extreme learning machine (SDELM) | UNB-ISCX | Network accuracy, precision of DDoS detection (PoD), recall of DDoS detection (RoD), precision of benign detection (PoB), recall of benign detection (RoB), and F-measure | Accuracy: 97.9 Precision: 98.1 TPR: 98.2 FPR: not available |
| [97] | Network DDoS attacks | CNN and LSTM | CISIDS2017 | Accuracy rate, recall, precision, and F1-score | Accuracy: 99.03 Precision :99.26 TPR: 99.35 FPR: not available |
| [98] | ICMP, UDP, and TCP | ELM | Synthetic dataset | Accuracy rate and training time with different hidden layers | Accuracy: 99.4 Precision: not available TPR: not available FPR: 0.020 |
| [99] | UDP, SYN, TCP | Deep autoencoder | Detection_of_IoT_botnet_attacks_N_BaIoT dataset | TPR and FPR | Accuracy: not available Precision: not available TPR: 100.0 FPR: 0.007 ± 0.01 |
| [100] | Network DDoS attacks | CNN | IoT DDoS malware dataset | Accuracy, confusion matrix for 2-class classification, confusion matrix for 3-class classification | Accuracy: 94.0 Precision: not available TPR: 94.67 FPR: 6.67 |
| [101] | UDP flood, ACK flood, SYN flood, and DNS flood. | BLSTM-RNN | Synthetic dataset | Accuracy and loss metrics | Accuracy: 99.99 Precision: not available TPR: not available FPR: not available |
| [162] | TCP SYN flood, UDP flood, and HTTP GET flood | K-nearest neighbors, random forests, decision trees, SVM, and deep neural networks | Synthetic dataset | Accuracy rate, precision, recall, f-measure, attack distribution, average bandwidth, packet intervals, and number of unique IP destinations | Accuracy: 99.9 Precision: 99.9 TPR: 99.8 FPR: not available |
| [129] | Application layer DDoS attack | CNN | N_BaIoT dataset | Accuracy rate, precision, recall, TPR, TNR, FPR, and FNR | Accuracy: 0.9430 Precision: 0.9348 TPR: 0.9367 FPR: 0.0520 |
| [130] | TCP, UDP, and ICMP | CNN | NSL-KDD dataset | Accuracy rate, detection rate, false alarm, and run time | Accuracy: 92.99 Precision: not available TPR: not available FPR: 0.70 |

## IX. DDoS ATTACK MITIGATION TECHNIQUES

Many different mitigation techniques have been proposed with regard to DDoS attack mitigation in modern networking environments. This section discusses mitigation strategies that have been employed to eliminate and prevent DDoS attacks in a diverse range of modern networking environments.

Dropping packets of identified attack traffic as a mitigation technique has been employed in modern networking environments such as an SDN [133]– [135]. It is a very quick and simple approach to prevent an attack source from disrupting services. However, this technique may also drop legitimate traffic and prevent normal users from accessing the services. Another mitigation method is blocking the
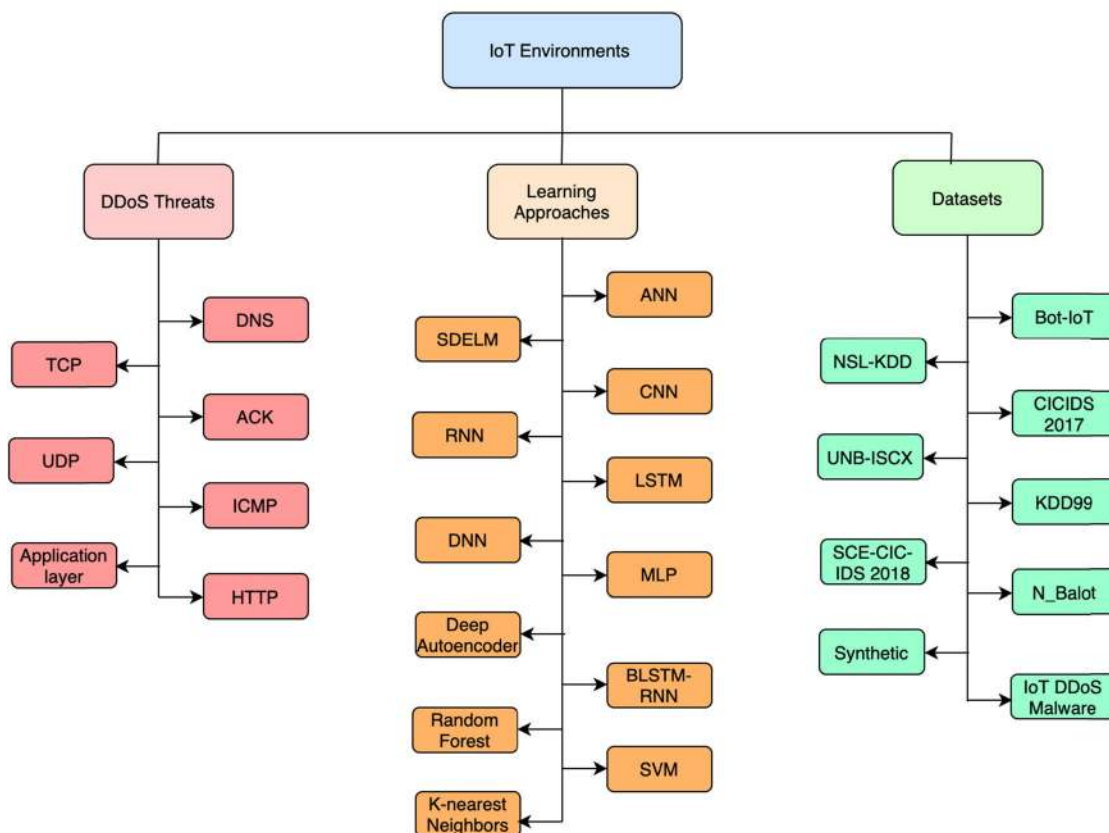
**FIGURE 20.** Summary of DDoS threats with the used learning approaches and datasets in IoT environments.

attacker's ports [136] so that no further traffic can proceed. In this case, the malicious traffic from the attacker source is not able to access the distention host; however, this may result in blocking the legitimate traffic port if it is mistakenly reported as an attacker source. Another known mitigation technique is redirection in which legitimate clients are redirected into a new IP address [137], so the attacker has no clue about the new IP address and cannot generate DDoS attacks directly at it. The critical part of this technique is that it is hard to distinguish attack traffic from the traffic of normal users, to correctly redirect normal clients to the new IP address and avoid wrongly redirecting attack traffic to the new IP address. Another mitigation strategy is the IP traceback method [138], [139], in which the defense system traces the attack traffic back to the source that originated the malicious traffic. Honeypot is another mitigation strategy that has been deployed in modern networking environments in which the honeypot entity acts as a real server, aiming to collect, extract, and analyze suspicious activities to identify attack patterns. Although a honeypot provides great security features, it has limitations, such as system capacity, time consumption for deployment, and high maintenance cost. Rate limiting is another approach that has been employed in previous works [140], [141] in which a technique forces a rate limit on the traffic detected as malicious packets via the detection approach. This approach is a useful mitigation strategy when it is hard to identify attack traffic with the detection

method, which decreases the false positive rate. Signature filtering is another prevention technique in which a defense strategy filters out known attack traffic that was reported by the detection mechanism. However, this technique is limited to known attack patterns, as it works based on a predefined attack signature, a filtering method that is not practical with malicious traffic that includes zero-day attacks.

Some mitigation strategies take advantage of NFV and SDN environments in preventing DDoS attacks. Although an SDN provides central control in which the controller maintains and manages the global network view, NFV promises flexibility to its virtualized security functions (VSFs) such as IDs or a firewall. NFV also has the ability to adapt new rules dynamically, or even to create a new security function on demand and remove it after a security function has completed its purpose, aiming to accelerate deployment and provisioning of network security services. Another great feature provided by NFV is scalability when a new instance must be added to the existing VSF (scaling out) or one or more instances removed from the existing VSF (scaling in). Additionally, NFV supports scale up or down when resources (e.g., CPU/memory) must be added or removed from the existing VSF. Scaling a network function in/out (horizontal) or up/down (vertical) can be done through the NFV orchestrator (NFVO). With these advantages, many works have proposed DDoS mitigation approaches with the help of SDN and NFV features [142]– [145].

**TABLE 7.** DDoS attack mitigation techniques.

| Mitigation techniques | Description |
|---|---|
| Dropping Packets | Dropping attack's packets and transmitting legitimate users based on the defined rules |
| Blocking ports | The malicious traffic from the attacker's port is entirely blocked |
| Redirection | The normal traffic will be redirected to the new IP address |
| IP Traceback | Tracing the attacks traffic back to the source that originates malicious traffic |
| Honeypot | Aim to collect and analyze suspicious activities to identify attacks pattern |
| Rate Limiting | Limiting the rate transmission during the incident |
| Signature Filtering | Filtering the network traffic based on the known attack signatures |

## X. DISCUSSION AND RESEARCH CHALLENGES

After a review was conducted and a broad analysis of the potential uses of ML to combat DDoS attacks was provided, further improvements are needed to design and develop a solid mitigation method based on ML techniques. As machine learning methods depend on the training phase to learn from the given dataset and establish the learning profile to distinguish patterns, many works reviewed in this article used a synthetic dataset (not a real dataset) which affected the level of accuracy. Another observation is the lack of new real datasets to allow researchers to evaluate their methods and compare the results with other works. Most of the current real datasets either are old (and thus, are not suitable for mitigating recent DDoS attacks) or do not include enough data patterns to learn from the most common attack features during the training phase which affects the training quality. In addition, even if a real dataset exists, it cannot be shared with the public due to privacy issues. As this review used ML methods to combat DDoS attacks in modern networking environments, the experimental evaluation should consider other factors to measure that are related to this environment, not only the accuracy level. Some modern networking technologies benefit from features such as automation and scaling resources to build a complete defense system with the integration of ML detection. This system's robustness related to such an environment should be investigated.

Although some works showed promising results in detecting attacks, validating the approaches in a large-scale network is highly recommended.

As attackers are capable of developing new techniques and trying harder to perform successful DDoS attacks, many works aimed to mitigate limited types of such attacks which make the approaches vulnerable to other types of DDoS attacks. In addition, some works did not consider advanced attacker techniques within the type of attack the works tried to solve. For example, attacks now make use of botnets, a large group of compromised devices mimicking normal users, which make the defense systems struggle in detecting this sophisticated technique.

As another observation regarding the experimental evaluation, many works used tools to simulate an attacker and normal user behavior, while an effective DDoS attack in

a real-world scenario uses a large group of real infected machine "zombies" to perform destructive DDoS attacks. This approach should test the effectiveness and robustness of a defense system in a real environment to validate the system's robustness. There are some research challenges while developing an effective and practical defense system using ML approaches.

### A. DATASET
As it is very difficult to identify a suitable dataset for a specific type of DDoS attack, most researchers either use existing datasets or create their own dataset. The major limitation of using an existing dataset that it is very old and so not applicable for testing a system's robustness [102], [103]. It is known that attacks such as DDoS attacks adapt advanced techniques and become more sophisticated in order to circumvent any security measures, which means that it is not good practice to rely on results based on old datasets. Even if researchers use a synthetic dataset, it is difficult to mimic a real dataset, that is, to reflect attacks that have already occurred and caused damaged to a victim. Another issue related to the dataset is privacy, as organizations that have experienced DDoS attacks in the past are unlikely to share the relevant information and log files with the public.

### B. FEATURE SELECTION
Choosing the most suitable features is crucial in relation to identifying the behavior of attacks. The selected features are trained and tested using ML techniques so that they can effectively predict attacks. Identifying a method that determines the optimal selected features from among the many other features represents another challenge facing researchers [9].

### C. FLASH CROWD
A flash crowd may form when numerous normal clients try to simultaneously access web services [104], [105]. Thus, a flash crowd typically occurs during special events taking place within a specific time frame. In such a situation, service providers encounter a heavy load due to many legitimate clients attempting to access a webserver at the same time. Many defense systems have developed different detection approaches, but some failed to identify DDoS attacks from

normal flash crowd event. A detection model should be capable of distinguishing a flash crowd from a DDoS attack in order to avoid blocking legitimate clients or allowing attackers to overwhelm a webserver during such an event.

### D. LIGHTWEIGHT DEFENSE SYSTEMS

DDoS attacks have become more advanced and so more difficult to mitigate in recent years. A lightweight defense system would help to reduce a system's overhead and to increase its detection speed, which should result in attacks being effectively and very quickly eliminated. Although some ML methods work effectively to mitigate DDoS attacks, the complexity level increases the system's overhead which affects the performance of detecting and mitigating such an attack.

### E. EARLY DETECTION

Many detection methods only begin investigating DDoS attacks after they have already taken place and caused damage to the system. A mechanism capable of detecting DDoS attacks at an early stage and preventing attackers from accessing services is a crucial part of any defense system. Some modern networking technologies such as SDN and NFV provide on demand instantiating network function and resource allocation. Such thing can help to develop an automated mechanism to trigger system's resources and observe anomalies or unusual behavior at an early stage.

### F. ATTACKERS MIMICKING NORMAL USERS BY USING A BOTNET

The need to mitigate a botnet should be considered when developing and implementing any detection approach. A DDoS attack in the form of a botnet is able to deceive the security measures of any defense system due to its ability to mimic a normal user's behavior, which makes it very difficult to detect and eliminate. Further, when an attacker attempts to send malicious requests from a huge group of botnets, the requests appear similar to normal user behavior, with their identical features making them difficult to discover. Moreover, when an attacker knows the threshold of a given detection model and starts launching DDoS attacks using a botnet below that threshold, the defense system will not detect the attack and will instead consider the requests to come from normal users. Even worse, botnet attacks that are not discovered sufficiently early may force service providers to increase the system's resources in an effort to meet client demands, which would be a poor decision because some of the requests are coming from malicious sources.

### G. SLOW-RATE DDoS ATTACK DETECTION

A slow-rate attack is one type of DDoS attack in which the attacker generates traffic in slow mode toward the victim's webserver; making the traffic resemble legitimate users. Because of the nature of this type of attack, it is very difficult to distinguish whether the traffic is normal or an attack [146].

The slow-rate DDoS attack is able to circumvent webserver security measures and bypass the victim host's mitigation strategies. Even worse are slow-rate DDoS attacks generated by botnets, which cause a tremendous impact on the victim side and make the webserver unreachable for its clients within a short period of time.

### H. DISTRIBUTED PROCESSING OF DDoS ATTACKS USING HADOOP AND SPARK

Hadoop is open source Apache software that implements different modules, including distributed file system, MapReduce, Hadoop common, and YARN. Hadoop has the ability to store and process a large amount of data in a parallel, reliable, and fault-tolerant manner. Although Hadoop provides great features in mitigating DDoS attacks [147]– [150], some challenges have been raised, such as the detection performance is affected when the process is distributed into different cluster nodes which increases the cluster size [147]. Another challenge is that a small log file cannot track a large number of attackers. In addition, the live capturing stage in Hadoop consumes a large amount of time during the detection phase [149], which affects the overall mitigation time.

Spark is another open source distributed engine system, which aims to deal with big data [151]. Spark distributes data into a cluster in parallel and works fast in processing data as it operates on memory rather than disk drives. Spark provides a small processing delay in contrast to Hadoop, and it is faster than Hadoop MapReduce [152]. Several related works employed the Spark framework to mitigate DDoS attacks [123], [152]– [155]; however, Spark does not support file management systems, which raises the need to integrate with other platforms. Another challenge is that memory becomes a bottleneck when dealing with a large amount of data. Keeping the data in memory is very expensive, and additional memory resources are required when a massive amount of data must be processed in computation [156].

### I. AUTOMATION

Automation is a very important feature when it comes to mitigating DDoS attacks without any involvement from the administrator. A defense system designer should implement an automated mitigation model that can identify and block attacks without the need for involvement on the part of the administration. A modern technology such as NFV is able to provide the automation feature [106], which should help developers to implement an automated online defense system. A detailed report concerning the attack details is automatically generated so that the administrator can make necessary changes or update the system's security measures to be more robust in the face of attacks.

### J. STANDARD METRICS PERFORMANCE

As this paper reviewed many prior works and reported on the different utilized evaluation metrics, there is no standard metric available that can be used to contrast with other related works. Such a standard evaluation metric would help to
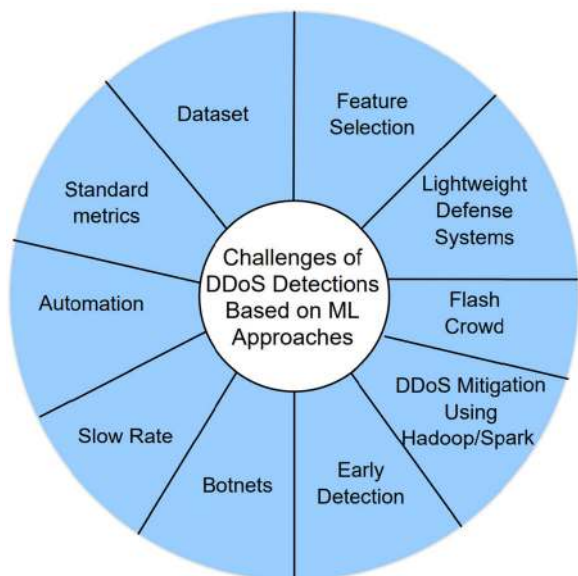
**FIGURE 21.** Challenges of DDoS detections based on ML approaches.

improve the research outcomes and also facilitate the performance of comparisons with related works. We believe that each environment should have a standard metric capable of evaluating the system's entire features in the context of DDoS detection and mitigation. Some network environments including NFV, employ the concept of virtualization which decuples the underlying computer infrastructure from dedicated hardware and deploy them as virtual network functions running on high-volume servers (x86 server) as software. The nature of virtualized environments differs from traditional networking environments. Such performance metrics should take this into account and evaluate the entire system's robustness in the face of DDoS attacks. Fig. 21 presents the challenges of DDoS detections based on ML approaches.

## XI. CONCLUSION
DDoS attacks have become much more difficult to mitigate in recent years, as attackers have found new ways of adapting modern technologies in order to circumvent security measures. Thus, although researchers have proposed a number of different mitigation approaches, DDoS attacks continue to pose a major threat to service providers. This paper elucidated the available DDoS mitigation approaches based on ML/DL techniques in a diverse range of modern networking environments. Additionally, this paper discussed the different classifications of DDoS attacks and ML/DL techniques. As virtualized environments are growing rapidly and becoming much more widely used due to the significant advantages they offer when compared with traditional environments, this paper also discussed DDoS attack mitigation based on ML/DL techniques in the context of cloud computing, SDN, and NFV environments. Moreover, this paper discussed DDoS attacks in IoT environments and detailed the different ML/DL approaches that have been adapted as

security solutions for attack mitigation. Finally, this paper explored some of the challenges currently facing this field of research and outlined important considerations with regard to the design of effective and practical defense systems for combating DDoS attacks.

### REFERENCES

[1] G. Somani, M. S. Gaur, D. Sanghi, M. Conti, M. Rajarajan, and R. Buyya, "Combating DDoS attacks in the cloud: Requirements, trends, and future directions," *IEEE Cloud Comput.*, vol. 4, no. 1, pp. 22–32, Jan./Feb. 2017, doi: 10.1109/MCC.2017.14.

[2] R. Vishwakarma and A. K. Jain, "A honeypot with machine learning based detection framework for defending IoT based botnet DDoS attacks," in *Proc. 3rd Int. Conf. Trends Electron. Informat. (ICOEI)*, Tirunelveli, India, Apr. 2019, pp. 1019–1024, doi: 10.1109/ICOEI.2019.8862720.

[3] J. Li, X. Yi, and S. Wei, "A study of network security situational awareness in Internet of Things," in *Proc. Int. Wireless Commun. Mobile Comput. (IWCMC)*, Limassol, Cyprus, Jun. 2020, pp. 1624–1629, doi: 10.1109/IWCMC48107.2020.9148549.

[4] J. J. Santanna, R. van Rijswijk-Deij, R. Hofstede, A. Sperotto, M. Wierbosch, L. Z. Granville, and A. Pras, "Booters—An analysis of DDoS-as-a-service attacks," in *Proc. IFIP/IEEE Int. Symp. Integr. Netw. Manage. (IM)*, Ottawa, ON, Canada, May 2015, pp. 243–251.

[5] Y. Soupionis and T. Benoist, "Cyber-physical testbed—The impact of cyber attacks and the human factor," in *Proc. 10th Int. Conf. Internet Technol. Secured Trans. (ICITST)*, London, U.K., Dec. 2015, pp. 326–331, doi: 10.1109/ICITST.2015.7412114.

[6] S. S. Priya, M. Sivaram, D. Yuvaraj, and A. Jayanthiladevi, "Machine learning based DDOS detection," in *Proc. Int. Conf. Emerg. Smart Comput. Inform. (ESCI)*, Pune, India, Mar. 2020, pp. 234–237, doi: 10.1109/ESCI48226.2020.9167642.

[7] F. Musumeci, V. Ionata, F. Paolucci, F. Cugini, and M. Tornatore, "Machine-learning-assisted DDoS attack detection with P4 language," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Dublin, Ireland, Jun. 2020, pp. 1–6, doi: 10.1109/ICC40277.2020.9149043.

[8] N. Sultana, N. Chilamkurti, W. Peng, and R. Alhadad, "Survey on SDN based network intrusion detection system using machine learning approaches," *Peer Peer Netw. Appl.*, vol. 12, no. 2, pp. 493–501, Mar. 2019.

[9] NETSCOUT. *Cloud in the Crosshairs NETSCOUT's 14th Annual Worldwide Infrastructure Security Report*. Accessed: Apr. 11, 2020. [Online]. Available: https://www.netscout.com/sites/default/files/2019-03/SECR_005_EN-1901%E2%80%93WISR.pdf

[10] D. Boro and D. K. Bhattacharyya, "DyProSD: A dynamic protocol specific defense for high-rate DDoS flooding attacks," *Microsyst. Technol.*, vol. 23, pp. 593–611, Mar. 2017. [Online]. Available: https://link.springer.com/article/10.1007/s00542-016-2978-0

[11] Y. Zhang and Y. Cheng, "An amplification DDoS attack defence mechanism using reinforcement learning," in *Proc. IEEE SmartWorld, Ubiquitous Intell. Comput., Adv. Trusted Comput., Scalable Comput. Commun., Cloud Big Data Comput., Internet People Smart City Innov. (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)*, Leicester, U.K., Aug. 2019, pp. 634–639, doi: 10.1109/SmartWorld-UIC-ATC-SCALCOM-IOP-SCI.2019.00145.

[12] A. Ghali, R. Ahmad, and H. Alhassan, "Comparative analysis of DoS and DDoS attacks in Internet of Things environment," in *Proc. Comput. Sci. Line Conf.* Cham, Switzerland: Springer, Aug. 2020, pp. 183–194, doi: 10.1007/978-3-030-51971-1_15.

[13] R. Doriguzzi-Corin, S. Millar, S. Scott-Hayward, J. Martínez-del-Rincón, and D. Siracusa, "LUCID: A practical, lightweight deep learning solution for DDoS attack detection," *IEEE Trans. Netw. Service Manage.*, vol. 17, no. 2, pp. 876–889, Jun. 2020, doi: 10.1109/TNSM.2020.2971776.

[14] H. Mohammadnia and S. B. Slimane, "IoT-NETZ: Practical spoofing attack mitigation approach in SDWN network," in *Proc. 7th Int. Conf. Softw. Defined Syst. (SDS)*, Paris, France, Apr. 2020, pp. 5–13, doi: 10.1109/SDS49854.2020.9143903.

[15] S. Haider, A. Akhunzada, I. Mustafa, T. B. Patel, A. Fernandez, K.-K. R. Choo, and J. Iqbal, "A deep CNN ensemble framework for efficient DDoS attack detection in software defined networks," *IEEE Access*, vol. 8, pp. 53972–53983, 2020, doi: 10.1109/ACCESS.2020.2976908.

[16] A. Abhishta, R. Joosten, and L. J. M. Nieuwenhuis, "Analysing the impact of a DDoS attack announcement on victim stock prices," in *Proc. 25th Euromicro Int. Conf. Parallel, Distrib. Netw. Process. (PDP)*, St. Petersburg, Russia, 2017, pp. 354–362, doi: 10.1109/PDP.2017.82.

[17] Q. Yan, F. Richard Yu, Q. Gong, and J. Li, "Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: A survey, some research issues, and challenges," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 1, pp. 602–622, 1st Quart., 2016, doi: 10.1109/COMST.2015.2487361.

[18] G. Somani, M. S. Gaur, D. Sanghi, M. Conti, and R. Buyya, "DDoS attacks in cloud computing: Issues, taxonomy, and future directions," *Comput. Commun.*, vol. 107, pp. 30–48, Jul. 2017.

[19] N. Agrawal and S. Tapaswi, "Defense mechanisms against DDoS attacks in a cloud computing environment: State-of-the-art and research challenges," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 4, pp. 3769–3795, 4th Quart., 2019, doi: 10.1109/COMST.2019.2934468.

[20] R. Vishwakarma and A. K. Jain, "A survey of DDoS attacking techniques and defence mechanisms in the IoT network," *Telecommun. Syst.*, vol. 73, no. 1, pp. 3–25, Jul. 2019.

[21] K. Alieyan, A. ALmomani, A. Manasrah, and M. M. Kadhum, "A survey of botnet detection based on DNS," *Neural Comput. Appl.*, vol. 28, pp. 1–18, Jul. 2017.

[22] R. R. Zebari, S. R. M. Zeebaree, and K. Jacksi, "Impact analysis of HTTP and SYN flood DDoS attacks on Apache 2 and IIS 10.0 Web servers," in *Proc. Int. Conf. Adv. Sci. Eng. (ICOASE)*, Duhok, Iraq, Oct. 2018, pp. 156–161, doi: 10.1109/ICOASE.2018.8548783.

[23] G. A. Jaafar, S. M. Abdullah, and S. Ismail, "Review of recent detection methods for HTTP DDoS attack," *J. Comput. Netw. Commun.*, vol. 2019, pp. 1–10, Jan. 2019.

[24] S. Bhatia, S. Behal, and I. Ahmed, "Distributed denial of service attacks and defense mechanisms: Current landscape and future directions," *Versatile Cybersecurity*, vol. 72, pp. 55–97, Oct. 2018.

[25] K. Singh, P. Singh, and K. Kumar, "Application layer HTTP-GET flood DDoS attacks: Research landscape and challenges," *Comput. Secur.*, vol. 65, pp. 344–372, Mar. 2017. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404816301365

[26] J. A. Pérez-Díaz, I. A. Valdovinos, K.-K. R. Choo, and D. Zhu, "A flexible SDN-based architecture for identifying and mitigating low-rate DDoS attacks using machine learning," *IEEE Access*, vol. 8, pp. 155859–155872, 2020, doi: 10.1109/ACCESS.2020.3019330.

[27] M. Shtern, R. Sandel, M. Litoiu, C. Bachalo, and V. Theodorou, "Towards mitigation of low and slow application DDoS attacks," in *Proc. IEEE Int. Conf. Cloud Eng.*, Boston, MA, USA, Mar. 2014, pp. 604–609, doi: 10.1109/IC2E.2014.38.

[28] S. H. Islam, P. Vijayakumar, M. Z. A. Bhuiyan, R. Amin, V. Rajeev M, and B. Balusamy, "A provably secure three-factor session initiation protocol for multimedia big data communications," *IEEE Internet Things J.*, vol. 5, no. 5, pp. 3408–3418, Oct. 2018, doi: 10.1109/JIOT.2017.2739921.

[29] I. M. Tas, B. G. Unsalver, and S. Baktir, "A novel SIP based distributed reflection denial-of-service attack and an effective defense mechanism," *IEEE Access*, vol. 8, pp. 112574–112584, 2020, doi: 10.1109/ACCESS.2020.3001688.

[30] A. R. Shaaban, E. Abd-Elwanis, and M. Hussein, "DDoS attack detection and classification via convolutional neural network (CNN)," in *Proc. 9th Int. Conf. Intell. Comput. Inf. Syst. (ICICIS)*, Cairo, Egypt, Dec. 2019, pp. 233–238, doi: 10.1109/ICICIS46948.2019.9014826.

[31] J. K. Chahal, A. Bhandari, and S. Behal, "Distributed denial of service attacks: A threat or challenge," *New Rev. Inf. Netw.*, vol. 24, no. 1, pp. 31–103, Jan. 2019, doi: 10.1080/13614576.2019.1611466.

[32] L. Huraj, M. Simon, and T. Horák, "IoT measuring of UDP-based distributed reflective DoS attack," in *Proc. IEEE 16th Int. Symp. Intell. Syst. Informat. (SISY)*, Subotica, Serbia, Sep. 2018, pp. 000209–000214.

[33] G. C. M. Moura, J. Heidemann, M. Müller, R. de O. Schmidt, and M. Davids, "When the dike breaks: Dissecting DNS defenses during DDoS," in *Proc. Internet Meas. Conf.*, Oct. 2018, pp. 8–21.

[34] B. Al-Duwairi, Z. Al-Qudahy, and M. Govindarasu, "A novel scheme for mitigating botnet-based DDoS attacks," *J. Netw.*, vol. 8, no. 2, p. 297, Feb. 2013. [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.369.3328&rep=rep1&type=pdf#page=37

[35] B. Bouyeddou, F. Harrou, Y. Sun, and B. Kadri, "Detecting SYN flood attacks via statistical monitoring charts: A comparative study," in *Proc. 5th Int. Conf. Electr. Eng. Boumerdes (ICEE-B)*, Boumerdes, Algeria, Oct. 2017, pp. 1–5, doi: 10.1109/ICEE-B.2017.8192118.

[36] M. Dulik, "Network attack using TCP protocol for performing DoS and DDoS attacks," in *Proc. Commun. Inf. Technol. (KIT)*, Vysoke Tatry, Slovakia, Oct. 2019, pp. 1–6.

[37] Z. Mašetić, D. Kečo, N. Doğru, and K. Hajdarević, "SYN flood attack detection in cloud computing using support vector machine," *TEM J.*, vol. 6, pp. 752–759 Nov. 2017.

[38] A. Koay, A. Chen, I. Welch, and W. K. G. Seah, "A new multi classifier system using entropy-based features in DDoS attack detection," in *Proc. Int. Conf. Inf. Netw. (ICOIN)*, Chiang Mai, Thailand, Jan. 2018, pp. 162–167, doi: 10.1109/ICOIN.2018.8343104.

[39] N. Bindra and S. Manu, "Detecting DDoS attacks using machine learning techniques and contemporary intrusion detection dataset," *Autom. Control Comput. Sci.*, vol. 53, pp. 419–428, Sep. 2019.

[40] X. Yuan, C. Li, and X. Li, "DeepDefense: Identifying DDoS attack via deep learning," in *Proc. IEEE Int. Conf. Smart Comput. (SMARTCOMP)*, Hong Kong, May 2017, pp. 1–8.

[41] M. Furdek and C. Natalino, "Machine learning for optical network security management," in *Proc. Opt. Fiber Commun. Conf. (OFC)*, San Diego, CA, USA, 2020, pp. 1–3.

[42] A. Dey, "Machine learning algorithms: A review," *Int. J. Comput. Sci. Inf. Technol.*, vol. 7, no. 3, pp. 1174–1179, 2016.

[43] S. Sen, K. D. Gupta, and M. Ahsan, "Leveraging machine learning approach to setup software-defined network(SDN) controller rules during DDoS attack," in *Proc. Int. Joint Conf. Comput. Intell.*, 2020, pp. 49–60.

[44] K. K. Mak, K. Lee, and C. Park, "Applications of machine learning in addiction studies: A systematic review," *Psychiatry Res.*, vol. 275, pp. 53–60, May 2019.

[45] Y. Gu, K. Li, Z. Guo, and Y. Wang, "Semi-supervised K-means DDoS detection method using hybrid feature selection algorithm," *IEEE Access*, vol. 7, pp. 64351–64365, 2019, doi: 10.1109/ACCESS.2019.2917532.

[46] T. Sakai, M. C. Plessis, G. Niu, and M. Sugiyama, "Semi-supervised classification based on classification from positive and unlabeled data," 2016, *arXiv:1605.06955*. [Online]. Available: http://arxiv.org/abs/1605.06955

[47] A. Mehnaz and K. S. Shreedhara, "Performance analysis of semi-supervised machine learning approach for DDoS detection," *Int. J. Innov. Res. Technol.*, vol. 6, no. 2, pp. 3193–3208, Jul. 2019.

[48] N. Zhang, F. Jaafar, and Y. Malik, "Low-rate DoS attack detection using PSD based entropy and machine learning," in *Proc. 6th IEEE Int. Conf. Cyber Secur. Cloud Comput. (CSCloud), 5th IEEE Int. Conf. Edge Comput. Scalable Cloud (EdgeCom)*, Paris, France, Jun. 2019, pp. 59–62, doi: 10.1109/CSCloud/EdgeCom.2019.00020.

[49] F. S. L. Filho, F. A. F. Silveira, A. de Medeiros Brito, Jr., G. Vargas-Solar, and L. F. Silveira, "Smart detection: An online approach for DoS/DDoS attack detection using machine learning," *Secur. Commun. Netw.*, vol. 2019, Oct. 2019, Art. no. 1574749.

[50] I. Sofi, A. Mahajan, and V. Mansotra, "Machine learning techniques used for the detection and analysis of modern types of ddos attacks," *Int. Res. J. Eng. Technol.*, vol. 4, no. 6, pp. 1085–1093, 2017.

[51] B. S. K. Devi, G. Preetha, G. Selvaram, and S. M. Shalinie, "An impact analysis: Real time DDoS attack detection and mitigation using machine learning," in *Proc. Int. Conf. Recent Trends Inf. Technol.*, Chennai, India, Apr. 2014, pp. 1–7.

[52] S. Das, A. M. Mahfouz, D. Venugopal, and S. Shiva, "DDoS intrusion detection through machine learning ensemble," in *Proc. IEEE 19th Int. Conf. Softw. Qual., Rel. Secur. Companion (QRS-C)*, Sofia, Bulgaria, Jul. 2019, pp. 471–477.

[53] Z. Liu, X. Yin, and Y. Hu, "CPSS LR-DDoS detection and defense in edge computing utilizing DCNN Q-Learning," *IEEE Access*, vol. 8, pp. 42120–42130, 2020.

[54] T. Alharbi, A. Aljuhani, and H. Liu, "Holistic DDoS mitigation using NFV," in *Proc. IEEE 7th Annu. Comput. Commun. Workshop Conf. (CCWC)*, Las Vegas, NV, USA, Jan. 2017, pp. 1–4, doi: 10.1109/CCWC.2017.7868480.

[55] T. Alharbi, A. Aljuhani, H. Liu, and C. Hu, "Smart and lightweight DDoS detection using NFV," in *Proc. Int. Conf. Compute Data Anal. (ICCDA)*, Lakeland, FL, USA, 2017, pp. 220–227.

[56] W. Wang, X. Du, and N. Wang, "Building a cloud IDS using an efficient feature selection method and SVM," *IEEE Access*, vol. 7, pp. 1345–1354, 2019.

[57] P. Gupta, A. Seetharaman, and J. R. Raj, "The usage and adoption of cloud computing by small and medium businesses," *Int. J. Inf. Manage.*, vol. 33, no. 5, pp. 861–874, Oct. 2013.

[58] O. A. Wahab, J. Bentahar, H. Otrok, and A. Mourad, "Optimal load distribution for the detection of VM-based DDoS attacks in the cloud," *IEEE Trans. Services Comput.*, vol. 13, no. 1, pp. 114–129, Feb. 2020, doi: 10.1109/TSC.2017.2694426.

[59] K. Gurulakshmi and A. Nesarani, "Analysis of IoT bots against DDOS attack using machine learning algorithm," in *Proc. 2nd Int. Conf. Trends Electron. Informat. (ICOEI)*, Tirunelveli, India, May 2018, pp. 1052–1057.

[60] A. R. Wani, Q. P. Rana, U. Saxena, and N. Pandey, "Analysis and detection of DDoS attacks on cloud computing environment using machine learning techniques," in *Proc. Amity Int. Conf. Artif. Intell. (AICAI)*, Dubai, United Arab Emirates, Feb. 2019, pp. 870–875.

[61] M. Zekri, S. E. Kafhali, N. Aboutabit, and Y. Saadi, "DDoS attack detection using machine learning techniques in cloud computing environments," in *Proc. 3rd Int. Conf. Cloud Comput. Technol. Appl. (CloudTech)*, Rabat, Morocco, Oct. 2017, pp. 1–7.

[62] Z. He, T. Zhang, and R. B. Lee, "Machine learning based DDoS attack detection from source side in cloud," in *Proc. IEEE 4th Int. Conf. Cyber Secur. Cloud Comput. (CSCloud)*, New York, NY, USA, Jun. 2017, pp. 114–120.

[63] P. Rivas, C. DeCusatis, M. Oakley, A. Antaki, N. Blaskey, S. LaFalce, and S. Stone, "Machine learning for DDoS attack classification using hive plots," in *Proc. IEEE 10th Annu. Ubiquitous Comput., Electron. Mobile Commun. Conf. (UEMCON)*, New York, NY, USA, Oct. 2019, pp. 0401–0407.

[64] A. Rukavitsyn, K. Borisenko, and A. Shorov, "Self-learning method for DDoS detection model in cloud computing," in *Proc. IEEE Conf. Russian Young Researchers Electr. Electron. Eng. (EIConRus)*, St. Petersburg, Russia, Feb. 2017, pp. 544–547.

[65] C. Xu, H. Lin, Y. Wu, X. Guo, and W. Lin, "An SDNFV-based DDoS defense technology for smart cities," *IEEE Access*, vol. 7, pp. 137856–137874, 2019.

[66] B. Mladenov, "Studying the DDoS attack effect over SDN controller southbound channel," in *Proc. 10th Nat. Conf. Int. Participation (ELECTRONICA)*, Sofia, Bulgaria, May 2019, pp. 1–4.

[67] S. Dong and M. Sarem, "DDoS attack detection method based on improved KNN with the degree of DDoS attack in software-defined networks," *IEEE Access*, vol. 8, pp. 5039–5048, 2020.

[68] W. Sun, Y. Li, and S. Guan, "An improved method of DDoS attack detection for controller of SDN," in *Proc. IEEE 2nd Int. Conf. Comput. Commun. Eng. Technol. (CCET)*, Beijing, China, Aug. 2019, pp. 249–253.

[69] Z. A. El Houda, A. S. Hafid, and L. Khoukhi, "Cochain-SC: An intra- and inter-domain DDoS mitigation scheme based on blockchain using SDN and smart contract," *IEEE Access*, vol. 7, pp. 98893–98907, 2019.

[70] Z. Liu, Y. He, W. Wang, and B. Zhang, "DDoS attack detection scheme based on entropy and PSO-BP neural network in SDN," *China Commun.*, vol. 16, no. 7, pp. 144–155, Jul. 2019.

[71] L. Yang and H. Zhao, "DDoS attack identification and defense using SDN based on machine learning method," in *Proc. 15th Int. Symp. Pervas. Syst., Algorithms Netw. (I-SPAN)*, Yichang, China, Oct. 2018, pp. 174–178.

[72] O. Rahman, M. A. G. Quraishi, and C.-H. Lung, "DDoS attacks detection and mitigation in SDN using machine learning," in *Proc. IEEE World Congr. Services (SERVICES)*, Milan, Italy, Jul. 2019, pp. 184–189.

[73] V. Deepa, K. M. Sudar, and P. Deepalakshmi, "Design of ensemble learning methods for DDoS detection in SDN environment," in *Proc. Int. Conf. Vis. Towards Emerg. Trends Commun. Netw. (ViTECoN)*, Vellore, India, Mar. 2019, pp. 1–6.

[74] V. Deepa, K. M. Sudar, and P. Deepalakshmi, "Detection of DDoS attack on SDN control plane using hybrid machine learning techniques," in *Proc. Int. Conf. Smart Syst. Inventive Technol. (ICSSIT)*, Tirunelveli, India, Dec. 2018, pp. 299–303.

[75] W. Zhijun, X. Qing, W. Jingjie, Y. Meng, and L. Liang, "Low-rate DDoS attack detection based on factorization machine in software defined network," *IEEE Access*, vol. 8, pp. 17404–17418, 2020.

[76] T.-M. Nguyen, M. Minoux, and S. Fdida, "Optimizing resource utilization in NFV dynamic systems: New exact and heuristic approaches," *Comput. Netw.*, vol. 148, pp. 129–141, Jan. 2019.

[77] A. Aljuhani and T. Alharbi, "Virtualized network functions security attacks and vulnerabilities," in *Proc. IEEE 7th Annu. Comput. Commun. Workshop Conf. (CCWC)*, Las Vegas, NV, USA, Jan. 2017, pp. 1–4, doi: 10.1109/CCWC.2017.7868478.

[78] L. Fang, X. Zhang, K. Sood, Y. Wang, and S. Yu, "Reliability-aware virtual network function placement in carrier networks," *J. Netw. Comput. Appl.*, vol. 154, Mar. 2020, Art. no. 102536. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1084804520300102?casa_token=xYGQ_Kkam8QAAAAA:RzitZTCUjL0uIkJqbc4RaGE0E8YlqhRIkdW6OvdLdv7YXzf7r1LHhCrKEUGiEApXEnK15A

[79] E. Hernandez-Valencia, S. Izzo, and B. Polonsky, "How will NFV/SDN transform service provider opex?" *IEEE Netw.*, vol. 29, no. 3, pp. 60–67, May 2015, doi: 10.1109/MNET.2015.7113227.

[80] L. Zhou and H. Guo, "Applying NFV/SDN in mitigating DDoS attacks," in *Proc. IEEE Region Conf. (TENCON)*, Penang, Malaysia, Nov. 2017, pp. 2061–2066.

[81] I. H. Abdulqadder, D. Zou, I. T. Aziz, and B. Yuan, "Enhanced attack aware security provisioning scheme in SDN/NFV enabled over 5G network," in *Proc. 27th Int. Conf. Comput. Commun. Netw. (ICCCN)*, Hangzhou, China, Jul. 2018, pp. 1–9.

[82] A. Kalliola, S. Lal, K. Ahola, I. Oliver, Y. Miche, and S. Holtmanns, "Testbed for security orchestration in a network function virtualization environment," in *Proc. IEEE Conf. Netw. Function Virtualization Softw. Defined Netw. (NFV-SDN)*, Berlin, Germany, Nov. 2017, pp. 1–4.

[83] A. Aljuhani, T. Alharbi, and B. Taylor, "Mitigation of application layer DDoS flood attack against Web servers," *J. Inf. Secur. Cybercrimes Res.*, vol. 2, no. 1, pp. 1–13, 2019, doi: 10.26735/16587790.2019.002.

[84] T. Alharbi, A. Aljuhani, and B. Taylor, "A collaborative SYN flooding detection ApproachA collaborative SYN," *Int. J. Comput. Eng. Inf. Technol.* vol. 11, no. 9, pp. 186–196, 2019.

[85] A. Aljuhani, T. Alharbi, and H. Liu, "XFirewall: A dynamic and additional mitigation against DDoS storm," in *Proc. Int. Conf. Compute Data Anal. (ICCDA)*, 2017, pp. 1–5.

[86] T. V. Phan and M. Park, "Efficient distributed denial-of-service attack defense in SDN-based cloud," *IEEE Access*, vol. 7, pp. 18701–18714, 2019.

[87] S. Janarthanam, N. Prakash, and M. Shanthakumar, "Adaptive learning method for DDoS attacks on software defined network function virtualization," *EAI Endorsed Trans. Cloud Syst.*, vol. 6, no. 18, Sep. 2020, Art. no. 166286.

[88] F. Li, K.-Y. Lam, L. Meng, H. Luo, and L. Wang, "Trading-based dynamic spectrum access and allocation in cognitive Internet of Things," *IEEE Access*, vol. 7, pp. 125952–125959, 2019, doi: 10.1109/ACCESS.2019.2937582.

[89] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, "Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on Internet-scale IoT exploitations," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2702–2733, 3rd Quart., 2019, doi: 10.1109/COMST.2019.2910750.

[90] M. A. M. Sadeeq, S. R. M. Zeebaree, R. Qashi, S. H. Ahmed, and K. Jacksi, "Internet of Things security: A survey," in *Proc. Int. Conf. Adv. Sci. Eng. (ICOASE)*, 2018, pp. 162–166.

[91] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on IoT security: Application areas, security threats, and solution architectures," *IEEE Access*, vol. 7, pp. 82721–82743, 2019.

[92] M. U. Farooq, M. Waseem, A. Khairi, and S. Mazhar, "A critical analysis on the security concerns of Internet of Things (IoT)," *Int. J. Comput. Appl.*, vol. 111, no. 7, pp. 1–6, Feb. 2015.

[93] C. Zhang and R. Green, "Communication security in Internet of Thing: Preventive measure and avoid DDoS attack over IoT network," in *Proc. 18th Symp. Commun. Netw. (CNS)*. San Diego, CA, USA: Society for Computer Simulation International, 2015, pp. 8–15.

[94] M. Roopak, G. Y. Tian, and J. Chambers, "Deep learning models for cyber security in IoT networks," in *Proc. IEEE 9th Annu. Comput. Commun. Workshop Conf. (CCWC)*, Las Vegas, NV, USA, Jan. 2019, pp. 0452–0457, doi: 10.1109/CCWC.2019.8666588.

[95] Y. N. Soe, P. I. Santosa, and R. Hartanto, "DDoS attack detection based on simple ANN with SMOTE for IoT environment," in *Proc. 4th Int. Conf. Informat. Comput. (ICIC)*, Semarang, Indonesia, Oct. 2019, pp. 1–5, doi: 10.1109/ICIC47613.2019.8985853.

[96] N. Ravi and S. M. Shalinie, "Learning-driven detection and mitigation of DDoS attack in IoT via SDN-cloud architecture," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 3559–3570, Apr. 2020, doi: 10.1109/JIOT.2020.2973176.

[97] M. Roopak, G. Y. Tian, and J. Chambers, "An intrusion detection system against DDoS attacks in IoT networks," in *Proc. 10th Annu. Comput. Commun. Workshop Conf. (CCWC)*, Las Vegas, NV, USA, Jan. 2020, pp. 0562–0567, doi: 10.1109/CCWC47524.2020.9031206.

[98] Z. Li, L. Wei, W. Li, L. Wei, M. Chen, M. Lv, X. Zhi, C. Wang, and N. Gao, "Research on DDoS attack detection based on ELM in IoT environment," in *Proc. IEEE 10th Int. Conf. Softw. Eng. Service Sci. (ICSESS)*, Beijing, China, Oct. 2019, pp. 144–148, doi: 10.1109/ICSESS47205.2019.9040855.

[99] Y. Meidan, M. Bohadana, Y. Mathov, Y. Mirsky, A. Shabtai, D. Breitenbacher, and Y. Elovici, "N-BaIoT—Network-based detection of IoT botnet attacks using deep autoencoders," *IEEE Pervas. Comput.*, vol. 17, no. 3, pp. 12–22, Jul. 2018, doi: 10.1109/MPRV.2018.03367731.

[100] J. Su, D. V. Vasconcellos, S. Prasad, D. Sgandurra, Y. Feng, and K. Sakurai, "Lightweight classification of IoT malware based on image recognition," in *Proc. IEEE 42nd Annu. Comput. Softw. Appl. Conf. (COMPSAC)*, Tokyo, Japan, Jul. 2018, pp. 664–669, doi: 10.1109/COMPSAC.2018.10315.

[101] C. D. McDermott, F. Majdani, and A. V. Petrovski, "Botnet detection in the Internet of Things using deep learning approaches," in *Proc. Int. Joint Conf. Neural Netw. (IJCNN)*, Rio de Janeiro, Brazil, Jul. 2018, pp. 1–8, doi: 10.1109/IJCNN.2018.8489489.

[102] S. Alzahrani and L. Hong, "Generation of DDoS attack dataset for effective IDS development and evaluation," *J. Inf. Secur.*, vol. 9, no. 04, p. 225, 2018.

[103] S. Behal and K. Kumar, "Trends in validation of DDoS research," *Procedia Comput. Sci.*, vol. 85, pp. 7–15, May 2016.

[104] S. Yu, W. Zhou, W. Jia, S. Guo, Y. Xiang, and F. Tang, "Discriminating DDoS attacks from flash crowds using flow correlation coefficient," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 6, pp. 1073–1080, Jun. 2012.

[105] D. Drinfeld and N. Vlajic, "Smart crawlers for flash-crowd DDoS: The attacker's perspective," in *Proc. World Congr. Internet Secur. (WorldCIS)*, Guelph, ON, Canada, 2012, pp. 37–44.

[106] T. Alharbi, A. Aljuhani, H. Liu, and C. Hu, "Smart and lightweight DDoS detection using NFV," in *Proc. Int. Conf. Compute Data Anal. (ICCDA)*, May 2017, pp. 220–227.

[107] K. Angrishi, "Turning Internet of Things(IoT) into Internet of vulnerabilities (IoV): IoT botnets," 2017, *arXiv:1702.03681*. [Online]. Available: http://arxiv.org/abs/1702.03681

[108] O. Osanaiye, K.-K.-R. Choo, and M. Dlodlo, "Distributed denial of service (DDoS) resilience in cloud: Review and conceptual cloud DDoS mitigation framework," *J. Netw. Comput. Appl.*, vol. 67, pp. 147–165, May 2016.

[109] O. Kupreev, E. Badovskaya, and A. Gutnikov. (May 21, 2019). *DDoS Attacks in Q1 2019*. [Online]. Available: https://securelist.com/ddos-report-q1-2019/90792/

[110] M. M. Salim, S. Rathore, and J. H. Park, "Distributed denial of service attacks and its defenses in IoT: A survey," *J. Supercomput.*, vol. 76, no. 7, pp. 5320–5363, Jul. 2020, doi: 10.1007/s11227-019-02945-z.

[111] D. Chaudhary, K. Bhushan, and B. B. Gupta, "Survey on DDoS attacks and defense mechanisms in cloud and fog computing," *Int. J. E-Services Mobile Appl.*, vol. 10, no. 3, pp. 61–83, Jul. 2018.

[112] B. Nugraha and R. N. Murthy, "Deep learning-based slow DDoS attack detection in SDN-based networks," in *Proc. IEEE Conf. Netw. Function Virtualization Softw. Defined Netw. (NFV-SDN)*, Leganes, Spain, Nov. 2020, pp. 51–56, doi: 10.1109/NFV-SDN50289.2020.9289894.

[113] M. Guarino, P. Rivas, and C. DeCusatis, "Towards adversarially robust DDoS-attack classification," in *Proc. 11th IEEE Annu. Ubiquitous Comput., Electron. Mobile Commun. Conf. (UEMCON)*, New York, NY, USA, Oct. 2020, pp. 0285–0291, doi: 10.1109/UEMCON51285.2020.9298167.

[114] A. Alsirhani, S. Sampalli, and P. Bodorik, "DDoS detection system: Using a set of classification algorithms controlled by fuzzy logic system in Apache spark," *IEEE Trans. Netw. Service Manage.*, vol. 16, no. 3, pp. 936–949, Sep. 2019, doi: 10.1109/TNSM.2019.2929425.

[115] M. S. Khaing, Y. M. Thant, T. Tun, C. S. Htwe, and M. M. S. Thwin, "IoT botnet detection mechanism based on UDP protocol," in *Proc. IEEE Conf. Comput. Appl. (ICCA)*, Yangon, Myanmar, Feb. 2020, pp. 1–7, doi: 10.1109/ICCA49400.2020.9022832.

[116] M. Zhang, G. Li, S. Wang, C. Liu, A. Chen, H. Hu, G. Gu, Q. Li, M. Xu, and J. Wu, "Poseidon: Mitigating volumetric DDoS attacks with programmable switches," in *Proc. Netw. Distrib. Syst. Secur. Symp.*, 2020, pp. 1–8. [Online]. Available: https://bit.ly/2vZviRE

[117] M. Aldaoud, D. Al-Abri, A. Al Maashri, and F. Kausar, "DHCP attacking tools: An analysis," *J. Comput. Virol. Hacking Techn.*, pp. 1–11, Jan. 2021, doi: 10.1007/s11416-020-00374-8.

[118] R. Chalapathy and S. Chawla, "Deep learning for anomaly detection: A survey," 2019, *arXiv:1901.03407*. [Online]. Available: http://arxiv.org/abs/1901.03407

[119] M. Ali Al-Garadi, A. Mohamed, A. Al-Ali, X. Du, and M. Guizani, "A survey of machine and deep learning methods for Internet of Things (IoT) security," 2018, *arXiv:1807.11023*. [Online]. Available: http://arxiv.org/abs/1807.11023

[120] R. Priyadarshini and R. K. Barik, "A deep learning based intelligent framework to mitigate DDoS attack in fog environment," *J. King Saud Univ. Comput. Inf. Sci.*, pp. 1–7, Apr. 2019, doi: 10.1016/j.jksuci.2019.04.010.

[121] S. Çakmakçı, T. Kemmerich, T. Ahmed, and N. Baykal, "Online DDoS attack detection using Mahalanobis distance and Kernel-based learning algorithm," *J. Netw. Comput. Appl.*, vol. 168, Oct. 2020, pp. 1–14, doi: 10.1016/j.jnca.2020.102756.

[122] K. B. Virupakshar, M. Asundi, K. Channal, P. Shettar, S. Patil, and D. G. Narayan, "Distributed denial of service (DDoS) attacks detection system for OpenStack-based private cloud," *Procedia Comput. Sci.*, vol. 167, pp. 2297–2307, Jan. 2020.

[123] S. Gumaste and S. Shinde, "Detection of DDoS attacks in OpenStack-based private cloud using Apache spark," *J. Telecommun. Inf. Technol.*, vol. 4, pp. 62–71, Jan. 2021, doi: 10.26636/jtit.2020.146120.

[124] M. M. Oo, S. Kamolphiwong, T. Kamolphiwong, and S. Vasupongayya, "Advanced support vector machine-(ASVM-) based detection for distributed denial of service (DDoS) attack on software defined networking (SDN)," *J. Comput. Netw. Commun.*, vol. 2019, pp. 1–12, Mar. 2019.

[125] N. N. Tuan, P. H. Hung, N. D. Nghia, N. V. Tho, T. V. Phan, and N. H. Thanh, "A DDoS attack mitigation scheme in ISP networks using machine learning based on SDN," *Electronics*, vol. 9, no. 3, p. 413, Feb. 2020.

[126] A. B. Dehkordi, M. Soltanaghaei, and F. Z. Boroujeni, "The DDoS attacks detection through machine learning and statistical methods in SDN," *J. Supercomput.*, vol. 77, pp. 1–33, Jun. 2020, doi: 10.1007/s11227-020-03323-w.

[127] K. S. Sahoo, B. K. Tripathy, K. Naik, S. Ramasubbareddy, B. Balusamy, M. Khari, and D. Burgos, "An evolutionary SVM model for DDOS attack detection in software defined networks," *IEEE Access*, vol. 8, pp. 132502–132513, 2020.

[128] B. V. Karan, D. G. Narayan, and P. S. Hiremath, "Detection of DDoS attacks in software defined networks," in *Proc. 3rd Int. Conf. Comput. Syst. Inf. Technol. Sustain. Solutions (CSITSS)*, Dec. 2018, pp. 265–270.

[129] G. De La Torre Parra, P. Rad, K.-K.-R. Choo, and N. Beebe, "Detecting Internet of Things attacks using distributed deep learning," *J. Netw. Comput. Appl.*, vol. 163, Aug. 2020, Art. no. 102662.

[130] L. Ma, Y. Chai, L. Cui, D. Ma, Y. Fu, and A. Xiao, "A deep learning-based DDoS detection framework for Internet of Things," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Dublin, Ireland, Jun. 2020, pp. 1–6, doi: 10.1109/ICC40277.2020.9148944.

[131] B. Jia, X. Huang, R. Liu, and Y. Ma, "A DDoS attack detection method based on hybrid heterogeneous multiclassifier ensemble learning," *J. Electr. Comput. Eng.*, vol. 2017, pp. 1–9, Mar. 2017.

[132] T. Chin, X. Mountrouidou, X. Li, and K. Xiong, "Selective packet inspection to detect DoS flooding using software defined networking (SDN)," in *Proc. IEEE 35th Int. Conf. Distrib. Comput. Syst. Workshops*, Columbus, OH, USA, Jul. 2015, pp. 95–99, doi: 10.1109/ICDCSW.2015.27.

[133] R. Sahay, G. Blanc, Z. Zhang, and H. Debar, "ArOMA: An SDN based autonomic DDoS mitigation framework," *Comput. Secur.*, vol. 70, pp. 482–499, Sep. 2017.

[134] S. C. Tsai, I. H. Liu, C. T. Lu, C. H. Chang, and J. S. Li, "Defending cloud computing environment against the challenge of DDoS attacks based on software defined network," in *Proc. Adv. Intell. Inf. Hiding Multimedia Signal Process.* Cham, Switzerland: Springer, 2017, pp. 285–292.

[135] J. Singh and S. Behal, "Detection and mitigation of DDoS attacks in SDN: A comprehensive review, research challenges and future directions," *Comput. Sci. Rev.*, vol. 37, pp. 1–25, Jun. 2020, doi: 10.1016/j.cosrev.2020.100279.

[136] C.-J. Chung, P. Khatkar, T. Xing, J. Lee, and D. Huang, "NICE: Network intrusion detection and countermeasure selection in virtual network systems," *IEEE Trans. Dependable Secure Comput.*, vol. 10, no. 4, pp. 198–211, Aug. 2013, doi: 10.1109/TDSC.2013.8.

[137] S. Lim, J. Ha, H. Kim, Y. Kim, and S. Yang, "A SDN-oriented DDoS blocking scheme for botnet-based attacks," in *Proc. 6th Int. Conf. Ubiquitous Future Netw. (ICUFN)*, Shanghai, China, Jul. 2014, pp. 63–68, doi: 10.1109/ICUFN.2014.6876752.

[138] W. Chen, S. Xiao, L. Liu, X. Jiang, and Z. Tang, "A DDoS attacks traceback scheme for SDN-based smart city," *Comput. Electr. Eng.*, vol. 81, pp. 1–12, Nov. 2019, doi: 10.1016/j.compeleceng.2019.106503.

[139] M.-H. Yang, J.-N. Luo, M. Vijayalakshmi, and S. M. Shalinie, "Hybrid multilayer network traceback to the real sources of attack devices," *IEEE Access*, vol. 8, pp. 201087–201097, 2020, doi: 10.1109/ACCESS.2020.3034226.

[140] A. Ahalawat, S. S. Dash, A. Panda, and K. S. Babu, "Entropy based DDoS detection and mitigation in OpenFlow enabled SDN," in *Proc. Int. Conf. Vis. Towards Emerg. Trends Commun. Netw. (ViTECoN)*, Vellore, India, Mar. 2019, pp. 1–5, doi: 10.1109/ViTECoN.2019.8899721.

[141] G. Dayanandam, T. V. Rao, D. B. Babu, and S. N. Durga, "DDoS attacks—Analysis and prevention," in *Innovations in Computer Science and Engineering*. Singapore: Springer, May 2018, pp. 1–10, doi: 10.1007/978-981-10-8201-6_1.

[142] A. H. M. Jakaria, W. Yang, B. Rashidi, C. Fung, and M. A. Rahman, "VFence: A defense against distributed denial of service attacks using network function virtualization," in *Proc. IEEE 40th Annu. Comput. Softw. Appl. Conf. (COMPSAC)*, Atlanta, GA, USA, Jun. 2016, pp. 431–436, doi: 10.1109/COMPSAC.2016.219.

[143] C. J. Fung and B. McCormick, "VGuard: A distributed denial of service attack mitigation method using network function virtualization," in *Proc. 11th Int. Conf. Netw. Service Manage. (CNSM)*, Barcelona, Spain, Nov. 2015, pp. 64–70, doi: 10.1109/CNSM.2015.7367340.

[144] V. F. Garcia, G. de Freitas Gaiardo, L. da Cruz Marcuzzo, R. C. Nunes, and C. R. P. dos Santos, "DeMONS: A DDoS mitigation NFV solution," in *Proc. IEEE 32nd Int. Conf. Adv. Inf. Netw. Appl. (AINA)*, Krakow, Poland, May 2018, pp. 769–776, doi: 10.1109/AINA.2018.00115.

[145] B. Rashidi, C. Fung, and E. Bertino, "A collaborative DDoS defence framework using network function virtualization," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 10, pp. 2483–2497, Oct. 2017, doi: 10.1109/TIFS.2017.2708693.

[146] T. Lukaseder, S. Ghosh, and F. Kargl, "Mitigation of flooding and slow DDoS attacks in a software-defined network," 2018, *arXiv:1808.05357*. [Online]. Available: http://arxiv.org/abs/1808.05357

[147] S. Hameed and U. Ali, "HADEC: Hadoop-based live DDoS detection framework," *EURASIP J. Inf. Secur.*, vol. 2018, no. 1, pp. 1–19, Dec. 2018, doi: 10.1186/s13635-018-0081-z.

[148] S. Tripathi, B. Gupta, A. Almomani, A. Mishra, and S. Veluru, "Hadoop based defense solution to handle distributed denial of service (DDoS) attacks," *J. Inf. Secur.*, vol. 4, no. 3, pp. 150–164, 2013.

[149] S. Hameed and U. Ali, "Efficacy of live DDoS detection with Hadoop," in *Proc. IEEE/IFIP Netw. Oper. Manage. Symp.*, Istanbul, Turkey, Apr. 2016, pp. 488–494, doi: 10.1109/NOMS.2016.7502848.

[150] B. Zhang, T. Zhang, and Z. Yu, "DDoS detection and prevention based on artificial intelligence techniques," in *Proc. 3rd IEEE Int. Conf. Comput. Commun. (ICCC)*, Chengdu, China, Dec. 2017, pp. 1276–1280, doi: 10.1109/CompComm.2017.8322748.

[151] Q. Yan, W. Huang, X. Luo, Q. Gong, and F. R. Yu, "A multi-level DDoS mitigation framework for the industrial Internet of Things," *IEEE Commun. Mag.*, vol. 56, no. 2, pp. 30–36, Feb. 2018, doi: 10.1109/MCOM.2018.1700621.

[152] A. Alsirhani, S. Sampalli, and P. Bodorik, "DDoS detection system: Utilizing gradient boosting algorithm and Apache spark," in *Proc. IEEE Can. Conf. Electr. Comput. Eng. (CCECE)*, Quebec City, QC, Canada, May 2018, pp. 1–6, doi: 10.1109/CCECE.2018.8447671.

[153] L. Chen, Y. Zhang, Q. Zhao, G. Geng, and Z. Yan, "Detection of DNS DDoS attacks with random forest algorithm on spark," *Procedia Comput. Sci.*, vol. 134, pp. 310–315, Jan. 2018.

[154] N. V. Patil, C. R. Krishna, and K. Kumar, "S-DDoS: Apache spark based real-time DDoS detection system," *J. Intell. Fuzzy Syst.*, vol. 38, no. 5, pp. 1–9, 2020.

[155] B. Zhou, J. Li, Y. Ji, and M. Guizani, "Online Internet traffic monitoring and DDoS attack detection using big data frameworks," in *Proc. 14th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Limassol, Cyprus, Jun. 2018, pp. 1507–1512, doi: 10.1109/IWCMC.2018.8450335.

[156] S. Tang, B. He, C. Yu, Y. Li, and K. Li, "A survey on spark ecosystem: Big data processing infrastructure, machine learning, and applications," *IEEE Trans. Knowl. Data Eng.*, early access, Feb. 24, 2020, doi: 10.1109/TKDE.2020.2975652.

[157] R. Swami, M. Dave, and V. Ranga, "Software-defined networking-based DDoS defense mechanisms," *ACM Comput. Surv.*, vol. 52, no. 2, 2019, Art. no. 28.

[158] M. Arafat, F. Ahmed, and M. Sobhan, "SIP security in IP telephony," in *Proc. Int. Conf. Elastix World Mexico*, Oct. 2013, pp. 1–11.

[159] M. M. Alam, M. Y. Arafat, and F. Ahmed, "Study on auto detecting defence mechanisms against application layer DDoS attacks in SIP server," *J. Netw.*, vol. 10, no. 6, p. 344, Jun. 2015.

[160] M. Y. Arafat, M. M. Alam, and F. Ahmed, "A realistic approach and mitigation techniques for amplifying DDOS attack on DNS," in *Proc. 10th Global Eng., Sci. Technol. Conf.*, Dhaka, Bangladesh, Jan. 2015, pp. 2–3.

[161] M. Y. Arafat, M. M. Alam, and F. Ahmed, "Study on security issue in open source SIP server," *Mod. Appl. Sci.*, vol. 8, no. 2, p. 124, Mar. 2014, doi: 10.5539/mas.v8n2p124.

[162] R. Doshi, N. Apthorpe, and N. Feamster, "Machine learning DDoS detection for consumer Internet of Things devices," in *Proc. IEEE Secur. Privacy Workshops (SPW)*, May 2018, pp. 29–35.

**AHAMED ALJUHANI** received the M.S. degree in computer science from the University of Colorado Denver, Denver, CO, USA, in 2013, and the Ph.D. degree in computer science/information security track from The Catholic University of America, Washington, DC, USA, in 2020. He is currently an Assistant Professor and the Chair of the Department of Computer Engineering, College of Computing and Information Technology, University of Tabuk, Saudi Arabia. He has published a number of articles on topics related to the network security field. His current research interests include information security, network security and privacy, secure system design, and system development.

• • •