Deep Learning for DDoS Attack Detection in IoT: A Survey

Mulualem Bitew Anley, Angelo Genovese(✉), and Vincenzo Piuri

Università degli Studi di Milano, Milano, Italy
{mulualem.anley,angelo.genovese,vincenzo.piuri}@unimi.it

Abstract. The Internet of Things (IoT) is evolving rapidly in many sectors, including personal health, home automation, industrial controls, and smart city infrastructures, with the number of connected devices constantly increasing. However, this growth has also increased the vulnerability space for Distributed Denial of Service (DDoS) attacks, which are becoming more frequent and sophisticated, making it difficult to detect them using conventional methods. To address this issue, machine learning approaches, especially deep learning-based techniques, have emerged as powerful tools for detecting and mitigating DDoS attacks. This paper reviews the state-of-the-art deep learning techniques for detecting DDoS attacks in the IoT. We have analyzed the origin, evolution, and taxonomy of DDoS attacks, benchmark datasets, ongoing research challenges, and future research directions.

Keywords: DDoS Detection · Cyber Security · IoT Security · Deep Learning

1 Introduction

The rise of the Internet of Things (IoT) is bringing ubiquitous connectivity in an increasing number of everyday life situations, ranging from personal health and smart homes to smart cities and industrial systems, with a growing number of connected devices exchanging information with a bandwidth that is constantly increasing. However, the diffusion of IoT-enabled devices is also causing a greater vulnerability of networks to cybersecurity risks, given that such devices often run simple operating systems with limited built-in security mechanisms. In particular, one of the major risks is represented by their vulnerability to Distributed Denial of Service (DDoS) attacks, which require a large number of vulnerable devices, a situation that can often arise with IoT devices. In DDoS attacks, an attacker can take control of such devices and use them to overwhelm target networks with excessive traffic, causing disruptions of services [62]. Reports published by the European Union Agency for Cybersecurity (ENISA) have shown the increasingly sophisticated and expanding threat posed by DDoS attacks, especially considering the proliferation of IoT devices. The reports note the dark web's role in enabling attacks, the emergence of ransom-driven attacks, and the increasing size and complexity of these threats [20].

To mitigate the problem of DDoS, various techniques have been employed to detect, prevent, and counteract the attacks. In particular, it is possible to categorize the techniques for DDoS detection into signature-based and anomaly-based [69], with signature-based detection techniques relying on predefined signatures to identify known attacks, and anomaly-based detection identifying new and unknown attacks by recognizing abnormal patterns using statistical methods or Machine Learning (ML) [31]. Among ML-based approaches, the research community is increasingly considering deep learning (DL) models due to their high classification accuracy and their capability of automatically learning feature representations [36]. DL-based approaches are thus an enabling factor for detection techniques that are both highly accurate and capable of adapting to the evolving threat landscape represented by DDoS attacks that change their nature over time [22]. However, the potential of DL-based DDoS detection is limited by challenges, including the scarcity of labeled data for certain types of attacks and data imbalance. Furthermore, conventional DL models, primarily centralized, face additional privacy-related challenges caused by the need to have training data locally stored. To address these concerns and enhance detection capabilities for novel DDoS attacks, different studies proposed the adoption of advanced DL models incorporating transfer learning [80], few-shot learning [15], federated learning [17,39,84] and adaptive learning [1,10].

This comprehensive survey aims to introduce the origin, evolution, and taxonomies of DDoS in IoT, review the DL-based techniques for detecting DDoS attacks, examine benchmark datasets used to train and evaluate DL models and identify the open research challenges in this domain. The remainder of the paper is structured as follows. Section 2 provides an overview of DDoS attack origin, motivation, evolution, and taxonomy. Section 3 presents the DL-based approaches for DDoS attack detection. Section 4 discusses available benchmark datasets. Section 5 outlines the open research challenges. Finally, Sect. 6 concludes the paper.

2 DDoS Attacks: Origin, Evolution, Taxonomy

This section reviews the definition and evolution of DDoS, the motivation and targets behind the attacks, and their taxonomy.

2.1 DDoS Attack: A Definition

DDoS attacks happen when an attacker takes control of several devices, known as bots or zombies, by covertly infecting them with malware, enabling remote control by the attacker. The attacker, often called the botmaster, creates a botnet under his/her control composed of a large number of such devices, with IoT devices being a preferred target [2,62]. Botnets vary in size from hundreds to millions of devices and are a primary tool for launching DDoS attacks, which consist of overwhelming target servers with excessive traffic, causing service disruptions [27,73].

Recently, the advent of DDoS as a Service (DDoSaaS) has facilitated the rental of botnets for conducting DDoS attacks. This business model, prevalent on the dark web and underground forums, offers customized attack parameters, such as duration and

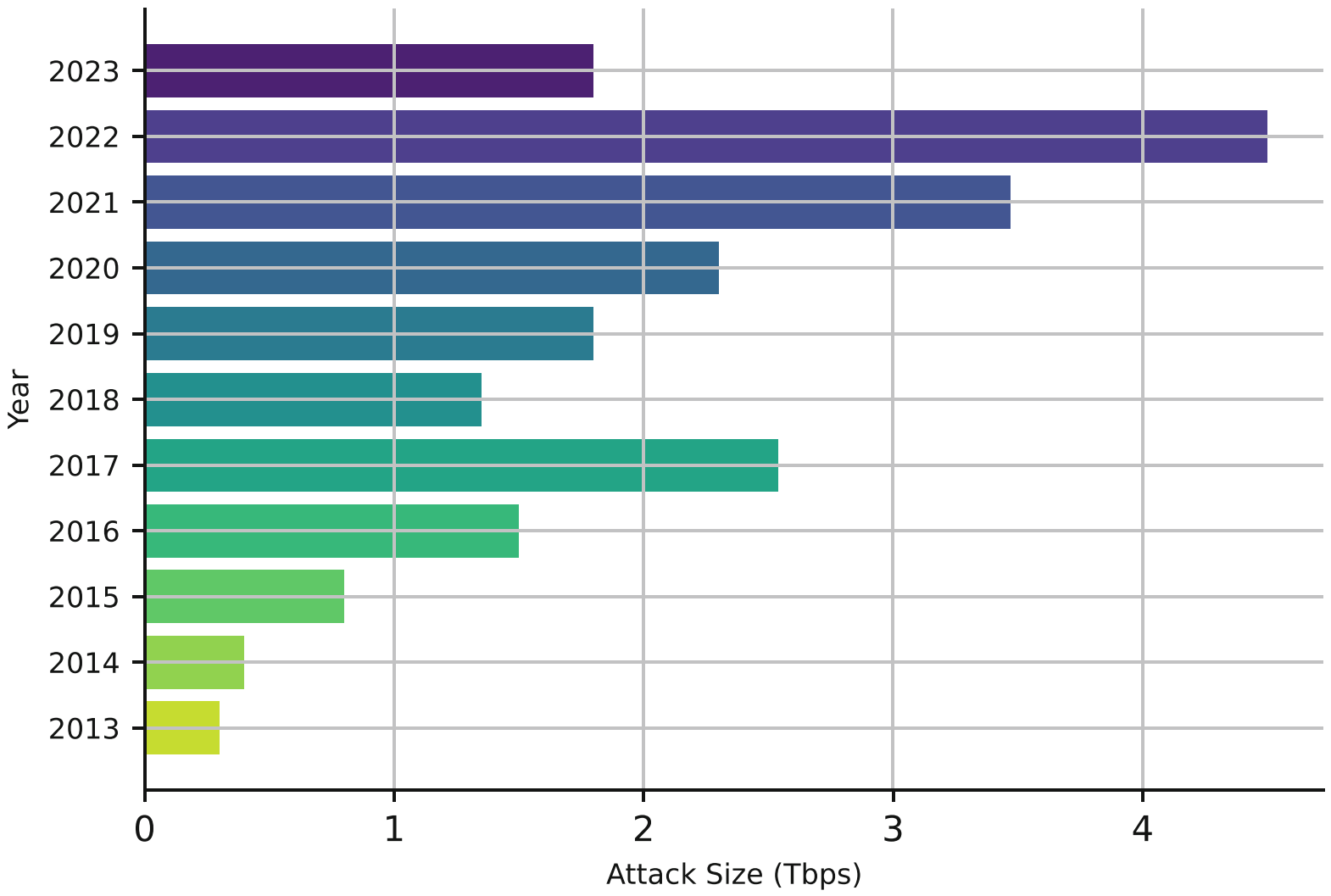

Fig. 1. Horizontal bar chart showing the largest attack sizes in terabits per second (Tbps) from 2013 to 2023. The attack size increases over the years, with 2022 and 2023 having the largest values, both exceeding 4 Tbps.

intensity, against specified targets. Transactions often use cryptocurrencies to maintain anonymity [20]. Moreover, DDoSaaS has significantly lowered the technical barrier for executing DDoS attacks, allowing individuals without extensive technical knowledge to orchestrate severe disruptions against online services and businesses. The convergence of botnets and DDoSaaS, as a consequence, is enhancing the scale, sophistication, and ease of access to DDoS capabilities [2].

2.2 The Evolution of DDoS Attacks

DDoS attacks have evolved significantly since their inception, growing in complexity, scale, and impact. This evolution reflects broader technological advancements and the increasing centrality of the Internet in global infrastructure [52]. Figure 1 illustrates the largest DDoS attacks measured in Tbps annually for the last ten years. The data have been taken from references [9, 11, 14, 19, 23, 32].

The Origins: 1974–2007

– In 1974, the concept of a network-based attack was inadvertently demonstrated by a 13-year-old student who managed to crash a system at the University of Illinois, foreshadowing the potential of network disruptions. The incident involving David Dennis and the PLATO system illustrates an early DoS attack, leveraging a system's limitations to force a shutdown, marking a primary understanding of network vulnerabilities [9].

- In 1988, the Morris Worm infected thousands of computers across the ARPANET, causing significant slowdowns and laying the groundwork for understanding network-based attacks. The Morris Worm represents a pivotal moment in cyber history, exploiting UNIX vulnerabilities to estimate the size of ARPANET [51].
- In 1996, the first documented DDoS attack occurred against Panix, an older Internet Service Provider, which was offline for several days due to a massive SYN Flood attack. However, according to [11], the first DDoS dates back to July 22, 1999, when the University of Minnesota network was suddenly attacked by a botnet of 114 terminals infected with a malicious script called Trin00 and went down in a few minutes.
- In 2000, a high-profile attack by a Canadian teenager known as Mafiaboy targeted major websites like CNN, Yahoo, and eBay, demonstrating the potential for significant economic and reputation damage [54].
- In July 2001, the Code Red Worm, by the time it was discovered on July 19, had already infected approximately 359,000 Microsoft IIS servers and caused billions of dollars in damage. The infected code ran entirely in memory, leaving no traces on permanent storage.
- In January 2003, the SQL Slammer/Sapphire worm spread at an extraordinary speed by exploiting a Microsoft SQL vulnerability. This caused numerous disruptions in many parts of the world and infected, according to estimates, around 75,000 hosts in different geographical areas in less than thirty minutes.
- In 2007, Estonia faced a series of crippling DDoS attacks amidst a diplomatic row with Russia, in what many consider one of the first instances of cyber warfare. Considered one of the first acts of cyber war, this attack simultaneously hit the public administration, the press, and financial institutions of the Estonian nation [9, 32].

Botnets and IoT Vulnerabilities: The 2010 s Until Now

- In 2013, Spamhaus, despite being a well-known non-profit organization with protection services against DDoS attacks, faced a significant attack. The attack, estimated at 300 Gbps, overwhelmed the anti-spam service within minutes, causing multiple disruptions and considerable damage to their reputation [9, 32].
- In 2014, CloudFlare experienced an attack rate estimated at 400 Gbps, which exploited a vulnerability in the widely used NTP protocol [14].
- In 2016, Dyn experienced a significant attack notable for its use of the Mirai botnet. The botnet consisted of more than 600,000 compromised IoT devices. According to some estimates, the attack reached peaks of 1.5 Terabits per second (Tbps), causing Dyn's DNS services to go offline and rendering important sites and applications inaccessible. This included Github, Netflix, Paypal, Airbnb, and more [32].
- In February 2018, Github experienced an attack by exploiting a vulnerability in the Memcached system. The attack generated 1.35 Tbps of traffic for 20 min, bypassing Github's DDoS security systems and obscuring its services.
- In February 2020, AWS experienced a three-day attack with peaks of 2.3 Tbps. The attack exploited an LDAP vulnerability and resulted in significant reputational damage for the cloud giant, although it caused very few disruptions [9, 32].

Table 1. Summary of notable DDoS attacks, attackers' motivation, goals, methods, techniques, targets, disruption levels, and attack size.

Attacked system	Motivation	Goal	Method	Techniques	Target	Resources	Disruption level	Attack Size
Microsoft Azure [8]	Activist	Financial gain	DDoS	Botnet	Web	Network bandwidth	Partial	2.4 Tbps
Poland's railway [24]	Political	Disruption	DoS	Signal spoofing	Railway	Radio–frequency	Total	Unknown
Akamai [67]	Unknown	Unknown	DDoS	Botnet	Web	Network bandwidth	Zero	633.7 Gbps
Killnet (US Hospital) [25]	Political	Revenge	DDoS	Botnet	Web	Network bandwidth	Unknown	Unknown
KA-SAT NETWORK (VIASAT) [20]	Warfare	Disruption	DoS	Exploitation	Satellite	Firmware	Total	Weeks

– In June 2022, Google reported mitigating a 4.5 Tbps HTTP DDoS attack, which is the largest ever recorded at the application layer [23].
– In February 2023, VMWare ESXi experienced a massive ransomware attack globally. On February 4, the CSIRT [11] issued a bulletin stating that the attack exploited a well-known vulnerability (CVE-2021-21974) on VMware ESXi systems. This vulnerability had already been remedied by the virtualization company in February 2021. According to estimates by the US Cyber Security and Infrastructure Security Agency (CISA) and the National Security Agency (NSA), the attack affected more than 3800 servers.

2.3 DDoS: Motivation and Target

The motivations behind DDoS attacks are diverse and complex and can vary widely depending on the attackers' objectives. However, the various goals can be broadly categorized into several macro-areas [83]. Table 1 illustrates some examples of damages to attacked systems, including the attackers' motivations, goals, impacts, methods, and levels of disruption.

Ransom. DDoS which floods a target with traffic is commonly used in ransomware attacks. Attackers may engage in DDoS attacks as part of a ransom scheme, where they demand payment from the victim to cease the attack. This strategy can also involve targeting competitors to disrupt their operations, thereby indirectly boosting the attacker's market share or profits [57].

Ideological or Political Motivations. Attackers motivated by ideological or political reasons often possess a sophisticated technical background, strong convictions, and the support of a well-coordinated group. The latest report from the ENISA on

the DDoS/DoS attacks threat landscape reveals that 66% of DoS attacks have political motivations [20]. The objectives behind such attacks vary widely but are united by their underlying ideological, political, or religious motivations. Notable instances include the 2007 cyber-attacks against Estonia [47].

Cyber Warfare and Espionage. This category predominantly encompasses actions undertaken for political and military objectives, often linked to governmental, military, or institutional bodies. The entities behind such attacks are notably well-coordinated and resourced, possessing the requisite financial and temporal means to execute their strategies effectively. These attacks target critical infrastructure, communication systems, and financial networks of opposing nations [19].

Individual Disappointment. In certain cases, DDoS attacks are driven by individual disappointment rather than financial gain or ideological motives. These attackers, fueled by personal opposition or conflicts, selectively target specific organizations or individuals to cause harm or disruption [83].

Threat or Testing. These attacks are usually conducted by inexperienced users who want to increase their knowledge, using already known botnets or creating new ones. In many cases, the attack is just an exercise in style without any purpose and for pure fun [83]. In some cases, criminal groups conduct attacks as a demonstration, showcasing their botnet's efficiency to attract buyers on the dark web. Moreover, human errors play a significant role in cyber incidents, occasionally leading to DoS situations, exemplified by the Morris Worm [51].

2.4 DDoS Attack Taxonomy

Diverse methods of taxonomy have been proposed for categorizing DDoS attacks, encompassing factors such as attack layers, methods, attack vectors, attack impacts, and the degree of automation [43, 64, 83]. Some classifications also consider the attack rate, distinguishing between low-rate and high-rate attacks [27]. In this survey, we have considered the major classification criteria and categorized DDoS attacks based on the targeted layer, the method of attack, the attack vector, and the impact of the attack.

Classification by Attack Layer. This classification categorizes DDoS attacks based on which layer of the Open Systems Interconnection (OSI) model they target. Each layer has specific protocols and vulnerabilities that attackers can exploit [83].

– **Network Layer Attacks.** The network layer is responsible for routing and forwarding data packets in different networks. DDoS attacks at this layer aim to reduce network bandwidth resources. Some of the most well-known network layer DDoS attacks include:

- **ICMP Flood (Ping Flood).** This type of attack involves overwhelming the target with ICMP Echo Request (ping) packets. This can consume both incoming and outgoing bandwidth, since the target will try to respond to each ping with an Echo Reply, leading to significant network congestion [12].
- **Smurf Attack.** This attack exploits ICMP and IP broadcast addresses to flood a target with traffic. The attacker sends ICMP requests to the broadcast addresses of a network, spoofing the IP address of the target. Every host on the network responds to the request, overwhelming the target with traffic [68].

– **Transport Layer Attacks.** The transport layer is responsible for transferring data across a network and provides error-checking mechanisms and data flow controls. DDoS attacks at this layer intend to overload target servers or network devices. Common attack subcategories include:

- **SYN Flood.** This attack exploits the TCP handshake process. Attackers send a flood of TCP/SYN packets, typically with a spoofed source IP address, to the target server. The server, expecting to complete the handshake, responds with an SYN-ACK and waits for an ACK that never arrives, leaving many connections half-open and eventually exhausting the server's resources [53].
- **UDP Flood.** Unlike TCP, UDP is connection-less, and a UDP flood attack sends a large number of UDP packets to random ports on a victim's system. This forces the system to repeatedly check for the application listening at that port, respond with an ICMP "Destination Unreachable" message when no application is found, and thus consume both system and network resources [53].
- **Amplification Attacks.** These attacks are common for both UDP and TCP protocols, where an attacker sends small queries to a third-party server, spoofing the target's IP address so the server responds to the target. When using protocols with large amplification factors, such as DNS or NTP, the attacker can generate a significant amount of traffic directed at the target, overwhelming its resources [68].

– **Application Layer Attacks.** The application layer facilitates essential services like email, web browsing, and file transfer. DDoS attacks at this layer aim to exhaust the resources of a web server, application server, or web application, making the service slow or unresponsive to legitimate users [56]. Some of the well-known application layer DDoS attacks include:

- **HTTP Flood.** This attack involves sending numerous HTTP requests to a web server, intending to overwhelm it. Unlike other DDoS attacks that rely on malformed packets or high traffic volumes to disrupt the service, an HTTP flood attack uses legitimate requests. However, the sheer number of requests is enough to exhaust the server's resources [53].
- **DNS Flood.** Although primarily targeting the infrastructure layer, DNS floods can be considered an application-layer attack when the aim is to overload the DNS services of a web application. The attacker floods the DNS server with requests, attempting to exceed the server's capacity to handle traffic, which can make the web application slow or inaccessible [56].
- **SSL.** SSL-based application layer attacks exploit vulnerabilities in SSL protocols, compromising internet communication security. Common attacks like SSL

renegotiation and SSL stripping inject unauthorized data or downgrade HTTPS connections, exposing sensitive data. Additionally, vulnerabilities like Heartbleed in TLS libraries can facilitate attacks, including DDoS attacks, allowing attackers to steal sensitive information and disrupt services [56].

Classification by Attack Method. This classification looks at the technique or method employed by the attack. Using this classification, it is possible to divide DDoS attacks as follows.

- **Volumetric DDoS Attacks.** Characterized by their aim to overwhelm a target's bandwidth, these attacks include the UDP flood, ICMP flood, amplification and DNS reflection attacks, SYN floods, and IP/ICMP fragmentation [68].
- **Protocol.** The protocol-based categorization of DDoS attacks involves classifying attacks according to the protocols they target, such as HTTP, DNS, SMTP, NTP, VoIP, and ICMP. Although the majority of protocols are crafted to optimize resource allocation [68], they are still vulnerable to DDoS attacks, which predominantly target the most commonly utilized protocols.
- **Application Layer Attacks.** These attacks send a vast number of requests to a web application, overwhelming it. Examples of such attacks include HTTP flood, DNS flood, and slowloris [56].

Classification by Attack Vector. Another approach to categorizing DDoS attacks is by their attack vector, which focuses on the specific method of delivery or exploitation employed by the attacker. This classification scheme outlines three primary types of DDoS attacks based on their attack vectors.

- **Direct Attacks.** The attacker directly floods the victim's infrastructure with packets or requests, overwhelming its capacity to handle legitimate traffic.
- **Reflection Attacks.** The attacker sends requests to intermediary servers with a fabricated IP address belonging to the victim, causing these servers to respond to the victim with amplified traffic, thereby exacerbating the impact of the attack.
- **Amplification Attacks.** These attacks consist of leveraging third-party servers specifically engineered to magnify the volume of the assault. For instance, DNS and NTP amplification attacks exploit the legitimate request-response mechanism of these protocols to force the servers into transmitting disproportionately large responses to the target, intensifying the DDoS attack [68].

Classification by Impact. Several studies in the field concentrate on categorizing DDoS attacks according to their intended impact. These classifications revolve around three primary objectives: disruption, degradation, and depletion.

- **Disruption-Oriented Attacks.** These attacks are aimed at directly interrupting the availability of services or resources.

– **Degradation-Focused Attacks.** These attacks seek to diminish the performance of services, rendering them less usable for legitimate users by slowing down their functionality.
– **Depletion-Based Attacks.** These attacks target specific resources such as bandwidth, connection tables, or server CPU capacity, aiming to exhaust them and consequently induce service outages or degradation [43].

3 Deep Learning-Based DDoS Attack Detection

This section presents a review of the existing literature related to DL-based DDoS attack detection methods. It is possible to categorize detection methods according to their architectural, data representation, and learning approaches into eight types [44]: *i)* supervised instance learning, *ii)* supervised sequence learning, *iii* semi-supervised learning, *iv)* hybrid learning, *v)* adaptive learning, *vi)* transfer learning, *vii)* few-shot learning, and *viii)* federated learning. Table 2 outlines the approaches presented in this survey.

3.1 Supervised Instance Learning

Supervised instance learning with DL methods focuses on classifying individual instances into specific classes using labeled datasets. In the context of DDoS detection, these techniques employ DL models to distinguish instances of normal network traffic from various types of DDoS attacks. Common DL-based supervised instance learning architectures used are Deep Neural Networks (DNN) and Convolutional Neural Networks (CNN).

DNN-Based Methods. Different studies presented the feasibility of utilizing DNNs for intrusion and DDoS attack detection. For example, the work presented in [72] proposes a DL model for DDoS attack detection specifically targeting bandwidth and connection flooding attacks. Employing algorithms such as Decision Trees (DT), K-Nearest Neighbors (KNN), Naive Bayes (NB), and DNNs, the authors compare various classifiers to identify the most effective for DDoS detection. The DNN model, chosen for its high precision and accuracy with dynamically generated datasets, outperforms other models. Similarly, the work described in [13] proposes a DNN model based on feed-forward mechanisms for detecting DDoS attacks. The authors employ a DNN with feature learning capabilities to automatically extract relevant features from raw network traffic data. Their proposed DNN model incorporates attention mechanisms, dynamically focusing on critical features within the network traffic data.

To evaluate the ability of a trained DNN to detect unseen attacks, the work in [61] introduces both DNN and Long Short-Term Memory (LSTM) models. The authors train the models on the CIC-IDS2017 dataset and measure the accuracy of the models on the synthesized ANTS2019 dataset. To evaluate unseen attacks, the authors merge both datasets, retrain the models, and observe enhancements in detection performance against newly synthesized unknown attacks. However, the models are limited in their ability to capture complex patterns and multi-class classification and are not tested in a real-time decision setting.

Table 2. Summary of recent DL-based DDoS attack detection studies.

Taxonomy	Ref.	Date	Architecture	Dataset used	Detection	Application area	Open challenges
Supervised instance learning	[61]	2019	DNN, LSTM	CIC-IDS2017, ANTS2019	Binary	General	Evolving attack detection
	[13]	2021	DNN	CIC-DDoS2019	Binary, Multi	General	Real-time detection
	[28]	2020	Ensemble CNN	CIC-IDS2017	Binary	SDN	Reduced false positives
	[34]	2020	CNN	CIC-IDS2018, KDDCup99,	Binary, Multi	General	Multi-class classification
	[5]	2020	CNN	CIC-IDS2018	Binary	IoT	Scalability
	[75]	2022	LSTM, CNN	CIC-DDoS2019	Binary	IIoT	Multi-class classification
Supervised sequence learning	[21]	2021	RNN, DNN, CNN	CIC-DDoS2019, TON_IoT	Binary, Multi	IoT	Data imbalance
	[30]	2023	AE+LSTM	CIC-IDS2018, CIC-IDS2017,	Binary	NIDS	Attention mechanisms
	[81]	2022	LSTM	DNS-STAT	Binary	Edge	Heterogeneous method
	[4]	2021	GRU	CIC-IDS2018, CIC-DDoS2019,	Binary	SDN	Multi-class classification
Hybrid learning	[18]	2021	RBM+CNN	Private	Binary	Smart city	Multi-class classification
	[76]	2021	AE + MLP	CIC-DDoS2019	Binary, Multi	NIDS	Generalizability
	[29]	2023	CNN+BiLSTM	CIC-IDS2018, Edge_IIoT	Binary, Multi	IoT	Feature selection
Transfer learning	[78]	2019	TL-ConvNet	NSL-KDD, UNSW-NB15	Binary	Cloud IoT	Multi-class classification
	[50]	2023	EfficientNet, MobileNet	CIC-IDS2018, CIC-IDS2017	Binary	Cloud IoT	Multi-class classification
	[80]	2021	CNN	CIC-IDS2017	Binary, Multi	IoV	Online adaptive model
Adaptive learning	[10]	2023	DNN	MAWI	Binary	SDN	Multi-class classification
	[1]	2023	CNN, RNN, DNN	CIC-IDS2018, CIC-DDoS2019	Binary, Multi	NIDS	Evolving attack detection
Few-Shot learning	[15]	2023	AVG 10-shot	WUSTL-EHMS, WUSTL-IIoT, BoT–IoT	Binary, Multi	IoT	Adaptation to evolving threats
	[79]	2020	FC-Net	ISCX2012, CIC-IDS2017	Binary	NIDS	Real-time detection
	[82]	2020	FSL	UNSW-NB15, NSL-KDD	Binary, Multi	NIDS	Active learning
Federated learning	[84]	2021	K-Means	CIC-DDoS2017, NSL-KDD	Binary, Multi	IoT	Detection of unknown attacks
	[17]	2024	FF NN	CIC-DDoS2019	Binary, Multi	NIDS	Detection of unknown attacks
	[38]	2021	GRU	UNSW NB-15	Binary	IIoT	Multi-class classification
	[49]	2022	DNN	CIC-DDoS2019	Multi	IIoT	Collaborative learning

Notes. DNN = Deep Neural Network; LSTM = Long Short-Term Memory, CNN = Convolutional Neural Network; RNN = Recurrent Neural Network; AE = AutoEncoder; MLP = Multi-Layer Perceptron; FF NN = Feed Forward Neural Network; SDN = Software-Defined Network; IIoT = Industrial Internet of Things; NIDS = Network Intrusion Detection System; IoV = Internet of Vehicles.

CNN-Based Methods. An example of a method using CNN to detect DDoS attacks is described in [34]. In their work, the authors propose a CNN model considering the effects of hyper-parameter variations, including image type (grayscale, RGB), the number of convolutional layers, and kernel size. The model is evaluated across the CIC-IDS2018 and KDDCup99 datasets. To further increase the adaptability and accuracy of the models, the work in [28] introduces a CNN ensemble model incorporating Recurrent Neural Networks (RNN), LSTM, and Reinforcement Learning (RL). An ensemble of CNN and LSTM is also proposed in [75] for a comprehensive analysis of DDoS attacks in industrial internet settings. However, deep CNNs and ensemble methods increase the computational complexity of detection.

To reduce the complexity of deep CNNs and detect DDoS attacks in a timely manner, the work presented in [5] introduces a near real-time CNN model for DDoS detection, designed to work autonomously. The authors propose two scenarios: in the first, the model is trained and evaluated on a self-produced dataset; in the second scenario, the model is trained and evaluated on CIC-DDoS2019 datasets. Similarly, the work introduced in [74] proposes a multilevel framework for the detection of DDoS attacks with high accuracy and low computational complexity. In the first level, a controller analyzes suspicious traffic through entropy detection directly on the router or switch, while in the second level, a CNN model makes a fine-grained distinction between normal and abnormal traffic. In [16], the authors present a lightweight framework based on a CNN and a network traffic pre-processing algorithm, which converts packet flow data into array-like structures and divides them into sub-streams based on time windows. This spatial representation aims to minimize complexity and execution time, making it suitable for implementation on devices with limited resources.

3.2 Supervised Sequence Learning

Supervised sequence learning involves utilizing sequences of data to train models by retaining information from previous inputs. Supervised sequence learning techniques, including LSTM and Gated Recurrent Unit (GRU), have been widely explored for DDoS attack detection due to their ability to handle sequential data effectively.

Long Short-Term Memory. To validate the use of supervised sequence learning approaches, the work presented in [21] describes a comparison between LSTM, DNN, and CNN. Specifically, the LSTM model comprises an input layer and 4 LSTM layers. All three models are trained and evaluated on three datasets: CIC-DDoS-2019 containing 2 (binary), 7, and 13 attack classes, respectively. On the binary data set, LSTM and CNN perform similarly better than DNN; on the multi-label data set, all models accurately detect benign traffic. Other examples of works proposing LSTM to detect DDoS attacks are described in [40, 81, 85]. The works describe DL architectures that capture the temporal dynamics of network traffic, effectively distinguishing between normal and anomalous patterns.

Solutions integrating LSTM layers with different architectures are also often investigated. For example, the work presented in [41] describes a solution composed of two LSTM layers, a dropout layer, and a dense layer, trained and evaluated on CIC-IDS2017. Similarly, the work described in [30] introduces a two-stage DL model,

LSTM-AE, combining LSTM with an AutoEncoder (AE) to further enhance detection performance. The integration of the AE enables a more efficient feature extraction and representation of network traffic data, leading to improved detection rates. To increase the explainability of LSTM-based approaches, the method described in [77] integrates heuristics into LSTM models.

Gated Recurrent Unit. GRU models are well-suited for detecting DDoS attacks because they can handle sequential data effectively and capture long-range dependencies in network traffic patterns. However, with respect to LSTMs, GRU speeds up the training process due to its fewer tensor operations compared to LSTM. To assess the effectiveness of GRUs for DDoS detection, the work described in [4] first proposes a model consisting of an input layer, a GRU layer, a dropout layer, a fully connected layer, and a dense layer. Then, the model is compared against other DL-based (DNN, CNN, LSTM) and ML-based models on the CIC-DDoS2019 and CIC-IDS2018 datasets. Similarly, the approach presented in [58] considers a GRU-based architecture trained on the CIC-DDoS2019 dataset.

To increase the explainability of DL-based approaches, the method described in [37] integrates a GRU-based model with fuzzy logic. The model was tested using two datasets: one with emulated traffic and the CIC-DDOS2019 dataset, with results demonstrating that combining GRU with fuzzy logic represents a viable option for detecting anomalies.

3.3 Semi-supervised Learning

Semi-supervised learning techniques, particularly using AEs, can detect DDoS attacks by utilizing both labeled and unlabeled data to enhance detection accuracy and adaptability. For example, the method presented in [33] describes an AE model trained and evaluated using synthetic datasets containing DDoS traffic, generated within the Kali Linux environment, alongside the CIC-IDS2017 and NSL-KDD datasets. An SVM then classifies the output of the AE model. Similarly, the work [7] proposes an architecture formed by combining a stacked sparse AE with a DNN for the binary classification of the traffic, all evaluated on the CIC-IDS2017 and NSL-KDD datasets.

3.4 Hybrid Learning

A hybrid DL approach enhances detection capabilities by actively addressing the complexity and evolving nature of DDoS attacks. By combining multiple DL architectures, such as CNNs, RNNs, and AE, in a hybrid approach, researchers can leverage the unique strengths of each model to enhance the accuracy and robustness of the detection system [18]. The most common hybrid architecture is represented by combining CNNs and LSTMs, such as the approach described in [29], which integrates CNN and Bidirectional-LSTM architectures, to leverage the ability of CNNs in extracting features and identifying patterns and anomalies in data, as well as the effectiveness of LSTMs to process sequence and temporal dependencies in data streams. Similarly, the work

described in [60] combines CNN and LSTM models with data preprocessing based on an evolutionary algorithm.

Different hybrid architectures can be obtained by combining AE with a specific classifier, such as the method proposed in [18]. The AE acts as the first step, with the output fed to the RNN and finally to an output layer that classifies the results. A similar approach is presented in [76] by combining an AE with MLP for DDoS detection and classification.

3.5 Adaptive Learning

In response to the continually evolving landscape of DDoS attacks, researchers have developed adaptive architectures for DL models. These architectures dynamically adjust their complexity, allowing them to effectively respond to changes in datasets and evolving patterns of cyberattacks. For example, the method described in [1] introduces an anomaly-based IDS for identifying DDoS attacks using DL techniques by considering adaptive architectures with an optimized number of neurons. Similarly, the work presented in [10] describes ADAM, an adaptive DDoS attack detection method merging information entropy and unsupervised anomaly detection, that can identify both known and unknown DDoS attacks without predefined characteristics.

3.6 Transfer Learning

Transfer learning (TL) in DDoS detection enables the utilization of knowledge from pre-trained models to enhance generalization and performance with limited datasets [42,78]. For DDoS detection, TL has emerged as a solution to overcome data limitations inherent in IoT environments. For instance, the methods described in [42,50,85] consider pre-trained CNNs to increase the accuracy and efficiency of IDS in scenarios with data scarcity, such as the Internet of Vehicles (IoV) [80].

To combine the advantages of TL with adaptive learning, the paper described in [3] presents a method utilizing adaptive TL to accurately classify network traffic as benign or malicious across changing environments. The paper emphasizes the use of TL techniques alongside adaptive optimization strategies to enhance model performance and ensure a dynamic adaptation to evolving attack patterns, aiming to enhance detection mechanisms against DDoS threats in varied network scenarios.

3.7 Few-Shot Learning

As an extension of supervised learning, Few-Shot Learning (FSL) enables models to make accurate predictions with minimal examples, effectively addressing the challenge posed by rapidly evolving DDoS attack vectors [66] and addressing the challenges of labeled data scarcity in IoT environments. However, implementing DL-based FSL for detecting DDoS attacks in IoT environments requires addressing the challenge of class imbalance, where normal traffic instances greatly outnumber attack instances. To address this problem, contrastive learning, and novel sampling techniques are used, to prevent the model from being biased towards the majority class, thereby improving its ability to detect attacks with greater sensitivity [82].

An example of FSL-based DDoS detection is presented in [79], applied on a dual-component architecture that includes a feature extraction network (F-Net) and a comparison network (C-Net), facilitating the generation of delta scores from paired sample comparisons. The dataset is based on real network traffic data and is customized for an FSL scenario. More recently, the work presented in [15] combines FSL, self-supervised learning, and KNN-based classification to reduce the reliance on large labeled datasets and improve the accuracy of minority class detection.

3.8 Federated Learning

Federated learning (FL) involves training models across decentralized devices or servers holding local data samples, without exchanging them. It can be particularly suited for IoT environments where privacy restrictions do not allow data exchange across the network. For example, the method proposed in [38,49,84] detects DDoS attacks by training local models using FL, without sharing private client data, considering fog/edge computing, and employing data augmentation to address imbalanced datasets. To further take into account the differences in local data samples, the paper presented in [17] introduces FLAD, an adaptive FL approach designed for DDoS attack detection, using a mechanism that dynamically adjusts computational resources between federation members based on the difficulty of learning their attack profiles without requiring the exchange of sensitive data. An alternative approach to tackle imbalanced datasets in an FL scenario is described in [39], which presents a federated IDS (FIDS). The FIDS explores feature combinations of DDoS attack behaviors, extracts additional features to represent correlations with the data flow, and uses prototypical vectors to capture correlations between the local and global data spaces.

4 DDoS Benchmark Datasets

This section provides a summary of commonly used datasets for DDoS attack detection, including the number of features and type of attacks. The datasets are also outlined in Table 3.

KDDCup99 [6]**.** Created for the KDDCup 1999 competition, aims to detect unauthorized access and malicious activities in computer networks. It comprises approximately 5 million network connections, covering both normal connections and 22 types of cyber-attacks classified into four major categories namely Denial of Service (DoS), Remote to Local (R2L), User to Root (U2R), and Probe attacks [70]. Each record is described by 42 features falling into three types which are basic, traffic, and content.

NSL-KDD [70]**.** Developed in 2009 by the Canadian Institute for Cybersecurity, improves upon the KDDCup99 dataset by removing duplicate records and ensuring a balanced representation of attack types. It includes a structured set of 42 features, and approximately 150,000 data points, including emulated records, divided into 125,973 training records and 22,544 testing records [59].

UNSW-NB15 [46]**.** Describes 9 unique attack types, including analysis, fuzzers, backdoors, DoS, exploits, reconnaissance, generic, shellcode, and worms, with 49 features.

Table 3. Summary of commonly used datasets in DDoS attack detection.

Dataset	Year	N. features	Attack types
KDDCup99	1998	42	DoS, Probe, R2L, U2R
NSL-KDD	2009	42	DoS, Probe, R2L, U2R
CAIDA-DDoS 2007	2007	14	DDoS
ISCX2012	2012	41	Infiltration, DDoS, HTTP DoS, brute force SSH
UNSW-NB15	2015	49	Fuzzers, reconnaissance, exploits, backdoors, generic, shellcode, DoS, worms
CIC-IDS2017	2017	80	DDoS, DoS, botnet, heartbleed, brute force SSH, web attack, infiltration, brute force FTP
CIC-IDS2018	2018	80	Heartbleed, botnet, brute force, DoS, web attacks, DDoS, infiltration
CIC-DDoS2019	2019	80	DDoS, MSSQL, NTP, SSDP, NETBIOS, PortMap
BoT-IoT	2018	115	DDoS, DoS, OS and service scan, keylogging, data exfiltration
ToN-IoT	2019	42	DoS, DDoS, ransomware
CIC-IoT2023	2023	46	DDoS, DoS, reconnaissance, web-based, brute force, spoofing, Mirai

These attack categories cover various cyber threats and facilitate a comprehensive evaluation of the IDS. It contains 2,540,044 records, with 2,218,761 benign records and 321,283 malicious records.

CIC-IDS2017 [63]**.** Generated in an emulated environment from 7 March to 7 July 2017, includes packet and bi-directional flow-based network traffic. A range of attacks including DoS, Heartbleed, Brute Force SSH/FPT, web attacks, botnets, infiltration, and DDoS are simulated alongside normal network activity. The CICFlowMeter tool was used to extract over 80 features per flow from this traffic, capturing the behavior of 25 simulated users across multiple protocols (FTP, SSH, HTTP, HTTPS, and email). The dataset contains 2,273,097 benign and 557,646 malicious records [26].

CIC-IDS2018 [63]**.** Compiled by the Communications Security Establishment (CSE) & the Canadian Institute for Cybersecurity (CIC), captures network traffic and system logs from a controlled lab environment. It contains both benign traffic and seven different cyberattack scenarios, involving 50 attacking machines against an organization with 420 machines and 50 servers spread across 5 departments [63]. The dataset contains 80 characteristics with information about seven types of DDoS attacks: GoldenEye, Slowloris, Hulk, SlowHTTPTest, LOIC-HTTP, HOIC, LOIC-UDP, and benign network traffic.

CIC-DDoS2019 [64]**.** Describes attack types including UDP flood, TCP SYN flood, and HTTP flood, enabling targeted analysis of specific attack characteristics [64]. The dataset contains over 80 traffic features and encompasses common DDoS attacks. Attacks are reflection-based (MSSQL, NTP, SSDP) and exploitation-based (UDP flood, SYN flood). Data collection spanned 2 days, with training capturing 12 attack types on January 12th, 2019, and testing capturing 7 attack types on March 11th, 2019. Benign

data comprises 0.16%, while attack data accounts for 99.84%, resulting in a significant data imbalance [1].

CIC-IoT2023 [48]**.** Created by the Canadian Institute of Cybersecurity, it is a comprehensive collection designed for IoT security research. It simulates real-world scenarios with 105 IoT devices and captures a broad spectrum of 33 attacks across seven categories: DDoS, DoS, reconnaissance, web-based, brute force, spoofing, and mirai. This dataset aims to enhance security analytics development for IoT environments by providing a realistic variety of attack vectors.

BoT-IoT [35], Developed in the University of New South Wales (UNSW) Canberra's Cyber Range Lab, it presents a blend of normal and malicious botnet traffic within a realistic network setting. With its comprehensive collection totaling 69.3 GB of pcap files and over 72 million records, the dataset describes various cyber threats, including DDoS, DoS, OS and Service Scan, Keylogging, and Data Exfiltration attacks [55].

ISCX2012 [65]**.** Created by the University of New Brunswick on a day of network activity from June 11 to June 17, 2010, it features a mix of normal and malicious traffic captured in an emulated network environment. This dataset is particularly noted for its inclusion of full-packet network data, facilitating the study of a range of attack behaviors such as network infiltration, DDoS, HTTP DoS, and brute force SSH, against a backdrop of regular user activities. Characterized by its imbalanced nature and labeled records, it offers 2,381,532 benign and 68,792 malicious entries.

TON_IoT [45]**.** Curated by the School of Engineering and Information Technology at UNSW Canberra, it provides a comprehensive benchmark for evaluating AI-driven cybersecurity applications in Industry 4.0 and IoT/IIoT environments. The dataset includes a diverse range of data sources, including telemetry from IIoT sensors, operating system logs from Windows and Ubuntu platforms, and network traffic. The data is collected using a network testbed that simulates real-world IoT infrastructures and is designed to capture a wide range of cyber-attack scenarios, such as DoS, DDoS, and ransomware attacks on various system components. The dataset is structured into raw, processed, and training/testing formats.

CAIDA-DDoS 2007 [71]**.** Offers an hour of network traffic data from a DDoS attack that occurred on August 4, 2007. Divided into 5-minute segments, it amounts to 5.3 GB when compressed (21 GB uncompressed). It specifically concentrates on the attack and its immediate responses, filtering out any unrelated traffic. To protect privacy, the data is anonymized using CryptoPAn, and payload information is omitted to highlight traffic patterns.

In addition to the benchmark datasets mentioned above, there are other publicly available datasets tailored to the study of DDoS attacks in IoT environments that go beyond the widely recognized benchmark datasets for cybersecurity research. Some of these datasets capture the FLAG and CDX in a variety of network traffic scenarios. In addition, host-based datasets are also available, providing a wide range of attack vectors and normal traffic patterns for comprehensive analysis [26].

5 Open Research Challenges in DDoS Attack Detection

This section reviews the most common open research challenges in the study, design, and analysis of DDoS attack detection systems.

Lack of Comprehensive Datasets. In DL for DDoS attack detection, imbalanced datasets pose a significant challenge. The datasets often have a disproportionate number of examples for some types of attacks, leading to a model bias towards more common threats and poor detection of rarer attacks [13, 18, 21, 61]. Maintaining a balance between attack and benign network traffic is crucial for creating models that can effectively detect a wide range of DDoS attacks. As mentioned in Sect. 4, some datasets feature such imbalance even in binary classification contexts.

Lack of Works on Real-Time Environments. The existing literature reveals a gap in deploying DL models for DDoS attack detection in real-time environments. While many studies [28, 44] have performed offline analyses of their models, the dynamic nature of DDoS attacks that occur in real-time underscores the need for models to be tested and validated in real-time scenarios. Offline analysis, even though valuable, does not fully capture the model's effectiveness against actual attacks. Therefore, there is a pressing need for developing and validating DL models within real-time contexts to ensure their practical applicability and effectiveness in thwarting DDoS threats as they happen.

Zero-Day and Adaptation to New Vectors of DDoS Attacks. ML and DL models typically perform well on datasets with known characteristics. However, attackers often introduce novel patterns, reducing the effectiveness of existing models in accurately identifying unforeseen threats [61]. To address this vulnerability, it's crucial to update models to recognize new attack patterns regularly, ensuring robust defense mechanisms against evolving cybersecurity threats. Adapting detection methods to evolving DDoS threats presents significant challenges, including rapid attack tactic adaptation, sophisticated evasion techniques, and exploitation of new vulnerabilities [44, 61]. Traditional models struggle to keep pace, necessitating continuous updates and the integration of advanced DL techniques. Additionally, attacks' increasing scale and complexity require more dynamic and scalable detection solutions.

False Positives and Negatives. Minimizing false positives and negatives in DDoS attack detection presents challenges crucial for maintaining operational security. False positives can lead to unnecessary alerts, waste resources and potentially divert attention from real threats. Conversely, false negatives allow malicious attacks to proceed undetected, causing potential damage [28]. To mitigate these errors, it's essential to refine detection algorithms for higher accuracy, utilize comprehensive and updated threat intelligence, and implement adaptive thresholds based on real-time network behavior.

Binary Classification. The majority of the existing literature has predominantly focused on binary classification rather than the multi-class classification of DDoS attacks [5,28,30,38,50,61,75,79,81]. Multi-class classification in DDoS attack detection can instead provide granular insights, tailored response strategies, improved threat intelligence, and adaptability to evolving attack techniques, compared to binary classification, thereby enabling a more comprehensive understanding of the threat landscape and more targeted and effective defense strategies [13,75].

Collaborative Learning. The development of privacy-preserving collaborative models presents another open research challenge. Different organizations vulnerable to DDoS attacks may withhold critical features due to concerns about maintaining customer trust and managing privacy issues. Some work has been done on DDoS attacks based on collaborative and federated learning, such as FLAD [17], FLDDoS [84], FIDS [39], and FLEAM [38]. However, there are still research gaps that are essential for the advancement of collaborative learning models in this domain. This can be achieved by improving algorithms to enhance accuracy and convergence time.

IoT-Based DDoS Attacks. DDoS attacks from compromised IoT devices present unique challenges due to the sheer number and variety of such devices that can easily be harnessed into botnets. These botnets amplify DDoS attacks by taking advantage of the widespread and often poorly secured nature of IoT devices. In addition, the computational limitations of these devices require lightweight models for detecting IoT DDoS attacks.

6 Conclusion

While numerous Deep Learning (DL)-based approaches for Distributed Denial of Service (DDoS) attack detection have been proposed by researchers over the years, with the evolution of the attackers' techniques and the rapid deployment of unknown zero-day DDoS attacks, there is still an attention need for robust defense mechanisms. In this survey, we addressed the origin, evolution, motivation, and taxonomy of DDoS attacks, emphasizing the key role of DL in improving the accuracy of attack detection. We categorized DL-based detection models based on architecture, data representation, and learning approaches. We described the available benchmark datasets used in existing studies, taking into account the number of features and attack types. Lastly, we highlighted the open research challenges that need to be addressed to strengthen the detection of complex DDoS attacks.

Acknowledgments. This work was supported in part by the EC under project GLACIATION (101070141) and project Chips JU EdgeAI (101097300), and by project SERICS (PE00000014) under the MUR NRRP funded by the EU - NextGenerationEU. Views and opinions expressed are however those of the authors only and do not necessarily reflect those of the European Union or the Italian MUR. Neither the European Union nor Italian MUR can be held responsible for them. We also thank the NVIDIA Corporation for the GPU donated.

References

1. Agostinello, D., Genovese, A., Piuri, V.: Anomaly-based intrusion detection system for DDoS attack with deep learning techniques. In: Proceedings of the 20th International Conference on Security and Cryptography, vol. 1, pp. 267–275. SCITEPRESS (2023)
2. Alomari, E., Manickam, S., Gupta, B.B., Karuppayah, S., Alfaris, R.: Botnet-based distributed denial of service (DDoS) attacks on web servers: classification and art. arXiv preprint arXiv:1208.0403 (2012)
3. Anley, M.B., Genovese, A., Agostinello, D., Piuri, V.: Robust DDoS attack detection with adaptive transfer learning. Comput. Secur. **144**(103962), 1–10 (2024). ISSN: 0167-4048
4. Assis, M.V., Carvalho, L.F., Lloret, J., Proença, M.L., Jr.: A gru deep learning system against attacks in software defined networks. J. Netw. Comput. Appl. **177**, 102942 (2021)
5. de Assis, M.V., Carvalho, L.F., Rodrigues, J.J., Lloret, J., Proen Jr, M.L.: Near real-time security system applied to SDN environments in IoT networks using CNN. Comput. Electr. Eng. (2020)
6. Bay, S.D., Kibler, D., Pazzani, M.J., Smyth, P.: The UCI KDD archive of large data sets for data mining research and experimentation. ACM SIGKDD Explor. Newsl. **2**(2), 81–85 (2000)
7. Bhardwaj, A., Mangat, V., Vig, R.: Hyperband tuned deep neural network with well posed stacked sparse autoencoder for detection of DDoS attacks in cloud. IEEE Access **8**, 181916–181929 (2020)
8. Blog, M.S.: Microsoft response to layer 7 DDoS. https://msrc.microsoft.com/blog/2023/06/microsoft-response-to-layer-7-ddos-attacks
9. Brooks, R.R., Yu, L., Ozcelik, I., Oakley, J., Tusing, N.: Distributed denial of service (DDoS): a history. IEEE Ann. Hist. Comput. **44**(2), 44–54 (2021)
10. Cai, T., Jia, T., Adepu, S., Li, Y., Yang, Z.: Adam: an adaptive DDoS attack mitigation scheme in software-defined cyber-physical system. IEEE Trans. Ind. Inf. (2023)
11. Center, CERT Coordination: Certr incident note in-99-07 distributed denial of service tools. CERT Coordination Center, Pittsburgh, Incident Note IN-99-07 (1999)
12. Chauhan, V., Saini, P.: ICMP flood attacks: a vulnerability analysis. In: Cyber Security: Proceedings of CSI 2015, pp. 261–268. Springer (2018). https://doi.org/10.1007/978-981-10-8536-9_26
13. Cil, A.E., Yildiz, K., Buldu, A.: Detection of DDoS attacks with feed forward based deep neural network model. Expert Syst. Appl. **169**, 114520 (2021)
14. Cloudflare: Cloudflare ddos threat report 2022 q3 (2022). https://blog.cloudflare.com/cloudflare-ddos-threat-report-2022-q3/
15. Dina, A.S., Siddique, A.B., Manivannan, D.: Fs3: few-shot and self-supervised framework for efficient intrusion detection in internet of things networks. In: Proceedings of the 39th Annual Computer Security Applications Conference, pp. 138–149. Association for Computing Machinery, New York, NY, USA (2023)
16. Doriguzzi-Corin, R., Millar, S., Scott-Hayward, S., Martinez-del Rincon, J., Siracusa, D.: Lucid: a practical, lightweight deep learning solution for DDoS attack detection. IEEE Trans. Netw. Serv. Manage. **17**(2), 876–889 (2020)
17. Doriguzzi-Corin, R., Siracusa, D.: Flad: adaptive federated learning for DDoS attack detection. Comput. Secur. **137**, 103597 (2024)
18. Elsaeidy, A.A., Jamalipour, A., Munasinghe, K.S.: A hybrid deep learning approach for replay and DDoS attack detection in a smart city. IEEE Access **9**, 154864–154875 (2021)
19. ENISA: Enisa threat landscape: Cyber espionage (2020)
20. European Union Agency for Cybersecurity (ENISA): ENISA Threat Landscape for DoS Attacks. Technical Report, European Union Agency for Cybersecurity (ENISA) (2023)

21. Ferrag, M.A., Shu, L., Djallel, H., Choo, K.K.R.: Deep learning-based intrusion detection for distributed denial of service attack in agriculture 4.0. Electronics **10**(11), 1257 (2021)
22. Gamage, S., Samarabandu, J.: Deep learning methods in network intrusion detection: a survey and an objective comparison. J. Netw. Comput. Appl. **169**, 102767 (2020)
23. Google Cloud: How google cloud blocked largest layer 7 DDoS attack (2024). https://cloud.google.com/blog/products/identity-security/how-google-cloud-blocked-largest-layer-7-ddos-attack-
24. Greenberg, A.: The cheap radio hack disrupted Poland's railway system. https://www.wired.com/story/poland-train-radio-stop-attack/
25. Greig, J.: Killnet DDoS attacks on U.S. hospitals (2023). https://therecord.media/ddos-hospitals-cisa-killnet-limited-effects
26. Gümüşbaş, D., Yıldırım, T., Genovese, A., Scotti, F.: A comprehensive survey of databases and deep learning methods for cybersecurity and intrusion detection systems. IEEE Syst. J. **15**(2), 1717–1731 (2020)
27. Gupta, B.B., Joshi, R.C., Misra, M.: Defending against distributed denial of service attacks: issues and challenges. Inf. Secur. J. Global Perspect. **18**(5), 224–247 (2009)
28. Haider, S., et al.: A deep CNN ensemble framework for efficient DDoS attack detection in software-defined networks. IEEE Access **8**, 53972–53983 (2020)
29. Hnamte, V., Hussain, J.: DCNNBiLSTM: an efficient hybrid deep learning-based intrusion detection system. Telematics Inform. Rep. **10**, 100053 (2023)
30. Hnamte, V., Nhung-Nguyen, H., Hussain, J., Hwa-Kim, Y.: A novel two-stage deep learning model for network intrusion detection: LSTM-ae. IEEE Access (2023)
31. Hwang, R.H., Peng, M.C., Huang, C.W., Lin, P.C., Nguyen, V.L.: An unsupervised deep learning model for early network traffic anomaly detection. IEEE Access **8**, 30387–30399 (2020)
32. Jung, T.: The most notorious DDoS attacks in history– 2021 update (2021). https://www.cloudbric.com/the-most-notorious-ddos-attacks2021
33. Kasim, Ö.: An efficient and robust deep learning based network anomaly detection against distributed denial of service attacks. Comput. Netw. **180**, 107390 (2020)
34. Kim, J., Kim, J., Kim, H., Shim, M., Choi, E.: CNN-based network intrusion detection against denial-of-service attacks. Electronics **9**(6), 916 (2020)
35. Koroniotis, N., Moustafa, N., Sitnikova, E., Turnbull, B.: Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: Bot-IoT dataset. Futur. Gener. Comput. Syst. **100**, 779–796 (2019)
36. LeCun, Y., Bengio, Y., Hinton, G.: Deep learning. Nature **521**(7553), 436 (2015)
37. Lent, D.M.B., Novaes, M.P., Carvalho, L.F., Lloret, J., Rodrigues, J.J., Proença, M.L.: A gated recurrent unit deep learning model to detect and mitigate distributed denial of service and portscan attacks. IEEE Access **10**, 73229–73242 (2022)
38. Li, J., Lyu, L., Liu, X., Zhang, X., Lyu, X.: Fleam: a federated learning empowered architecture to mitigate DDoS in industrial IotT. IEEE Trans. Industr. Inf. **18**(6), 4059–4068 (2021)
39. Li, J., Zhang, Z., Li, Y., Guo, X., Li, H.: Fids: detecting DDoS through federated learning based method. In: 2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pp. 856–862. IEEE (2021)
40. Li, M., Zhang, B., Wang, G., ZhuGe, B., Jiang, X., Dong, L.: A DDoS attack detection method based on deep learning two-level model CNN-LSTM in SDN network. In: 2022 International Conference on Cloud Computing, Big Data Applications and Software Engineering (CBASE), pp. 282–287. IEEE (2022)
41. Liang, X., Znati, T.: A long short-term memory enabled framework for DDoS detection. In: 2019 IEEE Global Communications Conference (GLOBECOM), pp. 1–6. IEEE (2019)
42. Masum, M., Shahriar, H.: A transfer learning with deep neural network approach for network intrusion detection. Int. J. Intell. Comput. Res. **12**(1) (2021)

43. Mirkovic, J., Reiher, P.: A taxonomy of DDoS attack and DDoS defense mechanisms. ACM SIGCOMM Comput. Commun. Rev. **34**(2), 39–53 (2004)
44. Mittal, M., Kumar, K., Behal, S.: Deep learning approaches for detecting DDoS attacks: a systematic review. Soft. Comput. **27**(18), 13039–13075 (2023)
45. Moustafa, N.: A new distributed architecture for evaluating AI-based security systems at the edge: network ton_iot datasets. Sustain. Cities Soc. **72**, 102994 (2021) (2021)
46. Moustafa, N., Slay, J.: Unsw-nb15: a comprehensive data set for network intrusion detection systems (unsw-nb15 network data set). In: 2015 Military Communications and Information Systems Conference (MilCIS), pp. 1–6. IEEE (2015)
47. Nazario, J., Czosseck, C., Geers, K.: Politically motivated denial of service attacks (2009)
48. Neto, E.C.P., Dadkhah, S., Ferreira, R., Zohourian, A., Lu, R., Ghorbani, A.A.: Ciciot2023: a real-time dataset and benchmark for large-scale attacks in IoT environment (2023)
49. Neto, E.C.P., Dadkhah, S., Ghorbani, A.A.: Collaborative DDoS detection in distributed multi-tenant IoT using federated learning. In: 2022 19th Annual International Conference on Privacy, Security & Trust (PST), pp. 1–10. IEEE (2022)
50. Okey, O.D., Melgarejo, D.C., Saadi, M., Rosa, R.L., Kleinschmidt, J.H., Rodríguez, D.Z.: Transfer learning approach to ids on cloud IoT devices using optimized CNN. IEEE Access **11**, 1023–1038 (2023)
51. Orman, H.: The Morris worm: a fifteen-year perspective. IEEE Secur. Priv. **1**(5), 35–43 (2003)
52. Osterweil, E., Stavrou, A., Zhang, L.: 20 years of DDoS: a call to action. CoRR abs/1904.02739 (2019)
53. Oyekunle, I.: What are the types of DDoS attacks? (2021). https://securitygladiators.com/threat/ddos/type/
54. Pagliery, J.: Mafiaboy: the infamous teenage hacker who took down the internet (2011). http://edition.cnn.com/2011/TECH/web/08/15/mafiaboy.hacker/index.html
55. Peterson, J.M., Leevy, J.L., Khoshgoftaar, T.M.: A review and analysis of the bot-IoT dataset. In: 2021 IEEE International Conference on Service-Oriented System Engineering (SOSE), pp. 20–27 (2021)
56. Praseed, A., Thilagam, P.S.: DDoS attacks at the application layer: challenges and research perspectives for safeguarding web applications. IEEE Commun. Surv. Tutorials **21**(1), 661–685 (2018)
57. Tandon, R.: A survey of distributed denial of service attacks and defenses. arXiv.org (2020)
58. ur Rehman, S., et al.: DiDDoS: an approach for detection and identification of distributed denial of service (DDoS) cyberattacks using gated recurrent units (Gru). Future Gener. Comput. Syst. **118**, 453–466 (2021)
59. Ring, M., Wunderlich, S., Scheuring, D., Landes, D., Hotho, A.: A survey of network-based intrusion detection data sets. Comput. Secur. **86**, 147–167 (2019)
60. Roopak, M., Tian, G.Y., Chambers, J.A.: An intrusion detection system against DDoS attacks in IoT networks. 2020 10th Annual Computing and Communication Workshop and Conference (CCWC), pp. 0562–0567 (2020)
61. Sabeel, U., Heydari, S.S., Mohanka, H., Bendhaou, Y., Elgazzar, K., El-Khatib, K.: Evaluation of deep learning in detecting unknown network attacks. In: 2019 International Conference on Smart Applications, Communications and Networking (SmartNets), pp. 1–6. IEEE (2019)
62. Salim, M.M., Rathore, S., Park, J.H.: Distributed denial of service attacks and its defenses in IoT: a survey. J. Supercomputing **76**(7), 5320–5363 (2019)
63. Sharafaldin, I., Lashkari, A.H., Ghorbani, A.A.: Toward generating a new intrusion detection dataset and intrusion traffic characterization. ICISSp **1**, 108–116 (2018)

64. Sharafaldin, I., Lashkari, A.H., Hakak, S., Ghorbani, A.A.: Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy. In: 2019 International Carnahan Conference on Security Technology (ICCST), pp. 1–8. IEEE (2019)
65. Shiravi, A., Shiravi, H., Tavallaee, M., Ghorbani, A.A.: Toward developing a systematic approach to generate benchmark datasets for intrusion detection. Comput. Secur. **31**(3), 357–374 (2012)
66. Snell, J., Swersky, K., Zemel, R.: Prototypical networks for few-shot learning. In: Advances in Neural Information Processing Systems, vol. 30 (2017)
67. Sparling, C., Rath, S.: Record-breaking DDoS in APAC (2023). https://www.akamai.com/blog/security/record-breaking-ddos-in-apac
68. Specht, S., Lee, R.: Taxonomies of Distributed Denial of Service Networks, Attacks, Tools and Countermeasures. CEL2003-03, Princeton University, Princeton, NJ, USA (2003)
69. Sultana, N., Chilamkurti, N., Peng, W., Alhadad, R.: Survey on SDN-based network intrusion detection system using machine learning approaches. Peer-to-Peer Networking Appl. **12**, 493–501 (2019)
70. Tavallaee, M., Bagheri, E., Lu, W., Ghorbani, A.A.: A detailed analysis of the KDD cup 99 data set. In: 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications, pp. 1–6. IEEE (2009)
71. The CAIDA UCSD: DDoS Attack 2007 Dataset (2007). https://www.caida.org/catalog/datasets/ddos-20070804_dataset/
72. Virupakshar, K.B., Asundi, M., Channal, K., Shettar, P., Patil, S., Narayan, D.: Distributed denial of service (DDoS) attacks detection system for openstack-based private cloud. Procedia Comput. Sci. **167**, 2297–2307 (2020)
73. Wang, A., Chang, W., Chen, S., Mohaisen, A.: Delving into internet DDoS attacks by botnets: characterization and analysis. IEEE/ACM Trans. Networking **26**(6), 2843–2855 (2018)
74. Wang, L., Liu, Y.: A DDoS attack detection method based on information entropy and deep learning in SDN. In: 2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), vol. 1, pp. 1084–1088. IEEE (2020)
75. Wei, W., Liu, X., Sheng, C., Feng, A.: A DDoS attack traffic classification model for industrial internet based on CNN-LSTM. In: 2022 China Automation Congress (CAC), pp. 3443–3448. IEEE (2022)
76. Wei, Y., Jang-Jaccard, J., Sabrina, F., Singh, A., Xu, W., Camtepe, S.: AE-MLP: a hybrid deep learning approach for DDoS detection and classification. IEEE Access **9**, 146810–146821 (2021)
77. Wu, C.s., Chen, S.: A heuristic intrusion detection approach using deep learning model. In: 2023 International Conference on Information Networking (ICOIN), pp. 438–442. IEEE (2023)
78. Wu, P., Guo, H., Buckland, R.: A transfer learning approach for network intrusion detection. In: 2019 IEEE 4th International Conference on Big Data Analytics (ICBDA), pp. 281–285. IEEE (2019)
79. Xu, C., Shen, J., Du, X.: A method of few-shot network intrusion detection based on meta-learning framework. IEEE Trans. Inf. Forensics Secur. **15**, 3540–3552 (2020)
80. Yang, L., Shami, A.: A transfer learning and optimized CNN based intrusion detection system for internet of vehicles. In: ICC 2022-IEEE International Conference on Communications, pp. 2774–2779. IEEE (2022)
81. Yeom, S., Choi, C., Kim, K.: LSTM-based collaborative source-side DDoS attack detection. IEEE Access **10**, 44033–44045 (2022)
82. Yu, Y., Bian, N.: An intrusion detection method using few-shot learning. IEEE Access **8**, 49730–49740 (2020)
83. Zargar, S.T., Joshi, J., Tipper, D.: A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. IEEE Commun. Surv. Tutorials **15**(4), 2046–2069 (2013)

84. Zhang, J., Yu, P., Qi, L., Liu, S., Zhang, H., Zhang, J.: FLDDoS: DDoS attack detection model based on federated learning. In: 2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pp. 635–642. IEEE (2021)
85. Zhang, Y., Liu, Y., Zhang, Y., Han, L., Zhao, J., Wu, Y.: A DDoS attack detection method based on LSTM neural network in the internet of vehicles. In: Proceedings of the 4th International Conference on Information Technologies and Electrical Engineering, pp. 1–5 (2021)