ITC 1/51
Information Technology
and Control
Vol. 51 / No. 1 / 2022
pp. 180-215
DOI 10.5755/j01.itc.51.1.29595

A Comprehensive Review of Deep Learning Techniques for the Detection of (Distributed) Denial of Service Attacks

Received 2021/08/11 | Accepted after revision 2022/01/25

http://dx.doi.org/10.5755/j01.itc.51.1.29595

HOW TO CITE: Malliga, S., Nandhini, P. S., Kogilavani, S. V. (2022). A Comprehensive Review of Deep Learning Techniques for the Detection of (Distributed) Denial of Service Attacks. *Information Technology and Control*, 51(1), 180-215. https://doi.org/10.5755/j01.itc.51.1.29595

A Comprehensive Review of Deep Learning Techniques for the Detection of (Distributed) Denial of Service Attacks

S. Malliga, P. S. Nandhini, S. V. Kogilavani

Department of Computer Science and Engineering; Kongu Engineering College; Tamil Nadu; India;
Phone: 919842278780; e-mail : mallisenthil.cse@kongu.edu

Corresponding author: mallisenthil.cse@kongu.edu

(Distributed) Denial of Service (DoS/DDoS) attacks are performed to bring down a target by flooding it with useless traffic. Because the DoS/DDoS attackers often change their styles and attack patterns, the nature and characteristics of these attacks need to be examined cautiously. Developing mechanisms to detect this menace is a challenging task. Recently, deep learning has played a major role in the growth of intrusion detection solutions. In recent years, significant attempts have been made to construct deep learning models for countering DoS/DDoS threats. In this review, we provide a taxonomy of DoS/DDoS attacks and deep learning-based DoS/DDoS detection approaches. Then, the article focuses on the recent (from 2016 onwards) defensive methods against DoS/DDoS attacks that exploit the advantages of deep learning techniques and discusses the key features of each of them. As datasets are imperative for deep learning techniques, we also review the traditional and contemporary datasets that contain traces of DoS/DDoS attacks. The findings from the review articles are as well summarized and they urge that more effort be made to strengthen the existing state-of-the-art approaches to coping with the dynamic behavior of the attackers. The imbalances in the surveyed articles are also highlighted. Finally, we outline a few key research directions that will need additional focus in the near future to ensure good security against DoS/DDoS attacks using deep learning approaches.

KEYWORDS: DoS, DDoS attacks, Datasets, Flooding, Deep Learning.

1. Introduction

A Denial of Service (DoS) attack involves overwhelming a target server with traffic, rendering it inoperable. Unlike other types of attacks, the main intention of a DoS attacker is not to steal information but to degrade the performance or bring down a target. A form of DoS attack, called as DDoS (Distributed DoS) attack, is initiated from multiple systems simultaneously, thereby leading to quick exhaustion of resources on a target system. Botnets of malware-infected computers are one way to create DDoS attacks. We present an insight into what these attacks are, by taking a look at some of the most notable DoS/DDoS attacks to date.

One of the largest DDoS assaults on GitHub was in February of 2018. During this attack, incoming traffic was detected at a pace of 1.3 Tbps. Fortunately, GitHub has a DDoS security mechanism that warned within 10 minutes of the attack's start and was able to instantly stop the attack. This was the one of world's largest DDoS strikes, which lasted about 20 minutes [87] In October 2020, Google stated that its infrastructure had been subjected to a large 2.5 Tbps DDoS attack, the highest-bandwidth attack reported to date, which employed numerous techniques of attacks. The attackers exploited many networks to fake 167 million of packets per second to 180,000 vulnerable CLDAP, DNS, and SMTP servers, which then sent massive responses. This was four times the size of the Mirai botnet's previous year's record-breaking 623 Gbps attack [87]. Amazon Web Services (AWS) was the target of a massive DDoS attacks in February 2020. This was the most severe DDoS attack in recent history, and it was launched against an anonymous AWS client via CLDAP reflection. This approach leverages insecure third-party CLDAP servers to multiply data delivered to the victim's IP address by 56 to 70 times. Three days later, the attack peaked at 2.3 Tbps. Having seen the recent DDoS attacks and their sheer scale, let us now look at the consequences.

According to NexusGuard survey [99], DoS/DDoS attacks rose by more than 542% in the first quarter of 2020 as compared to the fourth quarter of 2019. This is attributed to a surge in disruptive cyber behaviour during the Covid-19 pandemic. A report on DDoS attacks [101] enumerates the DDoS attacks and their effects throughout the first quarter of 2020. NETSCOUT Arbor's 13th annual Worldwide Infrastructure Security Report [86] identified the following findings:

1. In 2018, the cost of downtime caused by DoS/DDoS attacks was $221,836.80. Germany incurred the largest expenses of downtime, totaling $351,995.
2. Businesses were once again exposed to risk from within the firewall—indeed, from the firewall itself. 43% indicated that their firewall and/or intrusion prevention system contributed to an outage during a DoS/DDoS attack. Additionally, hostile insiders constituted a hazard, as more than a quarter of respondents reported that their business had been the victim of an attack by a malicious insider in 2018. In recent years, there have been multiple instances of similar attacks as a result of insider threats that have gone unreported by the victim organisations for fear of attracting unfavorable attention.
3. In 2017, the survey respondents reported revenue loss as a business impact of DDoS attacks. An estimated 10% of firms have been subjected to an attack with a cost of more than $100,000, which was five times more than the previous year. In addition, 57% listed reputation or brand damage as the key business impact of an attack.

According to the findings of NETSCOUT Threat Intelligence Report, in the first half of 2021 [85], adversaries floated nearly 5.4 million DDoS attacks, an 11% increase over the same time in 2020. Although attack counts went down from May to June 2020, the world is still on track to approach close to a record-breaking 11 million DDoS attacks in 2021. According to Imperva's 2019 Global DDoS Threat Landscape Report, the biggest application layer DDoS attacks has been observed in 2019 [84]. This attack lasted 13 days and reached 292,000 requests per second at its peak. Furthermore, according to another report [102], the number of application layer DoS/DDoS attacks doubles every quarter of the year, despite the fact that the number of network layer attacks in the fourth quarter of 2017 reduced by a massive 50% compared to the third quarter of 2017. Tripathi and Hubballi [121] listed application layer DoS/DDoS attack incidents and discussed the type of attacks and their impacts.

From above reports, it is very clear that the attackers hire systems to mount DDoS attacks against competitors' websites with the intention of not only to impact the website, but also impact the business. A DoS/DDoS attack is relatively inexpensive, but the impact on business can be huge. In addition to immediate financial expenses, this lack of service harms the company's reputation, which could have far-reaching consequences in the long run. A white paper which analyzed the business impact of DDoS attacks [126] identifies a few impacts of DoS/DDoS attacks on business namely disruption to access to the data, business disruption and hitting the customer trust and value. Of course, identifying who carried out a DoS/DDoS attack is quite difficult. Since the attack will not originate from attacker's IP address attempting to take legal action against an attacker being suspected is unlikely to be successful unless we have extensive financial resources.

As DoS/DDoS attackers change the nature of attacks often and these attacks do not have common characteristics, it is very difficult to detect and mitigate the impacts these attacks. It is to be exceedingly difficult to resist or trace these attacks. Generally, automated software tools, called botnets are deployed to launch DoS/DDoS attacks. Many defensive mechanisms have been suggested to thwart the DoS/DDoS attacks. A classification of DoS/DDoS defensive approaches is presented in [52, 55]. Kayacik et al. [52] classified the detection approaches either as signature based or anomaly based. The AI based approaches like machine learning techniques have been classified under anomaly-based techniques. And, Khalaf et al. [55] categorized the defensive mechanisms as statistical and AI based approaches. These classifications show the role of AI in DoS/DDoS defensive algorithms. But, in both classifications only machine learning algorithms have been covered. A recent survey by Gümüşbaş et al. [34] presented a comprehensive overview of machine learning and deep learning approaches for intrusion detection systems.

Deep learning has emerged as a new technique due to its ability to handle huge volume of data and provide high accuracy with its distinctive learning mechanism. Deep learning is one of the latest research developments in AI, and it seeks to overcome the challenges that conventional machine learning approaches have. Human efforts are required in machine learning algorithms for feature extraction. While processing huge amount of data, feature extraction by human would not be efficient. In such cases, deep neural networks perform better than a human. The success of deep learning algorithms in many domains grabbed the attention of researchers in cybersecurity too. Deep learning is a branch of machine learning approaches that use Artificial Neural Networks (ANN) as their foundation. An ANN has three layers: input, output, and a hidden layer. Deep Neural Network (DNN) is an ANN with many hidden layers, and this is where deep learning comes into play. A deep learning system learns itself by filtering information through multiple hidden layers. DNNs extract important features from data to solve the cyber-attack detection problem by the process of deep learning. Subsequently, the researchers have started to use deep learning techniques for addressing DoS/DDoS attacks also, but still applied less for the detection of DoS/DDoS attacks. Imamverdiyev and Abdullayeva [44] have presented a survey on deep learning based DDoS detection methods proposed till 2016 and also, the articles reviewed have been using only KDD CUP 99/ NSL KDD datasets. These datasets were created long back and do not really reflect the recent trends in the attack traffic. Thus, the primary aim of this article is to provide an overview of recent research activities that use deep learning models to detect DoS/DDoS attacks using both conventional and contemporary datasets.

The rest of the article is orchestrated as follows. Section 2 briefly provides recent DoS/DDoS detection approaches and our contributions in this work. In Section 3, we define strategies adopted to include and exclude the review articles in this study. A taxonomy of DoS/DDoS attacks and deep learning-based detection approaches are summarized in Section 4. This section also gives a brief overview of various deep learning algorithms. The traditional and recent datasets for DoS/DDoS attacks are explored in Section 5. We analyze all recent research attempts which use deep learning algorithms for defending against network/transport and application layer DoS/DDoS attacks in Section 6 and provide a detailed report of the same. Based on our study, we present our findings and observations in Section 7. Finally, Section 8 concludes our survey with a few guidelines for further research.

2. Recent Surveys on DoS/DDoS Detection Mechanisms

An Intrusion Detection System (IDS) is a common technique for tracking and detecting internal and external intrusions aimed at damaging a network or server. It includes tools and procedures for screening the computer system and network activity, as well as analyzing activities with the goal of detecting potential intrusions affecting the system. Many studies have been conducted to build IDS using machine learning and deep learning techniques. In this section, we intend to summarize the IDS solutions based on Deep Learning. Since long back, the researchers have been applying machine learning techniques to build IDS for detecting cyber-attacks. As the attackers and attacking tools like botnets have been changing their style of attacks and produce a very huge volume, the machine learning techniques faced many challenges and issues. One of the challenges is to handle the huge data, which requires more training time. Nevertheless, a subset of machine learning called, Deep Learning provides an effective learning mechanism from a huge data. So, numerous research attempts have been devoted to make use of deep learning for developing IDSs.

A review on deep learning methods for anomaly-based intrusion detection systems (almost 35 papers) was proposed by Arwa Aldweesh et al. [6]. The authors gave a detailed taxonomy of deep learning based IDSs and the datasets used for developing IDSs. Also, the authors have thrown a light on directions for future research. Elike Hodo et al. [37] presented a classification of IDSs and taxonomy of machine Learning based IDSs. This article also provided a survey on deep learning based IDSs. Many reviews [4, 66, 70] have also focused on the classification of different machine learning and deep learning approaches for intrusion detection. Another survey by Dilara et al. [34] presented a brief overview of various benchmark datasets used for developing IDSs, attack types in these datasets and common deep learning methods for IDSs. From these surveys, we understood that the researchers gave a significant attention to the intrusion detection and built IDSs to detect various intrusion activities like unauthorized access, man-in-the-middle attacks etc. DoS/DDoS attacks are one of the riskiest intrusion operations that intruders engage in. The DoS/DDoS attacks are considered as the serious attacks and the consequences of these attacks are disastrous. They inflicted damages to major Internet giants like Yahoo, Amazon, Microsoft, eBay etc. and caused them enormous financial losses [31]. Even though, these losses occur long back, the impact of these attacks still continues. Recent surveys conducted among business and security professional by Corero, Kaspersky Lab Study and Gartner revealed the importance to be given to address these attacks [60, 100, 103]. Therefore, the main intend of this survey is to address detection approaches for DoS/DDoS attacks exclusively.

In the recent years, threats to the network systems have been increasing. Especially, DoS/DDoS attacks have attracted the attention of many network security research groups. Perpetration of DoS/DDoS attacks requires almost no knowledge and inflicts the greatest damage to the victim. Most of the research efforts used DARPA 1998, NSL-KDD, KDD 99 [22, 54, 63] datasets to develop an IDS. These datasets, generated for many years, have been used as benchmark datasets and for performance evaluation of classification algorithms. They were generated in a laboratory set up. The attacks in databases, however, date back to 1999 and are very out of date [80] and cannot actually represent the behavior of the recent DoS/DDoS attacks. But, there are benchmark datasets that contain a huge number of records for recent flooding DoS/DDoS attacks. Therefore, we review the detection approaches that use contemporary datasets containing more recent attack traces. However, there are a few recent surveys on the detection mechanisms for DoS/DDoS attacks [46, 52, 88]. Nonetheless, these mechanisms rely on statistical, data mining, information theoretic, artificial intelligence, entropy-based and cloud-based approaches, but not on deep learning techniques.

As a result, we believe no previous research has offered a systematic overview of deep learning methods used to detect DoS/DDoS attacks. The following are our contributions to this study:

- We classify the DoS/DDoS attacks based on the amount of traffic an attacker injects to bring down a system.
- Since, the existing surveys provide deep learning solutions for generic intrusion activities, we present taxonomy of the cutting-edge deep learning-based solutions for DoS/DDoS attacks.
- We present a comprehensive survey of network and application layer DoS/DDoS attacks and mention the type of models, attacks detected, dataset used by each model.
- Additionally, we discuss recent benchmark datasets that aid in the development of deeper learning based solutions for DoS/DDoS attacks.

- We also present a set of botnet tools used to launch DoS/DDoS attacks.
- We have extensively reviewed more than 100 articles and shortlisted the articles related to the subject of study. We also explore the strengths and limitations of each of the shortlisted defense mechanism, as well as how they compare to one another on a number of different metrics.
- Towards the end of article, we also present the findings from the reviewed articles and the possible extension of work proposed in most of the research efforts.

Even though, there are a few recent surveys on the detection mechanisms for DoS/DDoS attacks [46, 52, 88], but not based on deep learning techniques. Hence, we believe no previous research has offered a systematic overview of deep learning methods used to detect DoS/DDoS attacks. To summarize, we provide researchers with a greater understanding of the DoS/DDoS attacks and defensive mechanisms using deep learning techniques.

3. Review Methodology

In order to identify the research efforts related to the proposed study, we adopted the following search strategies.

1 Identifying the appropriate digital libraries to search for the articles related to the proposed study: The following digital libraries have been searched for.

- Elsevier (https://www.elsevier.com/)
- Science Direct (https://www.sciencedirect.com/)
- IEEE Xplore (https://ieeexplore.ieee.org/)
- Web of Science
- (https://apps.webofknowledge.com/)
- Scopus (https://www.scopus.com/)
- Wiley (https://onlinelibrary.wiley.com/)
- ResearchGate (https://www.researchgate.net/)
- Hindawi(https://www.hindawi.com)
- MDPI (https://www.mdpi.com/
- https://dl.acm.org/conference/ccs/ proceedings/
- https://dblp.org/ (include all conferences)

2 Identifying the key terms related to the proposed study: The key search terms used have been chosen based the subject under study. We have used the search terms such as “DoS attacks”, “DDoS attacks”, “DoS/DDoS attacks” and “Deep Learning” to retrieve the articles for the review. In recent years, deep learning-based identification of DoS/DDoS attacks has piqued researchers' attention. Therefore, publications during the last five years (from 2016 onwards) have been selected. This search has led to a large number of papers, and we sorted out the most relevant articles.

3 Examining the title, abstract and methodology used in the articles downloaded from digital libraries and deciding to include and exclude them for review: The title and abstract of each of the articles downloaded from the digital libraries were examined and shortlisted based on subject under study during the initial selection. For further screening, the methodology and datasets used in the shortlisted articles were investigated. The selection process during the screening includes inclusion and exclusion criteria. Studies that use deep learning algorithms to detect DoS/DDoS attacks exclusively, studies that use deep learning models to detect intrusion detection but including DoS/DDoS attacks, studies that focus on the taxonomy of DoS/DDoS attacks, studies that detect DoS/DDoS attacks in IoT, SDN, and studies that used datasets containing DoS/DDoS traces have all been included. We have excluded the studies that use deep learning model for intrusion detection in general, the studies conducted before 2016 and studies that used NSL/KDD datasets only.

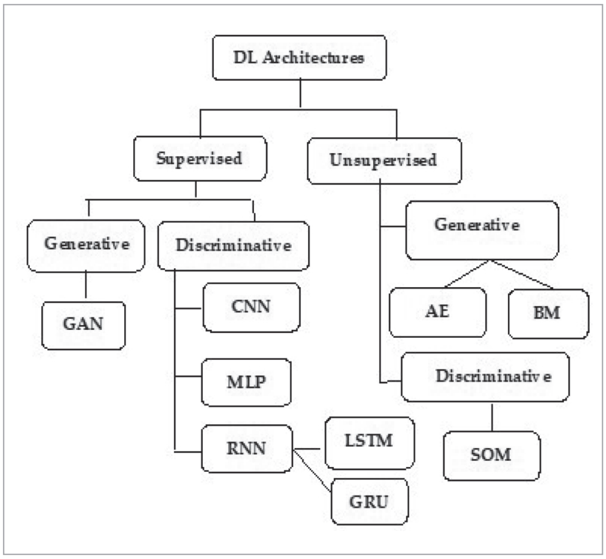
4. Taxonomy of Deep Learning Models for DoS/DDoS Attacks Detection

This section explores the types of DoS/DDoS attacks and commonly used deep learning techniques for detecting these attacks. Architectures for deep learning are represented by a spectrum of options that can be used to develop solutions for a variety of domains. These systems can be either feed-forward focused or recurrent networks that allow for the consideration of previous inputs to be taken into consideration. The following section provides a high-level overview of common deep learning architectures.

4.1. Taxonomy of Deep Learning Models

After reviewing the articles on deep learning models for detecting DoS/DDoS attacks, we classify them based on the nature of learning they use and further on statistical techniques used by them and present the classification in Figure 1.

Figure 1
Taxonomy of Deep Learning Architectures



4.1.1. Nature of Learning

Deep Learning algorithms can be commonly classified into supervised and unsupervised. A supervised learning algorithm is the one which learns from labelled data and predicts the outcome of an unseen data. Unsupervised learning is a type of learning in which a system learns on its own to find knowledge and is mostly used for unlabeled data. Supervised deep learning techniques are used for classification of image and text data, object detection, face recognition etc. whereas unsupervised deep learning techniques are used for word embedding, image encoding into lower or higher dimensional etc. Based on the type of datasets, whether labelled or un-labelled, suitable deep learning techniques have been employed by the researchers for detecting DoS/DDoS attacks.

4.1.2. Statistical Models of Learning

In statistical classification, the deep learning approaches are further classified into generative and discriminative. Generative models are the models which take an input and produce multiple results, commonly in sequence, that is relevant or related to the input, whereas the discriminative models take an input and produce a single result, which is the classification of the input. Thus, generative models are suitable for unsupervised learning and discriminative models are appropriate for supervised learning. Below we present a brief overview of various deep learning approaches.

4.1.3. Multilayer Perceptron

One of the most common types of neural networks is the multilayer perceptron, or MLP. There are one or more layers of neurons in it. The input layer receives data, one or more hidden layers have levels of abstraction, and the output layer makes predictions. MLPs are well suited to classification prediction problems in which inputs are given a class or label, as well as regression prediction problems.

4.1.4. Convolutional Neural Network

A Convolutional Neural Network (CNN) or Convnet is a neural network with a series of layers, each of which uses a differentiable function to translate one volume of activations to another. There are two basic building blocks of CNN namely feature extraction and classification blocks. The feature extraction block has a set of convolution and pooling layers. The classification block has flattening and fully connected layers. Filters represent lower dimensional slices of the input data in a convolutional layer. To create feature maps, the filters convolve the entire input. The feature maps are then sub-sampled and the dimensionality of the feature maps is minimized by the pooling layer [94]. The flattening layer flattens the data into an array so that CNN can read it. Finally, we have fully connected layer having two or three hidden layers and an output layer generally using Softmax classifier that classifies among a large number of classes. CNNs are used as feature extractors and classifiers for intrusion detection, despite their use in image processing and classification. This is due to their ability to work with complex data.

4.1.5. Recurrent Neural Networks

RNNs, or recurrent neural networks, are neural networks that learn sequential data over time steps. The types of inputs and outputs supported are the best way to explain sequence prediction problems. In a typical neural network, each neuron's output is determined by the current input, with no relationship between the input and the neuron's previous output. However, if we want to predict the next word in a sentence, we must recall the previous words in order to do so correctly. Thus, RNN was introduced [69]. Unlike feed forward neural networks, RNN have cyclic connections thus making them more appropriate for modeling sequence of data. As a result, in recent years, RNN has played an important role in machine translation, robot control, time series prediction, speech recognition, speech synthesis, language modeling, human action recognition, intrusion detection, and other areas[9]. Long Short-Term Memory (LSTM) and Gated Recurrent Unit (GRU) are two types of RNN.

LSTM: When training, conventional RNNs face the issue of vanishing gradients. The LSTM algorithm is used to solve this problem. RNN also has a problem with short-term memory. RNN cannot carry information from earlier time steps to later ones for long-term dependencies if a series is long enough. Hence, LSTM is a good choice for sequences with long term dependencies.

GRU: An LSTM without an output gate is known as a GRU. At each time step, GRU is able to write the contents of memory cells to the larger net. The vanishing gradient problem in RNN is also addressed by GRU. Since both are constructed similarly and, in some cases, produce equally excellent results, GRU can be considered a variant of the LSTM.

4.1.6. Auto Encoder

The Auto Encoder (AE) is a kind of neural network with the output layer having the same dimensionality as the input layer [10]. An AE consists of three components:

Encoder: a fully connected, feed-forward neural network that compresses an input into latent space representation. The encoder also encodes the input, mostly images, as compressed representations in a reduced dimension.

Code: a reduced representation of the input that will be fed into the decoder.

Decoder: a feedforward network that reconstructs the input from the code back to its original dimensions.

Stack AE (SAE), sparse AE, and de-noising AE, Convolutional AE, variational AE, Deep AE, Contractive AE, and Undercomplete AE are some of the AE extensions. Dimensionality reduction, image compression and generation, recommendation system, image denoising, feature extraction, sequence to sequence prediction are some of the applications of AE.

4.1.7. Self-organizing Map

Self-organizing Map (SOM) is an unsupervised neural network based on visual clustering that maps high-dimensional data space to low-dimensional space and produces a topological structure that represents all high-dimensional data in low-dimensional representation. SOM and its variants have evolved extensively as potential application candidates in intrusion detection [97]. As intrusion detection can be very well implemented based on topological relationships and new intrusion behaviors can be efficiently detected, SOMs are used extensively.

4.1.8. Boltzmann Machine

A Boltzmann Machine (BM) is a generative deep learning model that consists of one visible layer known as the input layer and one or more hidden layers. It is used for feature learning, dimensionality reduction, regression, classification, and topic modelling, among other things. A BM employs recurrent structure in accordance with stochastic learning processes, which serve as the basis for the optimization techniques used in ANN.

Before moving on to the taxonomy of DoS/DDoS attacks, we provide a brief comparison of various deep learning models presented above. All of the above architectures can be interpreted as a neural network. Even though, MLPs are capable of learning weights that map any input to any output, still they are incapable of capturing sequential information in input data, which is essential for dealing with sequence data. CNNs are the most commonly used deep learning models for computer vision tasks. They operate best when the data comprises of arrays with associated neighbouring values in an array, as is the case with image, video, and sound data. When compared to other deep learning architectures, CNNs have produced very competitive results in other fields, such as natural language processing. CNNs, in particular, are capable of extracting local information from text and analyzing significant semantic and syntactic links between phrases and words. RNNs are frequently used to solve problems involving sequential data, such as voice and language processing or modelling. RNN connections can form cycles. This makes it possible to simulate dynamical changes over time. They are intended to handle data sequences and are the basis for forecast models and language models. Autoencoders, on the other hand, almost never describe the network's topology. The goal is to find a decent neural transformation that will allow the input to be reconstructed. They are made up of encoders (which project the input to a hidden layer) and decoders (which decode the input). A set of latent characteristics or latent factors is learned by the hidden layer. Linear autoencoders learn a number of bases to explain the data's underlying pattern given a dataset. BMs are also a type of neural network. However, the network's interpretation is quite different. BMs perceive the network as a bipartite graph in which the goal is to learn the joint probability distribution of hidden and input variables. They are perceived as a graphical model. The BM is a generative model. It can produce samples based on previously learnt hidden representations. An SOM is a type of artificial neural network that is taught through competitive learning rather than error-correction learning, as is the case with most ANNs.

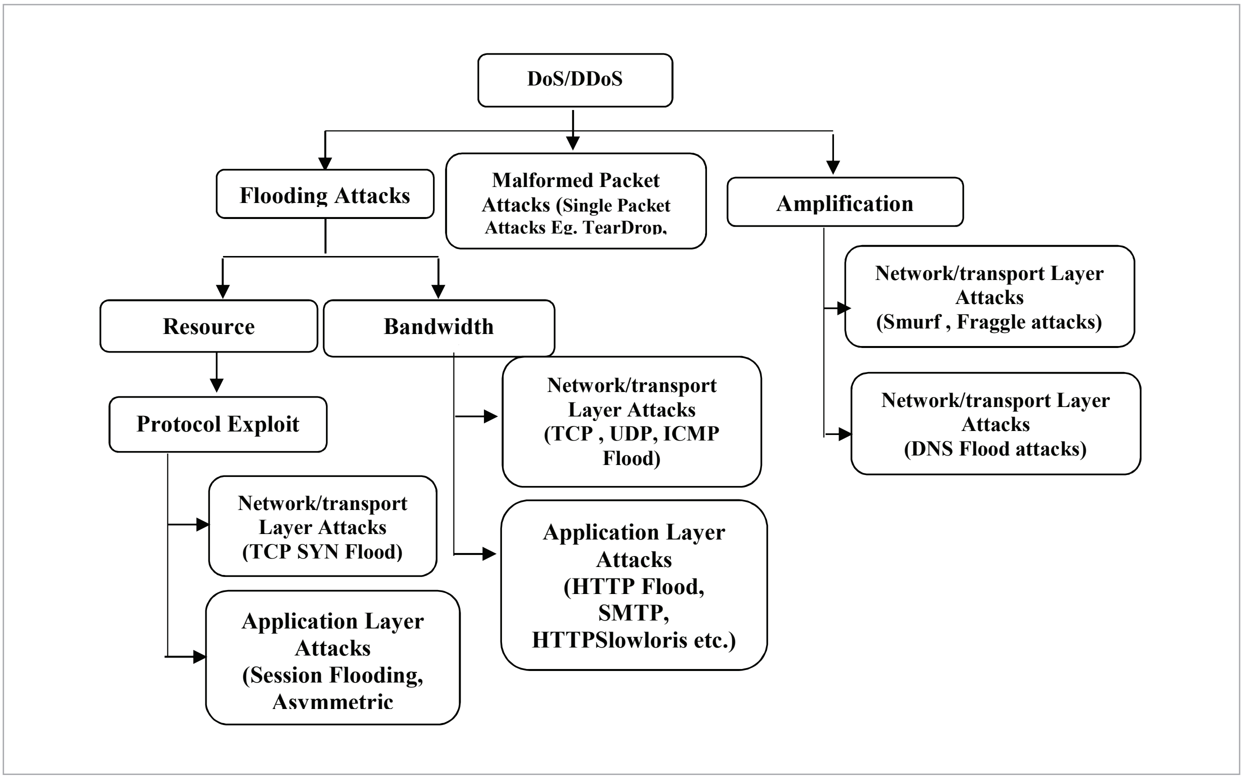
Finding the correct application for a deep learning model is difficult because their application domains are not mutually exclusive. Instead, as the preceding discussion demonstrates, there is significant overlap, and in many circumstances, the best model can only be found through a comparison analysis. One of the key benefits of deep learning is its ability to solve complex problems that necessitate the discovery of hidden patterns in data and/or a thorough knowledge of complex relationships among a large number of interdependent variables. Deep learning algorithms can discover hidden patterns in data on their own, combine them, and create far more efficient decision rules. Due to the advent of graphics processor units, deep learning algorithms have become extremely popular in network security, notably for identifying DoS/DDoS attacks. Based on the learnt patterns, deep learning models can predict normal or abnormal activity. Due to the deep structure of the data, deep learning-based algorithms are good at automatically learning complicated features. As a result, numerous attempts have been made to use deep learning models for the detection of DoS/DDoS attacks.

4.2. Taxonomy of DoS/DDoS Attacks

A DoS/DDoS attacker's primary motivation is to humiliate and degrade a server's infrastructure so that legitimate users are denied access to the services they have requested[64]. Kevin and Chris [64] have identified that the DoS/DDoS attacks exhibit following characteristics: destructive, resource consumption and bandwidth consumption and also highlighted the devastating effects of DoS attacks. Many researchers have tried to classify DoS/DDoS attacks using a number of criteria as discussed in [15, 23, 28, 48, 73, 81, 108, 118]. Mirkovic and Reiher [81] suggested the first comprehensive taxonomy of DoS/DDoS attacks. This taxonomy was based on the characteristics of the attack, the effect on the victim, execution of the attacks etc. Following this, many taxonomies were proposed in different attempts. Manavi [73] has classified the DoS/DDoS attacks into two main groups namely applications layer and network/transport layer attacks. The applications layer attacks are further classified into HTTP flood and SIP flood and network/transport layer attacks are classified into flooding and amplification attacks. Bhatia et al. and he authors of [15, 28] classified the DoS/DDoS attacks into high-rate flooding and semantic attacks. High-rate attacks overload the target by submitting a huge number of bogus queries, whereas semantic attacks take advantage of a protocol's design weaknesses. In addition, the authors also reviewed a few other taxonomies. Kalkan et al. [48] categorized DoS/DDoS attacks based on attack tools (Trinoo, TFN etc). Three major facets of DoS/DDoS attacks, namely the execution approach, the nature and the impact of the attacks were used by [118]. Silva et al. [23] grouped different DoS/DDoS attacks into three types which include application layer attacks, volumetric attacks and resource exhaustion attacks. Sharafaldin et al. [108] presented a comprehensive taxonomy of DDoS attacks, splitting them into reflection-based and exploitation-based attacks. Despite the fact that the current taxonomies of DDoS attacks are comprehensive in and of themselves, [23, 73, 81] have addressed only bandwidth depletion. Still, these efforts did not pay much attention towards attacks on application layer. To fill this gap, in this study, we perform an in-depth examination of recent DoS/DDoS attacks and create a taxonomy that considers both network/transport and application layers attacks. We show a comprehensive taxonomy of DoS/DDoS attacks in Figure 2. The reason for such classi-

Figure 2

Taxonomy of Dos/DDoS attacks


DoS/DDoS
Flooding Attacks
Malformed Packet Attacks (Single Packet Attacks Eg. TearDrop,
Amplification
Resource
Bandwidth
Protocol Exploit
Network/transport Layer Attacks (TCP SYN Flood)
Application Layer Attacks (Session Flooding, Asymmetric
Network/transport Layer Attacks (TCP , UDP, ICMP Flood)
Application Layer Attacks (HTTP Flood, SMTP, HTTPSlowloris etc.)
Network/transport Layer Attacks (Smurf , Fraggle attacks)
Network/transport Layer Attacks (DNS Flood attacks)

fication is to reiterate how danger DoS/DDoS attacks are. Amplification attack uses an amplification factor to multiply its power. The attackers require relatively less resources to cause a significantly greater number of target resources to malfunction or fail. In case of flooding attacks, the attackers themselves send a huge volume of traffic to a victim to bring it down. Single-packet attacks are also known as malformed packet attacks. ICMP Redirect, Teardrop are the types of malformed packet attacks. Tripathi and Hubball [122] described a few well-known DoS/DDoS attacks and their impact on bandwidth and resource consumption. The taxonomy in Figure 2 shows the network/transport and application layer DoS/DDoS attacks. There are a few attacks targeting MAC and Physical layers, but they are generally not flooding attacks. So, we have not considered those attacks in this review.

Network / Transport layer attacks exploit the vulnerabilities of network and transport layer protocols such as TCP, UDP, ICMP. IP spoofing is one such exploitation which uses the inherent weakness of IP protocol. DoS/DDoS attacks targeting application layer intend to deplete the victim servers' resources such as memory, CPU, sockets etc. through flooding of traffic. To deplete resources at the server, the attackers take advantage of weakness of the HTTP/HTTPS protocols over the ports 443 and 80 respectively and try to send traffic to consume the resources. Session flooding, asymmetric flooding attacks etc. are such type of attacks [114]. Bandwidth attacks will consume the bandwidth of the server by keeping them engaged. For example, an attacker might submit an HTTP request to download a large file, using all usable bandwidth and stopping the server from servicing other legitimate users. Get/Post request flooding attack is one such type of attacks. Current research and challenges in detecting these attacks are presented in [111]. In order to detect these attacks, there are several approaches elaborated in [88]. And, these approaches do not cover deep learning methods. However, DoS/DDoS detection approaches using deep learning are proposed by [44] and this work covered the approaches proposed till 2016. But, in this study, we review the very recent research works (up to 2021) on the detection of DoS/DDoS attacks using deep learning techniques.

5. Datasets for DoS/DDoS Attacks

This section presents a brief overview of benchmark datasets for DoS/DDoS attacks, considering the evolving nature of the attacks. The choice of datasets plays a crucial role in the validation of DoS/DDoS detection approaches. Also, the size of the dataset plays a significant role in deep learning models. There are a few publicly accessible datasets that have been commonly used as benchmark datasets, such as DARPA, KDD, NSL-KDD, and others. This section addresses existing datasets that are used to construct a detection system, as well as a description of these datasets. Datasets can usually be obtained in two ways namely real time traces and publicly available datasets. For collecting real time traffic trace, tools like Winshark are used. Generally, research groups create a testbed environment to collect real time traffic. In order to create DoS/DDoS attacks, botnets may also be employed. Botnets are collection of internet-connected devices which are controlled by an attacker without the administrator's knowledge. By gaining the control of massive distributed devices, attackers can perpetrate DoS/DDoS attacks against a specific target. BASHLITE and Mirai [61, 93] are two such botnets. These two botnets are especially used for compromising IoT devices to launch DoS/DDoS [77]. There are simulator tools like BoNeSi to generate a few types of attacks including UDP flood attacks, ICMP flood attacks and TCP SYN attacks [59]. These methods of generating dataset are suitable for collecting short-term or small amounts of data. For large volume of data, long-term data collection is to be carried out. The remaining part of this section deals with DoS/DDoS attack datasets that are accessible over the Internet. We especially give review of the datasets that are used by the deep learning approaches for detecting these attacks.

EPA-HTTP (Environmental Protection Agency-Hypertext Transfer protocol): The logs for this dataset were collected in 1995 and contain the traces of HTTP requests. Johnson et al. [47] used this dataset to detect HTTP DoS attacks. As it was a very old dataset and contains a smaller number of features, recent attempts have not used this dataset.

The CAIDA ″DDoS Attack 2007″ Dataset: This is one of the first datasets used in an intrusion detection system. This dataset includes approximately one hour of anonymized DDoS attack traffic traces. This DDoS attack prevented access to the targeted server by using all of the server's processing resources as well as the entire bandwidth of the network connecting the server to the Internet. These traces only contain attack traffic to the victim and victim responses to the attack [17]. We found that some of recent research works [18, 44] use this dataset for detecting DoS/DDoS attacks. However, the CAIDA DDoS dataset does not adequately reflect the various types of attacks that may occur. For instance, the DDoS attack databases only include spoofed-source DDoS attacks and exclude other types of DDoS attacks [34].

DARPA 1998: MIT Lincoln Labs prepared and managed the DARPA Intrusion Detection Evaluation Program in 1998 [4]. The aim was to survey and evaluate intrusion detection research. The dataset contains four types of attacks: DoS, U2R, R2L, and Probe. Furthermore, this dataset does not reflect real-world network traffic. The dataset is outdated for successful IDS evaluation on modern networks.

KDD CUP 99: This dataset has been a well-known benchmark in the research of IDSs. It covers more than 20 different forms of attacks, like DoS. Despite the fact that this dataset was preferred by the researchers at the time, it has many flaws, including duplicated samples, unbalanced groups, and a lack of coverage of the most recent attack forms.

NSL KDD: NSL KDD dataset is an improvement over KDD Cup 1999 dataset since KDD CUP 99 contains huge number of redundant records making difficult to process the data accurately. This dataset has the same attributes as KDD CUP 99. The data in NSL-KDD dataset is either labelled as normal or as one of the 24 different kinds of attacks. These 24 attacks can be grouped into four classes: Probe, DoS, R2L, and U2R. Though, most of the issues in KDD Cup 99 have been addressed, this dataset still lacks newer attack types and it dates back to the year 1998/1999.

UNB ISCX 2012: The ISCX dataset was generated in a testbed for seven days. A systematic approach is used to generate an attack detection dataset which incorporates HTTP DoS, DDoS and Brute Force SSH attacks [53]. This dataset includes new DoS attack types. While KDD CUP99/NSL datasets were commonly used to test IDS techniques, they are now too old to represent modern-day traffic and attacks. In comparison, ISCX 2012 is more up to date and relevant.

CICIDS2017 and CICIDS2018: These datasets contain benign and up-to-date common attacks that approximate true real-world data [45]. A testbed environment exercising HTTPS, HTTP, SMTP, POP3, IMAP, SSH, and FTP protocols has been created to collect the traffic traces. Variants of DoS attacks (DoS Slowloris, DoS Slowhttptest, Hulk, GoldenEye), web attacks, infiltration attacks, Brute Force attacks are covered in the datasets. These datasets possess characteristics like heterogeneity, attack diversity etc. that are required for creating a reliable benchmark dataset. This dataset, in particular, contains application layer DoS attacks as well as data describing high-volume traditional DoS attacks.

UNSW-NB15: The UNSW-NB15 dataset's network packets were created in the Australian Centre for Cyber Security's Cyber Range Lab using the IXIA PerfectStorm tool, which generated real modern normal activities and synthetic contemporary attack behaviours [89]. Fuzzers, Analysis, Backdoors, DoS, Exploits, Generic, Reconnaissance, Shellcode, and Worms are among the nine types of attacks in this dataset. The Argus and Bro-IDDSL tools are used, along with twelve classifier algorithms, to produce 49 features in this dataset. A total of 49 attributes determining the features of connections present for each data instance. The major drawback of this dataset is that the existence of several missing samples.

USTC-TFC2016: There are ten different forms of malware traffic in this dataset, which was obtained from a real network environment between 2011 and 2015 [41, 42]. There are also ten categories of benign, natural traffic that were collected using IXIA BPS, a network traffic simulation equipment. The USTC-TFC2016 dataset is 3.71 GB in size and in pcap format.

TUIDS (Tezpur University Intrusion Detection System): TUIDS intrusion dataset, TUIDS coordinated scan dataset, and TUIDS DDoS dataset are real-world intrusion datasets [16]. TUIDS intrusion dataset contains 22 distinct attack types (like smurf, fraggle). The coordinated scan dataset includes six attack types (like UDP scan) and six attacks (like DDoS attacks) were included in DDoS dataset. The above datasets were generated by establishing a testbed with 250 clients and a few routers.

CIDDS-001/002 (Coburg Intrusion Detection Dataset): The main goal of CIDDS is to build evaluation datasets for anomaly-based network intrusion detection systems and to generate customizable and up-to-date datasets. For generating malicious traffic, DoS attacks, Brute Force attacks and Port Scans were executed within the network [75]. An external server with publicly accessible IP address has been used to include actual network traffic thus exposing the server to real and up-to-date attacks from the internet.

CICDDoS2019: This dataset contains benign and up-to-date popular DDoS attacks, and it closely resembles real-world data. It contains the results of a network traffic analysis performed with CICFlowMeter-V3 and labeled flows based on the time stamp, source and destination IP addresses, source and destination ports, and other factors [20]. This dataset contains traffic traces from a variety of modern reflective DDoS attacks, including PortMap, NetBIOS, LDAP, MSSQL, UDP, UDP-Lag, SYN, NTP, DNS, and SNMP. Table 1 provides a summary of the datasets used by the research efforts reviewed in this study.

All the above datasets have been used in various research works, which we present in Section 6. The reason for having variety of datasets is that the behaviour and pattern of attacks by the intruders change, that is, intruders evolve over the period of time. So, it is imperative to shift from the static and one-time datasets to dynamically generated real-time datasets. Such datasets will reflect the actual composition of traffic and invade attempts carried out by the attackers. Hence, a systematic approach for generating real-time dataset to develop DoS/DDoS attacks detection approach and to analyze, test and evaluate the same is necessary. Such an attempt has been made by [16].

Table 1
Summary of datasets for DoS/DDoS attacks traffic traces

Year	Dataset	Target Layer(s)	Types of attacks	Limitations
1995	EPA-HTTP [47]	Application layer	HTTP DoS	Contains only the traces of HTTP DoS attacks.
1998	DARPA [22, 53, 72, 91]	Network/Transport layers	SYN Flood, UDP Flood, Smurf etc.	Because the DARPA dataset is made up of raw files, researchers must extract features from them in order to use them in machine learning algorithms.
1999	KDD CUP 99 [54]	Network/Transport layers	DoS, Probe, R2L, U2R	There are duplicate and redundant records. It is a heavily skewed dataset containing attack instance records from recent malware attacks, as well as a large number of redundant records.
1999	NSL KDD [63]	Network/Transport layers	DoS, Probe, R2L, U2R	Despite the fact that NSL KDD 99 addresses the redundancy in the KDD CUP 99 dataset, the results are unsatisfactory because they do not reflect current trends in normal and attack traffic.
2007	CAIDA [17, 56, 112]	Network/Transport layers	DDoS	The attacks in the CAIDA dataset are not diverse. Furthermore, the gathered data lacks features from the entire network, making it difficult to distinguish between abnormal and normal traffic flows.
2012	ISCX 2012 [43, 45, 56, 107]	Application and Network/Transport layers	HTTP DoS attacks, IRC Botnet attacks, Brute Force SSH, unknown TCP and ICMP attacks, attacks by exploiting SMTP, IMAP, DNS	Nearly 70% of today's network traffic is HTTPS and this dataset contains no HTTPS traces. Furthermore, the distribution of the simulated attacks does not correspond to real-world statistics. High class imbalance
2012	TUIDS [16, 56]	Network/Transport layers	22 types of attacks	High class imbalance
2015	UNSW NB15 [34, 107]	Network/Transport layers	TCP attacks, UDP attacks, attacks by HTTP, FTP, SMTP	High class imbalance
2017	CICIDS2017/2018 [2, 92, 119]	Network/Transport layers	DoS Slowloris, DoS SlowHTTPTest, DoS Hulk and DoS GoldenEye, DDoS-LOIC	High class imbalance. The data samples from network flow analysis are saved in files, and processing these files is a time-consuming task due to the large number of data instances in each file.
2017	CIDDS 001/002 [56, 123]	Application Layer	HTTP DoS	High class imbalance
2018	BoT-IoT [62]	Application and Network/Transport layers	DoS TCP, DoS UDP, DoS HTTP	-
2019	CICDOS2019 [20, 40]	Application and Network/Transport layers	SYN flood attacks, MSSQL attacks, UDP-Lag, LDAP attacks, UDP flood attacks, PortScan, and NetBIOS attacks, WebDDoS attacks, SSDP	High class imbalance

6. Deep Learning Solutions for DoS/DDoS Attacks

Various research attempts have been carried out for the detection of DoS/DDoS attacks using Deep Learning approaches. Since 2015, deep learning techniques have been explored for developing techniques to detect DoS/DDoS attacks. This survey considers the research articles published from 2016 to till date. This section contains a brief summary of each of the research papers. We group the articles reviewed based on the types of DoS/DDoS attacks they detect (network/transport or application layer or both), nature of learning, (supervised or unsupervised) and statistical model of learning, namely generative or discriminative.

Due to the devastating impacts of DoS/DDoS attacks, the security research community has paid its attention on the mitigation techniques for these attacks. Since the appearance of DoS/DDoS attacks, there were many solutions to prevent, detect and alleviate these attacks and approaches based on Data mining, Soft Computing, Machine learning etc. Recently, the field of deep learning has made a remarkable progress in several applications like image recognition, computer security, and speech recognition.

Hence, several variants of deep learning techniques have been built to detect DoS/DDoS attacks. First, we summarize the recent research works that use deep [58]learning approaches for detecting application layer DoS/DDoS attacks only.

6.1. Deep Learning Approaches for Application Layer Attacks

Johnson et al. and Asad et al. [11, 47] proposed a MLP based classification model with Genetic Algorithm (GA) for detecting the application layer DoS/DDoS attacks. The proposed algorithm is a supervised, discriminative in nature. The only difference between the two efforts lies in the use of datasets only. Johnson et al. [47] used datasets from the EPA-HTTP, CAIDA 2007, DARPA 2007, BoNeSi-based datasets, and the experimentally generated dataset. Asad et al. [11] used the EPA-HTTP dataset, which included HTTP logs from a web server, the CAIDA 2007 dataset, and a Slowloris attacks dataset. These two studies used different metrics to illustrate the proposed system's efficacy, which are presented in Table 2.

A detection approach based on AE has been proposed in [12, 104, 130] which are unsupervised, generative algorithms. CICIDS2017 and an environment that generated realistic traffic patterns were used to evaluate accuracy and detection rate of application layer flooding DoS/DDoS attacks like slowloris, slowpost, session flooding, asymmetric attacks etc. There are a few research works based on ANN with more number of layers leading to deep models[71, 74, 78, 90, 105]. In addition, Odusami et al. [90] also implemented Naive Bayes, Linear Discriminant Analysis (LDA) and variational AE. This attempt used CIDDS-001 dataset to detect HTTP DoS attacks. Yao et al. and Asad et al. [11, 130] used CICIDS2017 dataset. Benzaïd et al. [12] focused the detection of DoS/DDoS attacks in Software Defined Networks (SDN). Unlike general feed forward network types, LSTMs have feedback connections and do not only process images, but also entire sequences of data. This is because of its property to remember patterns for long time. So, recently there are a few research activities which use RNN and LSTM for DoS/DDoS attacks detection. [71, 90, 104, 105] mainly used LSTM which is an RNN based deep learning model. These efforts fall under supervised learning algorithms. Furthermore, Roopak et al. [104] also implemented MLP, CNN, LSTM with CNN, which make this work generative too. The datasets used were CICIDS2017 and CAIDA. All the datasets used in these efforts contain HTTP and its related attacks only. A work by Manimuruagn et al. Manimurugan et al. [74] explored the use of Deep Belief Neural(DBN) for developing a system for detecting application layer attacks. Meng et al. [78] attempted to use statistical methods to develop a system for detecting CPU exhaustion attacks in web applications.

6.2. Deep Learning Approaches for Network/Transport Layer Attacks

As attention paid towards detecting application layer DoS/DDoS attacks, several attempts have been made for detecting network/transport layer attacks. The research attempts by Ghanbari et al., Hussain et al. and Singh et al. [32, 39, 111] proposed CNN based network/transport layer DoS/DDoS attacks detection approaches and used their own generated traffic traces. These approaches are supervised and discriminative in nature. These CNN based techniques used multiple hidden layers leading to deep neural networks which help the systems learn better. An unsupervised and generative learning method was proposed by [35, 77, 82]. The authors generated their own real time traces by establishing a test-bed in their laboratories and detected network/ transport layer DoS/DDoS attacks. AE based deep learning technique was employed in these attempts. The authors of [76, 93, 96] proposed LSTM based detection method which successfully detects the DoS/DDoS and they are supervised and generative learning algorithms. These approaches used botnet/tools to create traces for DoS/DDoS attacks. Saied et al. [106] suggested a supervised, discriminative ANN which used real time traffic pattern generated using a simulator. This approach detected TCP, UDP and ICMP DDoS attacks. And, Min et al. [80] proposed stacked SOM, an unsupervised feature dynamic deep learning method that uses ISP-collected netflow data to tackle the dynamic nature of novel DoS/DDoS attacks. BoNeSi simulator tool has been used in this attempt to produce three types of attacks: UDP flood attack, ICMP flood attack, and TCP SYN attack. Premkumar and Sundararajan [95] proposed a deep neural model based on the Radial Basis Function for designing an IDS that detects network/transport layer attacks such as jamming, misbehaviour, black hole, flooding, and so on.

6.3. Deep Learning Approaches for Application Layer and Network/Transport Attacks

Next, we cover the mechanisms that detect both application and network/transport layer DoS/DDoS attacks. There are quite a large number of research works carried out for detecting both types of attacks and a brief survey of these works is presented below. First, we find that there are a few efforts using DNNs [5, 19, 51, 117] for detecting DoS/DDoS attacks. These attempts were using UNSW-NB15/ AWID, UNSW-NB15/ CICIDS2017, CIDDS-001, BoT-IoT datasets for developing the detection system and testing the same.

RNN/LSTM based detection mechanisms are proposed to model flow sequences [14, 25, 42, 58, 67, 98, 110, 131]. These research efforts used ISCX 2012, DARPA 1998, USTC-TFC2016, CAIDA, CICDDoS2019 datasets and real time traffic traces to learn network behaviors and further to detect DoS/DDoS attacks. Even though, the ISCX dataset is labelled, [98] detected patterns of malicious activity without the assistance of labelled datasets, that is, it is developed as an unsupervised learning algorithm. But all the other attempts are supervised learning and generative, as they used RNN as their basic deep learning technique. In addition, the authors of [58] also implemented a basic neural network architecture and compared with RNN/LSTM in order to illustrate the power of RNN/LSTM.

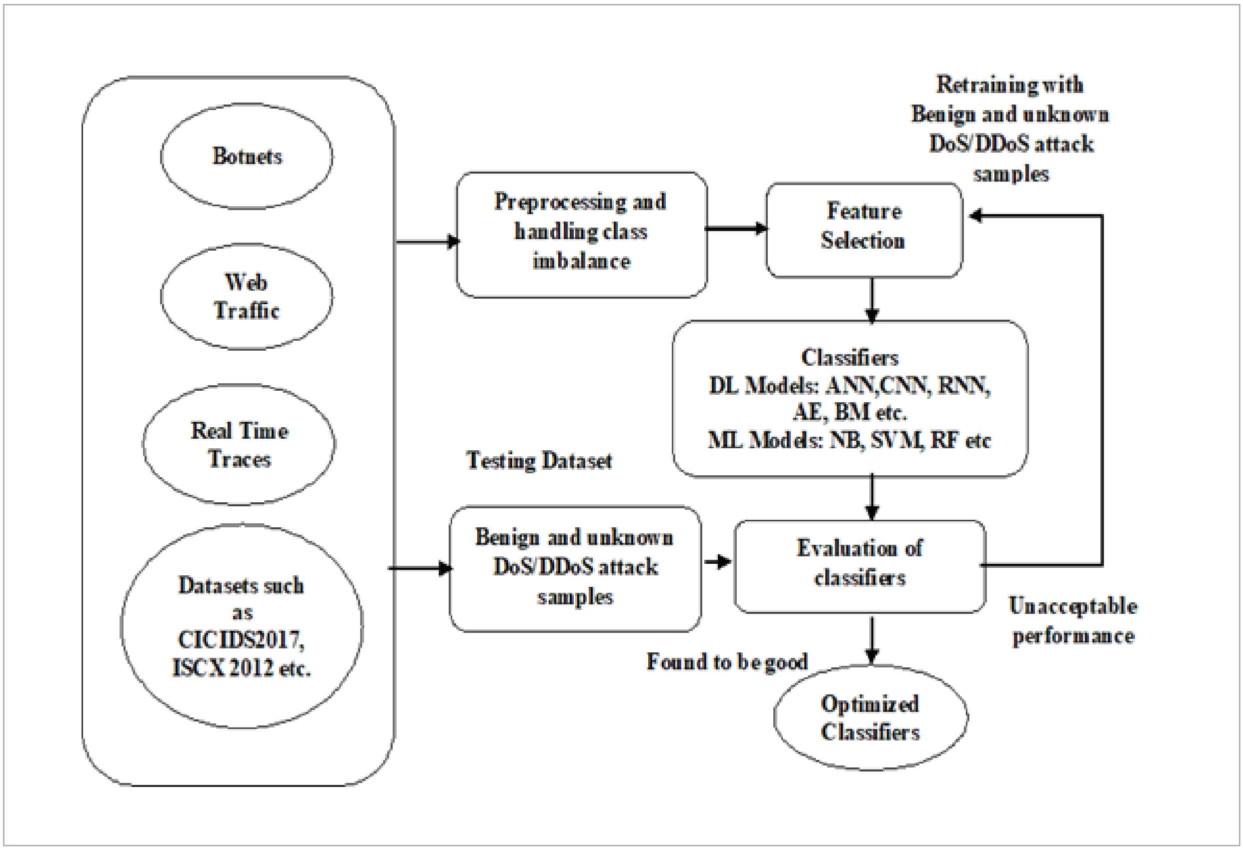
Even though, CNNs have been recognized as suitable for image processing, they were not exploited in the field of IDSs. As the researchers believed that CNNs can make a difference in intrusion detection especially in DoS/DDoS attack detection, they attempted to use CNN to overcome the low detection rates in conventional approaches. Doriguzzi-Corin et al. , Kim et al. and min et al. [24, 57, 80] used CNN to extract the features from the datasets to build a detection system[68]. The datasets ISCX 2012, KDD CUP, CIC2017 and CIC2018 have been used in these attempts and all are labelled. Hence, all these approaches follow supervised learning and are discriminative.

Some research attempts were performed considering both CNN and RNN/LSTM [46, 104, 105]. As all these approaches use both CNN and RNN, they are considered to be both discriminative and generative. They used different datasets like ISCX 2012, DARPA and their own traffic datasets and moreover, botnets like Mirai and BASHLITE have been used to create DoS/DDoS attacks. Based on the nature of datasets, they act either as supervised or unsupervised learning technique.

In addition, the authors of [29, 116] used multiple deep learning models to evaluate the performance of each of them against detecting the DoS/DDoS attacks and suggested the model which gives better performance. In this survey, we also reviewed the attempts which used AE and published between 2018 and till date [52, 108-118]. In these attempts, the auto encoders have been used either for feature extraction or classification. The AEs are unsupervised learning algorithms and generative models. CICDDoS2019, CSECICIDS 2018 and ISCX2012 have been the datasets used in these techniques in addition to real time traces. Additionally, botnets like Mirai, BASHLITE have been used to launch DoS/DDoS attacks. In comparison to other methods like CNN, LSTM, and other machine learning algorithms like Support Vector Machine, Random Forest, Logistic Regression, and many others, the authors of these efforts claim that accuracy, precision, and other performance metrics show bet-

Figure 3

Architecture for detecting DoS/DDoS attacks using deep learning models


Botnets
Web Traffic
Real Time Traces
Datasets such as CICIDS2017, ISCX 2012 etc.
Preprocessing and handling class imbalance
Feature Selection
Retraining with Benign and unknown DoS/DDoS attack samples
Classifiers
DL Models: ANN,CNN, RNN, AE, BM etc.
ML Models: NB, SVM, RF etc
Testing Dataset
Benign and unknown DoS/DDoS attack samples
Evaluation of classifiers
Unacceptable performance
Found to be good
Optimized Classifiers

ter values. After reviewing the articles, we tend to generalize the architecture followed by the reviewed articles to detect DoS/DDoS attacks and present it in Figure 3.

As can be seen in Figure 3, the articles gather the datasets from heterogenous sources like web traffics, Botnets, evaluation datasets provided by different organizations etc. Since the models proposed in the reviewed articles include machine learning models in addition to deep learning models, pre-processing is also shown in Figure 3. The datasets have been divided into training (with/ without validation sets) and testing sets with different ratios like 80-20 / 70-30 etc. The models have been trained using training datasets and evaluated for their performance using testing datasets. If the evaluation is found not to be acceptable, the retraining happens with new samples. Table 2 provides a comprehensive comparison of all recent research activities undertaken between 2016 and the present.

7. Discussion and Findings

Even though deep learning concept has been around long back, the real time applications of deep learning to large-scale started about 2010. Since then, deep learning finds its application in many spheres. The exploration of deep learning methods for intrusion detection has also started since the beginning of this decade. There are very recent surveys related to the application of deep learning for intrusion detection [34]. But, these surveys cover general intrusion detection only. Imamverdiyev and Abdullayeva [44]

Table 2
Summary of the Deep Learning based DoS/DDoS attacks detection approaches

S.No	Authors and Year	Models used	Nature of learning	DL types	Dataset	Attacks detected	Advantages / characteristics
				Deep learning algorithms that detect Application layer DoS attacks			
1.	Johnson et al. [47] (2016)	Multilayer Perceptron with Genetic Algorithm back propagation	Supervised	Discriminative	EPA-HTTP datasets	Slowloris attack, HTTP GET flooding request	Live DoS attack detection
2.	Zolotukhin et al. [133] (2016)	1. Clustering algorithms (for dividing extracted feature vectors into clusters) 2.Stacked auto-encoder for classification.	Unsupervised	Generative	RGCE, a Real time dataset	Slowloris and Slowpost	a realistic cyber environment to generate realistic traffic, detection of all conversations related to DoS attacks in the real time traffic
3.	Yadav and Subramanian [129] (2016)	1. Stacked Auto Encoder (feature learning) 2. Logistic Regression (classification)	Unsupervised	Generative (SAE) and Discriminative (LR)	Real time dataset	Request Flooding attacks, Session Flooding attacks, Asymmetric Attacks	Classification of different types of application layer attacks.
4.	Singh and De [113] (2017)	Multilayer Perceptron with a Genetic Algorithm (MLP-GA)	Supervised	Discriminative	EPA-HTTP datasets, CAIDA 2007	Slowloris attack	minimum False Positive when compared with traditional classifiers
5.	Abdulhammed et al. [1] (2018)	1. DNN (3 variations) 2. Random Forest, 3. Voting Technique, 4. Stacking technique with LDA, NB and OneR	Supervised	Discriminative and Generative	CIDDS-001 (Benchmark for HTTP DDoS detection systems)	HTTP DoS	Ability to handle imbalanced class distribution with a smaller number of samples.
6.	Yao et.al. [130] (2018)	Graph-based feature learning algorithm with Random Forest Regressor	Supervised	Discriminative	CIC IDS 2017	slowloris,DoS Slowhttptest, DoS Hulk, DoS GoldenEye	Traffic patterns are modelled as attributed graph to achieve space efficiency

Table 2 (continued)

S.No	Authors and Year	Models used	Nature of learning	DL types	Dataset	Attacks detected	Advantages / characteristics
7.	Asad et al. [11](2019)	Artificial Neural Networks	Supervised	Discriminative	CIC IDS 2017	DoS Slowloris, DoS SlowHTTPTest, DoS Hulk and DoS GoldenEye	Ability to detect a malicious behaviour from an entirely new malicious pattern. Usage of the most relevant high-level features of packet flows
8.	Roopak et al. [104] (2019)	1. MLP, 2.1d-CNN, 3.LSTM 4. CNN+LSTM	Supervised	Discriminative	CIC IDS 2017	slowloris,DoS Slowhttptest, DoS Hulk, DoS GoldenEye	Compared the performance of machine and deep learning algorithms
9.	Odusami et al. [90] (2019)	LSTM	Supervised	Discriminative	CAIDA	AL DoS	Detecting low-rate and high-rate L7DDoS attacks.
10.	Benzaïd et al.[12] (2020)	MLP with more hidden layers	Supervised	Discriminative	CIC IDS 2017	HTTP Hulk, HTTPslowloris	Ability to mitigate adversarially generated attack flows
11.	Kasim [50] (2020)	AE with SVM	Unsupervised	Generative	CIC IDS 2017 and NSL KDD	slowloris,DoS Slowhttptest, DoS Hulk, DoS GoldenEye	Ability to handle unlabeled and unbalanced DDOS traffic
12.	Muraleedharan and Janet [83](2020)	A fully connected feed forward deep network	Supervised	discriminative	CIC IDS 2017	slowloris,DoS Slowhttptest, DoS Hulk, DoS GoldenEye	Ability to prevent slow DoS attacks before it reaches the victim. Can be used in any web server without configuration changes at server
13.	Sabeel et al. [105] (2020)	DNN and LSTM	Supervised	Discriminative	CIC IDS 2017 and ANTS2019 (real time dataset)	slowloris,DoS Slowhttptest, DoS Hulk, DoS GoldenEye	Generated synthetic dataset to mimic real life attacks and detected them.
14.	Liu et.al. [71] (2020)	CNN and LSTM	Supervised	Discriminative	CIC IDS 2017	slowloris,DoS Slowhttptest, DoS Hulk, DoS GoldenEye	Prediction model for anomaly traffic of future networks.
15.	Manimuruga et al. [74] (2020)	DBN for classification	Unsupervised	Generative	CIC IDS 2017	slowloris,DoS Slowhttptest, DoS Hulk, DoS GoldenEye	Ability to detect different types of attacks in IoT systems
16.	Meng et al. [78] (2017)	Anomaly detection models using statistical methods for classification	Unsupervised	Generative	Real-time data by runiing web applications	CPU Exhaustion	Ability to adaptively synthesizes and updates filtering rules to block future attack requests

Table 2 (continued)

S.No	Authors and Year	Models used	Nature of learning	DL types	Dataset	Attacks detected	Advantages / characteristics
17.	Saied et al. [106] (2015)	ANN	Supervised	Discriminative	simulated using Java Neural Network Simulator (JNNS)	NL/TL DoS (TCP; UDP and ICMP DDoS attacks)	Trained, deployed and tested the solution in a physical environment. Reduce the strength of the attack before it reaches the victim
Deep learning algorithms that detect Network / Transport layer DoS attacks							
18.	Ghanbari and Kinsner [32] (2018)	CNN and SVM	Supervised	Discriminative	CAIDA 2007	NL/TL DoS	Ability to detect anomalous behavior in real time and in various environments
19.	McDermott et al. [76] (2018)	Bidirectional Long Short Term Memory based Recurrent Neural Network	Supervised	Discriminative	Real time dataset and Mirai Botnet to create DoS attacks.	UDP flood, TCP Flood, Acknowledgement flood, Domain Name System (DNS) flood, SYN flood attacks	Generated own dataset using Mirai Bots. A progressive model that can evolve over the time.
20.	Meidan et al. [77] (2018)	Auto Encoder for feature extraction and classification	Unsupervised	Generative	Real traffic dataset infected by Mirai and BASHLITE Botnets	UDP flood, TCP Flood, Acknowledgement flood, SYN flood attacks	ability to learn complex patterns and thus provide very low false alarms.
21.	Priyadarshini ans Barik [96] (2019)	LSTM (with 1,2,3 hidden layers) in Software Defined Networks	Supervised	Discriminative	Data from CTU-13 Botnet and ISCX 2012 datasets	TCP, UDP and ICMP protocols attacks	Ability to block the traffic at the earliest possible using a Fog server
22.	Ko et al. [59] (2019)	Stacked SOM (classification)	Unsupervised	Discriminative	BoNeSi simulator tool to generate t UDP flood attack, ICMP flood attack and TCP SYN attack	UDP flood attack, ICMP flood attack and TCP SYN attack	uses the Apache Spark framework for fast distributed computation to provide horizontal scalability in the face of large-scale attacks
23.	Hussain et al. [39](2020)	Deep CNN residual network with 50 layers (ResNet-50) and deep rudimentary CNN (DRC) model having 6 layers	Supervised	Discriminative	an open dataset released by Telecom Italia	Silent call attack, Signaling attack, SMS flooding attack	Detects the attacks in 5G Cyber Physical Systems.

Table 2 (continued)

S.No	Authors and Year	Models used	Nature of learning	DL types	Dataset	Attacks detected	Advantages / characteristics
24.	Guo et al. [35] (2020)	Autoencoder	Unsupervised	Generative	real time data captured from certain Virtual IP addresses	UDP and TCP flows	Ability to handle real-world DDoS Traffic from a large commercial cloud platform. Detect anomalies on unordered and noisy features with high recall
25.	Premkumar and Sundararajan [95] (2020)	Deep Learning-based Defense Mechanism	Unsupervised, but linear perceptron used in supervised manner.	generative	Real time data colelcted from sensors	jamming, misbehavior, black hole, flooding, desynchronization, and homing attack	Maintains flexibility in the framework structure during different DoS attack defense
26.	Mirsky et al. [82](2018)	Ensemble of neural networks (Autoencoders) for classification	Unsupervised	Generative	Synthesized data using the tools like Nmap, Sfuzz	SSDP flood, SYN DoS, SSL Integration	Improved run time performance ensemble of small autoencoders
27.	Gadze et al. [30](2021)	LSTM and CNN	Supervised	Discriminative	Dataset generated using Mininet and Floodlight	TCP, UDP, and ICMP flood attacks	Ability to detect and mitigate DDoS attacks in SDN environment
28.	Wang et al. [125] (2017)	HAST-IDS includes CNN (to learn low-level spatial features) and LSTM (to learn high-level temporal features)	Supervised	Discriminative	DARPA1998 and ISCX2012	BFSSH, HttpDoS, DDoS(TCP, ICMP)	Ability to learn the spatial and temporal features of a long sequence of data.
Deep learning algorithms that detect Application and Network / Transport layer DoS attacks							
29.	Yuan et al. [131] (2017)	LSTM,CNN-LSTM, GRU, 3LSTM	Supervised	Discriminative	ISCX 2012	HTTP DoS attacks, IRC Botnet attacksS, Brute Force SSH, unknown TCP attacks, ICMP attacks, attacks by exploiting SMTP, IMAP, DNS	Ability to learn much longer historical features than conventional machine learning methods.

Table 2 (continued)

S.No	Authors and Year	Models used	Nature of learning	DL types	Dataset	Attacks detected	Advantages / characteristics
30.	Min et al. [80] (2018)	Word embedding and text convolutional neural network (Text-CNN) for feature extraction and Random Forest for classification.	Supervised	Discriminative	ISCX2012	HTTP DoS attacks, IRC Botnet attacks, Brute Force SSH, unknown TCP attacks, ICMP attacks, attacks by exploiting SMTP, IMAP, DNS	Resistant to noise and does not overfit. Computationally efficient and can run on large-scale datasets with high dimensions ability to handle unbalanced datasets
31.	Li et al. [67] (2018)	Recurrent Neural Network (RNN) with Restricted Boltzmann Machines (RBM)	Supervised	Discriminative	ISCX-2012 and DARPA 1998	HTTP DoS attacks, IRC Botnet attacksS, Brute Force SSH, unknown TCP attacks, ICMP attacks, attacks by exploiting SMTP, IMAP, DNS	Ability to support streaming type of data.
32.	Cui et al. [21](2018)	Word embedding (feature selection) and DNN for classification	Supervised	Discriminative	ISCX 2012	HTTP DoS attacks, IRC Botnet attacks, Brute Force SSH, unknown TCP attacks, ICMP attacks, attacks by exploiting SMTP, IMAP, DNS	Ability of dimension reduction and learning features from data with sophisticated structure.
33.	Li, et al. [68] (2018)	Recurrent neural network (RNN),long short-term memory (LSTM), and convolutional neural network (CNN)	Supervised	Discriminative	ISCX2012	HTTP DoS attacks, IRC Botnet attacks, Brute Force SSH, unknown TCP attacks, ICMP attacks, attacks by exploiting SMTP, IMAP, DNS	Simplifies the real-time update of detection system. Reduces the degree of dependence on environment.
34.	Kim [58] (2019)	a basic neural network (BNN) and a long short-term memory recurrent neural network (LSTM RNN)	Supervised	Discriminative	CAIDA 2007, DARPA 1998, Real time data	HTTP Flood, SQL Injection Distributed Denial of Service (SIDDOS), UDP Flood, and Smurf attacks	Fast learning convergence due to hyper-parameter optimization.

Table 2 (continued)

S.No	Authors and Year	Models used	Nature of learning	DL types	Dataset	Attacks detected	Advantages / characteristics
35.	Hwang et al. [42](2019)	Word embedding to extract the features and LSTM for classification.	Supervised	Discriminative	ISCX2012, USTC-TFC2016, collected two datasets from Mirai botnet	HTTP DoS attacks, IRC Botnet attacks, Brute Force SSH, unknown TCP attacks, ICMP attacks, attacks by exploiting SMTP, IMAP, DNS , TCP ACK flood, TCP SYN flood, UDP flood	Does not require pre-process packets into flows, thus boosting detection speed.
36.	Doriguzzi-Corin et al. [24] (2020)	CNN	Supervised	Discriminative	ISCX2012, CIC2017 and CSECIC2018	DoS slowloris, DoS Slowhttptest, DoS Hulk, DoS GoldenEye, BFSSH,HttpDoS, DDoS(TCP, ICMP)	Reduced feature engineering process and processing time. Suitable in resource constraint environment.
37.	Kim et al. [57] (2020)	CNN	Supervised	Discriminative	KDD CUP 99 and CSE-CIC-IDS 2018	DoS-Hulk, DoS-SlowHTTPTest, DoS-GoldenEye, DoS-Slowloris, DDoS-LOIC-HTTP DDoS-HOIC, Neptune Attack, Smurf Attack	Hyper-parameters tuning for designing an optimal model
38.	Parra et al. [93](2020)	Distributed Convolutional Neural Network (DCNN) and a cloud-based temporal Long-Short Term Memory (LSTM)	Supervised	Discriminative	Real time data generated by IoT devices and Botnets	UDP flood, TCP Flood, Acknowledgement flood, Domain Name System (DNS) flood, SYN flood attacks	capability to detect attacks at various levels on client devices and back-end servers
39.	Homayoun et al. [38] (2018)	BoTShark-SA that applies stacked Autoencoders and BoTShark-CNN that uses CNNs	Supervised and Unsupervised	Generative and Discriminative	ISCX2012 dataset	HTTP DoS attacks, IRC Botnet attacksS, Brute Force SSH, unknown TCP attacks, ICMP attacks, attacks by exploiting SMTP, IMAP, DNS	Automatic and efficient extraction of features without experts.
40.	Hwang et. el. [41] (2020)	Convolutional Neural Network (CNN) and Autoencoder	Supervised (feature extraction) and unsupervised	Discriminative and Generative	USTC-TFC2016, Mirai-RGU, and Mirai-CCU	ACK flood, SYN flood, UDP flood, HTTP flood, DNS flood, VSE flood, GREIP flood	speeding up the detection

Table 2 (continued)

S.No	Authors and Year	Models used	Nature of learning	DL types	Dataset	Attacks detected	Advantages / characteristics
41.	Thing [120] (2017)	Stacked AE (stacking multiple layers of sparse auto-encoders)	Unsupervised	Generative	Real time dataset	Probe Request and Probe Response Flooding attacks	Self-learns the characteristics required to detect network anomalies and is capable of accurately classifying attacks..
42.	Karim et.al. [49](2018)	Stacked AE (Taguchi Method for parameter optimization)	Unsupervised	Generative	UNSW-NB15	TCP attacks, UDP attacks, attacks by HTTP, FTP, SMTP	More robust than some well known attacks.
43.	Ali and Li [8] (2019)	AE for feature learning and multiple kernel learning (MKL) algorithm for combining the multilevel features	Unsupervised	Generative	ISCX 2012 and UNSW-NB15 datasets	HTTP DoS attacks, IRC Botnet attacks, Brute Force SSH, unknown TCP attacks, ICMP attacks, attacks by exploiting SMTP, IMAP, DNS	computations are more efficient. Learn robust features for DDoS detection
44.	Gurina and Eliseev [36] (2019)	AE	Unsupervised	Generative	Real time data	TCP flood, SYN flood, UDP flood, ICMP flood, and HTTP flood	High-quality attack detection for a reasonably simple web server; independence from expert labelling for training the classifier.
45.	Kumar and Bhama [65] (2019)	Sparse AE	Unsupervised	Generative	DoS attacks created by botNets like Mirai, BASHLITE, FBOT, ARIS, EXIENDO and APEP	GREETH, UDPPlain, HTTP, UDP, VSE, DNS, SYN, ACK, STOMP and GRE-IP	Ability to handle a flash crowd. Controlling IoT botnets and cryptojacking by forecasting them in advance.
46.	Gormez et al. [33](2020)	Ensemble models and AE based deep learning classifiers	Unsupervised	Generative and Discriminative	Digiturk and Labris	SYN ACK DDoS, ICMP DDoS, FIN DDoS, HTTP_GET flooding,	Hyper-parameter tuning using Bayesian Optimization to reduce search space and choose optimal values for hyper-parameters

Table 2 (continued)

S.No	Authors and Year	Models used	Nature of learning	DL types	Dataset	Attacks detected	Advantages / characteristics
47.	Elsayed et al. [26] (2020)	RNN with Autoencoder	Unsupervised	Generative	CICDDoS2019	SYN flood attacks, MSSQL attacks, UDP-Lag, LDAP attacks, UDP floof attacks, PortScan, and NetBIOS attcks, WebDDoS attcks, SSDP DDoS	Highest evaluation metrics in terms of recall, precision, F-score, and accuracy. Reduce the data dimensionality by automatically extracting the features from input data
48.	Catak and Mustacoglu [18](2019)	AE and DNN	Unsupervised	Generative	Real time traffic trace and KDD CUP 99	SYN flood, Neptune Attack, Smurf Attack, HTTP and FTP flows	Ability to support datasets used in cyber security areas.
49.	Radford et al. [98] (2017)	LSTM RNN	Unsupervised *	Discriminative	ISCX 2012	HTTP DoS attacks, IRC Botnet attacks, Brute Force SSH, unknown TCP attacks, ICMP attacks, attacks by exploiting SMTP, IMAP, DNS	Adaptable to a wide array of computer network topologies and architectures
50.	Mighan and Kahani [79] (2018)	Stacked AE (SAE) network for dimensionality reduction and support vector machine for binary classification	Unsupervised and Supervised (for classification)	Generative	ISCX2012 dataset	HTTP DoS attacks, IRC Botnet attacks, Brute Force SSH, unknown TCP attacks, ICMP attacks, attacks by exploiting SMTP, IMAP, DNS	Automatic learning of features.
51.	Zhang et al. [132] (2020)	SGM-CNN (SGM - combination of Synthetic Minority Over-Sampling Technique (SMOTE) and under-sampling for clustering based on Gaussian Mixture Model (GMM))	Supervised	Discriminative	UNSW-NB15 and CICIDS2017	DoS-Hulk, DoS-SlowHTTPTest, DoS-GoldenEye, DoS-Slowloris, DDoS-LOIC-HTTP DDoS-HOIC, BotNet attacks, general DoS attacks (UDP,TCP)	Ability to address class imbalance problem.

Table 2 (continued)

S.No	Authors and Year	Models used	Nature of learning	DL types	Dataset	Attacks detected	Advantages / characteristics
52.	Chiba et al. [19] (2019)	Deep Neural Network (DNN) based on Improved Genetic Algorithm (IGA) and Simulated Annealing	Supervised	Discriminative	CICIDS2017, NSL-KDD version 2015 and CIDDS-001.	DoS Slowloris, DoS SlowHTTPTest, DoS Hulk and DoS GoldenEye, HTTPDoS, DDoS attack using UDP, TCP, or HTTP requests	Reduction in execution time and saving of processing power
53.	Kasongo and Sun [51] (2020)	Feed-Forward Deep Neural Network (FFDNN) with Wrapper Based Feature Extraction algorithm	Supervised	Discriminative	UNSW NB15, AWID	TCP attacks, UDP attacks, attacks by HTTP, FTP, SMTP	Ability to generate feature subsets under a variety of scenarios, in terms of the target class.
54.	Ferrag et al. [29](2019)	DNN, CNN, RNN, RBM, DBN, DBM, DA	Supervised & unsupervised	Discriminative & Generative	CIC IDS 2018	slowloris,DoS Slowhttptest, DoS Hulk, DoS GoldenEye, DDoS LOIC-UDP, DDoS LOIC-HTTP	comparative analysis of deep learning techniques for DoS/DDoS attacks detection
55.	Tama and Rhee [117] (2017)	DNN	Supervised	Discriminative	UNSW-NB15, CIDDS-001, GPRS	TCP attacks, UDP attacks, attacks by HTTP, FTP, SMTP	Discovered best hyper-parameters setting for each of the datasets used.
56.	Alguliyev et al. [7] (2019)	Improved CNN and LSTM models	Supervised	Discriminative & Generative	Real time data from Twitter	TCP, UDP and HTTP attacks	Ability to handle social media data.
57.	Shurman et al. [110] (2020)	LSTM	Supervised	Discriminative	CICDDoS2019	SYN flood attacks, MSSQL attacks, UDP-Lag, LDAP attacks, UDP flood attacks and many more	capable of detecting unknown network packets and banning unwanted IPs
58.	Bhati et al. [14] (2020)	RNN	Supervised	Discriminative	ISCX2017, ISCX2018 and CICD-DoS2019	SYN flood attacks, MSSQL attacks, UDP-Lag, LDAP attacks, UDP flood attacks, PortScan, and much more	Reduced memory requirement Reduce feature set.
59.	Aldhaheri et al. [5] (2020)	Deep Learning and Dendritic Cell Algorithm	Supervised	Discriminative	BoT-IoT	DoS TCP, DoS UDP, DoS HTTP	minimized false alarm generation High detection rate

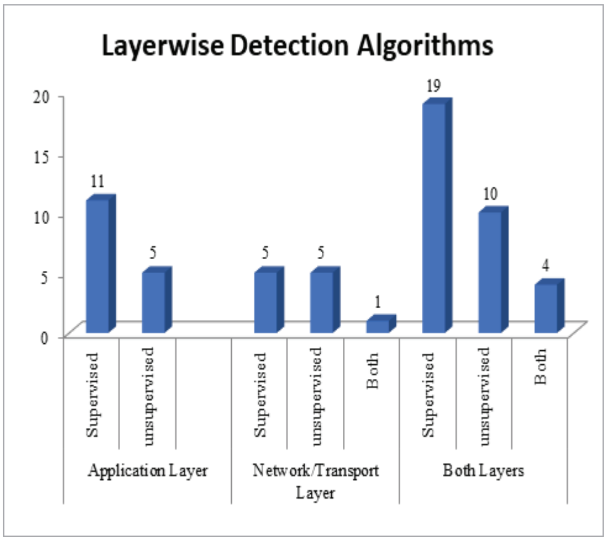
Table 2 (continued)

S.No	Authors and Year	Models used	Nature of learning	DL types	Dataset	Attacks detected	Advantages / characteristics
60.	Susilo and Sari [116] (2020)	CNN, MLP, RF	supervised	discriminative	BoT-IoT	DoS TCP, DoS UDP, DoS HTTP	Tuning hyper-parameter for speeding up the calculation
61.	Du et al. [25] (2017)	Stacked LSTM	Supervised	Discriminative	Real-time dataset created from HDFS and Openstack	TCP,UDP, HTTP	Ability to learn log patterns from normal execution and detect anomalies. Supports online update/training and adapt to new execution patterns
62.	Agarwal et al. [3] (2021)	Feature Selection Based Whale Optimization DNN	Supervised	Discriminative	CICIDS2017	DoS Slowloris, DoS SlowHTTPTest, DoS Hulk and DoS GoldenEye, DDoS-LOIC	Storing the non-attacked data in cloud to provide security and avoiding the entry of DDOS attacks
63.	Sumathy and Karthikeyan [115] (2021)	Auto Encoder	Unsupervised	Generative	Mixed dataset consists of Conficker CAIDA and UNINA	AL DoS, NL/TL DoS	Implementation of cost minimization algorithm to reduce the classification error.
64.	Wang and Li [124](2021)	Transformer Network (encoder and decoder) and CNN	Supervised & Unsupervised	Discriminative & Generative	CICDDoS2019	SYN flood attacks, MSSQL attacks, UDP-Lag, LDAP attacks, UDP flood attacks, PortScan, and many more	Improved computational efficiency and scalability
65.	Shieh et al. [109](2021)	BI-LSTM and GMM with incremental learning	Supervised	Discriminative	CIC-IDS2017 and CIC-DDoS2019	DoS Slowloris, DoS SlowHTTPTest, DoS Hulk and DoS GoldenEye, etc.	Ability to discriminate between normal and malicious packets
66.	Xu et al. [128] (2021)	CNN and GRU	Supervised	Discriminative	Real traffic traces gathered from Internet traffic	Low-rate DoS attacks such as Slowloris, Slowhttptest, Pwnloris, Torshammer, and Httpbog	Ability to detect LDoS attacks in fluctuating HTTP traffic

presented a review of the Deep learning-based DDoS attacks detection methods proposed till 2016. With the recent advancements in deep learning, there are a number of efforts made after 2016. To the best of our knowledge, we believe that our survey is the first study after 2016 [128]. From the study, we find that there are research attempts focusing network/transport and/or application layer DoS/DDoS attacks. Deep learning models such as MLP, ANN, DNN, CNN, LSTM, RNN, AE, DBN etc. have been used by these research efforts and presented in this study.

Figure 4 shows the number of supervised and unsupervised deep learning algorithms for detecting different types of DoS/DDoS attacks that have been reviewed in this study. Surprisingly, we identify that irrespective of many recent improvements in deep learning approaches like LSTM, GRU etc., the basic DNNs/MLPs/ANNs [1,11, 12, 27,47, 95, 104, 106, 113, 117, 130, 132] were also performing equally well in classification.

Figure 4
Layer-wise Detection Algorithms



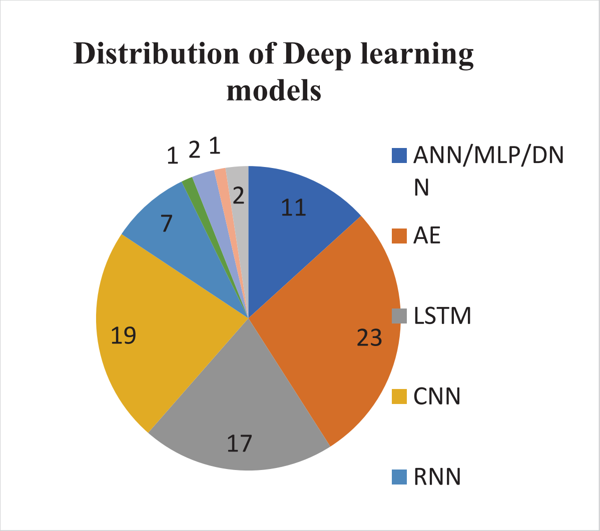
These models extracted appropriate features using different feature selection algorithms. The authors of these attempts built NNs by tuning the hyper-parameters such as number of hidden layers and neurons in each layer appropriately in order to learn better. We also found that both supervised and unsupervised algorithms perform well in classifying DoS/DDoS attacks. The authors of supervised algorithms claimed that their approaches performed well while classifying the test data, which has the classes similar to training data, whereas the accuracy of classification is comparatively less in case of unsupervised learning algorithms. This is due to the fact that these algorithms excel in clustering rather than classification.

Another interpretation from Figure 4 is that supervised learning techniques have been used in many research efforts as they provide more accuracy. But, by increasing the learning experience, there is scope to improve the accuracy of unsupervised techniques also. Figure 4 may serve as a guideline for future researchers on choosing techniques for detecting DoS/DDoS attacks. As deep learning methods are efficient in identifying the relationships between features in a dataset, they are not only used for classification, but also for feature learning. In the reviews taken, some of them used deep learning models for feature extraction and some for classification [13, 21, 27, 129, 133]. The models, AE and SOM are mostly used for feature extraction. We also noticed that a significant number of efforts used RNN/LSTM for classification along with word embedding for feature extraction [18, 42, 80] as they preserve the semantic relations between each data and reduce the feature dimension. Also, the temporal features from the input data can be easily extracted by RNN. LSTM is a variant of RNN [127] and has the ability to keep track of the long term relationship in the sequential data while dropping out short-lived temporal noises if needed. The study of hybrid models is also becoming hot in recent years. Figure 5 shows the distribution of various deep learning models reviewed in this survey.

From Figure 5, we realize that the CNN and AE are more commonly used for building DoS/DDoS attack detection systems. High level feature representations can be very well extracted by CNN and abstract form of low-level feature sets of network traffic traces can then be represented using those high-level feature representations. As AE based deep learning approaches performed exceedingly well in challenging classification problems, a number of research efforts using AE to detect DoS/DDoS attacks have also been carried out. There are also other reasons like its use in dimensionality reduction and capability to address the imbalanced classification problems [27].

While looking for the deep learning techniques to detect DoS/DDoS attacks, we found a large number of articles on AE and CNN rather than on other deep learning techniques. This shows that AE and CNN are superior to the other state-of-the-art approaches. Future researchers may focus on these techniques for building DoS/DDoS attack detection systems.

Figure 5
Distribution of Deep Learning Models



Having seen how various deep learning models implement the detection mechanism, now, we present a brief comparison of various deep learning algorithms and different scenarios where these approaches have been preferred.

Since most of the DoS/DDoS attacks datasets are time series data, and RNNs can integrate a temporal layer to capture time series data and learn variations in the data with the hidden recurring unit, RNN and its variations namely LSTM and GRU have been mostly used in recent times. We understand that when a dataset with arbitrary length of large-scale sequence data exhibits dynamic temporal behaviours, RNN is most appropriate model to analyze the dataset. This is due to the fact that RNN architectures are capable of storing and adjusting information over time-lags for long-term dependencies with successive connection sequence information. So, RNN techniques have shown better performance over other non-recurring networks in the identification of attacks. Following RNN, AE has been the next frequently used model. Surprising we find that, for real traffic traces, AE based models have been proposed. AE models, which are unsupervised training algorithms, are used for extracting the features from the traffic traces. The extracted features have been used for classification by various deep learning models. But we believe that the ensemble and hybrid architectures are still poorly explored.

Following AE, CNN is found to be next most commonly used deep learning models. CNN is thought to be more powerful than RNN. Since CNN has more feature compatibility than RNN, many authors who work on detection of DoS/DDoS attacks have used CNN. As same filters are applied to multiple parts of the images at the same time, computations can happen simultaneously in CNN and in turn, CNN runs faster. Apart from classification, CNN has also been used for feature extraction. As the datasets such as CICIDS2017/2018 and CIC DoS2019 have more number of features, CNN has been used for feature extraction and then, RNN is used for classification [71, 105]. From this, we interpret that when there is more number of features in a dataset, instead of using RNN directly, the researchers have used CNN for feature extraction and extracted features have been given to RNN for classification. To the best of our knowledge, although CNN has proven to be a good classifier, it has not been fully utilized in the field of intrusion detection and need to be explored further. DBN is also new to its exploitation in this field, and the experimental work to determine the reliability of this learning is still underway.

Having seen the deep learning models, we now explore how the datasets presented in Section 5 are used for training and testing these models. Most of the datasets including ISCX 2012, CICIDS2017 etc. used in the reviewed articles are labelled only. So, we find that most of the authors have used supervised learning algorithms. Novel DoS/DDoS attacks, on the other hand, can alter traffic patterns. If a model is trained using labeled datasets, it may not perform well when faced with new and unknown forms of attacks with varying traffic patterns. Interestingly, we identify that labelled datasets are used by unsupervised algorithms to learn better and classify unseen attack traffic [8, 38].

From the surveyed articles, we understand that there are quite a few unsupervised deep learning techniques like Auto Encoders [8, 13, 26, 38, 49, 50, 82] which used the datasets as unlabeled and achieved more than 90% classification accuracy. The authors of [25, 35, 36, 59, 77, 82, 93, 95, 120, 129, 133] have generated their own datasets and implemented unsupervised algorithms to identify the unseen attack traffic. Even though ISCX 2012 dataset is a labelled one, Radford et al. [98] used the labels for validation, but not for training the model. From the study, we comprehend that, for new kind of traffic patterns, generative unsupervised algorithms would exhibit a good performance. Another interesting point we find in this study is the use of datasets. The KDD CUP 99 and NSL KDD datasets have been the most common intrusion detection datasets. Since it was generated by simulation over a virtual computer network and contains redundant data, the KDD CUP 99 dataset does not represent real traffic data. So, NSL KDD 99 has been introduced by addressing the redundancy in KDD CUP 99 dataset. Still, both KDD99 and NSLKDD do not provide satisfactory results because they lack in exhibiting current trends in normal and attack traffic. To address these issues, a huge collection of datasets for a large variety of attacks have been generated by Canadian Institute of Cybersecurity. However, today's applications produce a wide range of traffic types, each with its own set of service specifications. As a result, the classification of such traffic is critical to improving the detection system's efficiency. In such case, the historical datasets may not be suitable. We noticed that most of the research works on DoS/DDoS attacks detection using deep learning used ISCX 2012 dataset. This dataset contains attacks from network/transport and application layer protocols. CICIDS2017, containing application layer DoS/DDoS attacks, is the next commonly used dataset by the efforts reviewed in this study [22]. In some of the attempts, botnets like Mirai, BASHLITE etc. have been used for creating DoS/DDoS attacks.

Another significant point we noted from this review is that, even though there have been datasets containing both application and network/transport layer attack traces, real time datasets have been generated and used for detecting attacks. This shows that the existing datasets do not contain traces of more types of attack traffic.

We also realize that the authors of most of the attempts suggest that their models could be extended to detect many other emerging attacks. But, we believe that this requires generation of real time datasets and more training. Furthermore, the authors of the reviewed articles have not ensured that their models can detect real time DoS/DDoS attacks or provide detection while the monitored system is under attack. However, the authors of [68, 98] have mentioned that their models could be extended to detect real time DoS/DDoS attacks by combining a few deep learning models. As a result, we suggest that future researchers in this field concentrate on developing hybrid deep learning models to detect real-time DoS/DDoS attacks, as well as using transfer learning to detect new attacks by transferring knowledge from previous detections.

Given the limitations of the current datasets in Table 1, we believe a comprehensive framework for generating benchmarking datasets for DoS/DDoS attacks is essential. By using the work by Abdulhammed et al. and Catak and Mustacoglu [1, 18], we summarize the requirements such a framework shall meet. The requirements include being real world traces, labelled dataset, unbiased in size of both benign and malicious traffic instances, appropriate feature set, diverse in attack scenarios, data from heterogeneous sources, proper documentation about data (meta data), traces from variety of traffic like HTTP, FTP, VOIP, web browsing, online purchasing etc.

But, we find that no dataset satisfies all the aforementioned requirements. The main reason is that it is very difficult to have up-to-date dataset due to the ever-increasing number and kind of attacks. Nevertheless, authors of the surveyed articles felt that some of the datasets more appropriate than others. For instance, using KDD Cup 99 / NSL KDD datasets cannot aid in the development of a better deep learning model to detect DoS/DDoS attacks. In such cases, we recommend the researchers to consider recent, updated and more realistic datasets such as UNSW NB15, CICDDoS2019 and CICIDS2017/2018.

This survey also reviewed deep learning approaches for detecting DoS/DDoS attacks over Software defined networking (SDN) [12, 26, 68, 105]. SDN has been emerging as a new networking technology because of its centralized controlling nature. However, it is vulnerable to different forms of attacks, including DoS/DDoS attacks [68. These attacks have severe impact because it degrades the performance of the SDN by overloading its different components. Our review explored a large number of DoS/DDoS detection approaches based on deep learning. From these attempts, we made certain observations and found imbalances in some aspects namely in the choice of datasets and performance metrics. There are several datasets available, and Section 5 listed several of the most widely used datasets for detecting DoS/DDoS attacks. Based on the nature of the deep learning algorithms, the authors have used datasets of their choice. We have also noticed that there is also disparity in the number of records for different types of DoS/DDoS attacks in both benchmark and real time datasets. This is not advisable for a good learning model. Moreover, the performance metrics used by these authors are also not uniform. We find it difficult to compare the performance of the various research efforts as they have adapted different datasets and/or different metric combinations. For instance, the research efforts using ISCX 2012 dataset measured the performance using one or more metrics like accuracy, precision, recall, false alarm rate, true positive and true negative rate etc. Among these efforts, the only common metric is accuracy. Wang et al. [125] provides highest accuracy when compared with all the other attempts using the same dataset. So, we were not able to compare its performance with competing models based on other metrics. This leads to some imbalances in identifying a most appropriate model. Such issues may be addressed by future researchers.

Following an examination of the articles, we have found a number of extension works that could be used by future scholars to further explore the subject of the study. They include:

- A variety of deep learning models may be tried.
- Imbalance in the datasets may be addressed.
- Detection of unknown and new attacks may be attempted.
- Transfer learning techniques may be tried.
- Attacks on Real SDN architecture may be detected.
- Ensemble of learning methods may be used to improve the performance.
- Diversity of DDoS attacks can be attempted.
- Optimization techniques may be attempted to improve the performance
- Exploring a variety of feature selection methods to improve the detection performance.
- Detection of attacks in real time environment.
- Minimizing the computational requirements while detecting the attacks

8. Conclusion

DoS/DDoS attacks continue to be the most serious danger to the availability of business networks, applications, and services. Because of their unique characteristics, DoS/DDoS attacks are still seen as a serious danger by businesses that are concerned about being the target of an assault. Modern security systems have evolved ways to fight against most types of DoS/DDoS attacks. With deep learning receiving increased attention in a variety of domains these days, this study investigated the application of deep learning models for detecting DoS/DDoS attacks and compared the numerous attempts made by researchers. This investigation gave a thorough examination of algorithms, the nature of learning, discovered threats, performance metrics, and so on. In particular, recent efforts from 2016 have been analyzed in this paper, with a focus on single and hybrid deep learning techniques.

A few findings have been uncovered as a result of a thorough investigation. From one of the findings, we understand that deep learning algorithms are being utilized not only for classification, but also for feature extraction and learning. Furthermore, we find that using an ensemble of multiple methods, we might attain good results. According to the results of the survey, we learned that the majority of the recommended methodologies rely on the benchmark datasets. Despite the fact that we have datasets that have been created lately during 2019, DoS/DDoS attackers continue to adapt their attack patterns and techniques. A considerable urge exists to develop more recent and real-time datasets, due to the fact that such novel patterns are not discussed in the benchmark datasets. These findings suggest that additional research is needed to strengthen the present state-of-the-art approaches in the subject of the study. In addition to the benefits, we have also presented the possible extension of the research efforts. This would definitely provide valuable research information and give the researchers suggestions for new research directions and stimulate the need for and encourage additional research into the subject of study.

This would definitely provide valuable research information and give the researchers suggestions for new research directions and stimulate the need for and encourage additional research into the subject of study.

References

1. Abdulhammed, R., Faezipour, M., Abuzneid, A., AbuMallouh, A. Deep and Machine Learning Approaches for Anomaly-based Intrusion Detection of Imbalanced Network Traffic. IEEE Sensors Letters, 2018, 3 (1), 1-4. https://doi.org/10.1109/LSENS.2018.2879990
2. Abdulhammed, R., Musafer, H., Alessa, A., Faezipour, M., Abuzneid, A. Features Dimensionality Reduction Approaches for Machine Learning based Network Intrusion Detection. Electronics, 2019, 8(3), 322. https://doi.org/10.3390/electronics8030322
3. Agarwal, A., Khari, M., Singh, R. Detection of DDOS Attack using Deep Learning Model in Cloud Storage Application. Wireless Personal Communications, 2021, 1-21. https://doi.org/10.1007/s11277-021-08271-z
4. Al-Garadi, M. A., Mohamed, A., Al-Ali, A. K., Du, X., Ali, I., Guizani, M. A Survey of Machine and Deep Learning Methods For Internet of Things (IoT) Security. IEEE Communications Surveys and Tutorials, 2020, 22 (3), 1646-1685. https://doi.org/10.1109/COMST.2020.2988293
5. Aldhaheri, S., Alghazzawi, D., Cheng, L., Alzahrani, B., Al-Barakati, A. DeepDCA: Novel Network-based Detection of IoT Attacks using Artificial Immune System. Applied Sciences, 2020, 10(6), 1909. https://doi.org/10.3390/app10061909
6. Aldweesh, A., Derhab, A., Emam, A. Z. Deep Learning Approaches for Anomaly-based Intrusion Detection Systems: A Survey, Taxonomy, and Open Issues. Knowledge-Based Systems, 2020, 189, 105124. https://doi.org/10.1016/j.knosys.2019.105124
7. Alguliyev, R. M., Aliguliyev, R. M., Abdullayeva, F. J. The Improved LSTM And CNN Models FOR DDoS Attacks Prediction in Social Media. International Journal of Cyber Warfare and Terrorism, 2019, 9(1), 1-18. https://doi.org/10.4018/IJCWT.2019010101
8. Ali, S., and Li, Y. Learning Multilevel Auto-Encoders for DDoS Attack Detection in Smart Grid Network. IEEE Access, 2019, 7, 108647-108659. https://doi.org/10.1109/ACCESS.2019.2933304
9. Almiani, M., AbuGhazleh, A., Al-Rahayfeh, A., Atiewi, S., Razaque, A. Deep Recurrent Neural Network for IoT Intrusion Detection System. Simulation Modelling Practice and Theory, 2020, 101, 102031. https://doi.org/10.1016/j.simpat.2019.102031
10. Alom, M. Z., Taha, T. M. Network Intrusion Detection for Cyber Security Using Unsupervised Deep Learning Approaches. Proceedings of IEEE Aerospace and Electronics Conference (NAECON 2017), Big Sky, MT, USA, March 04-11, 2017, 63-69.https://doi.org/10.1109/NAECON.2017.8268746
11. Asad, M., Asim, M., Javed, T., Beg, M. O., Mujtaba, H., Abbas, S. Deepdetect: Detection of Distributed Denial Of Service Attacks Using Deep Learning. The Computer Journal, 2020, 63(7), 983-994. https://doi.org/10.1093/comjnl/bxz064
12. Benzaïd, C., Boukhalfa, M., Taleb, T. Robust Self-protection Against Application-layer (D) DoS Attacks in SDN Environment. Proceedings of IEEE Wireless Communications and Networking Conference (WCNC). May 25-28, 2020, 1-6. https://doi.org/10.1109/WCNC45663.2020.9120472
13. Best, N., Ott, J., Linstead, E. J. Exploring the Efficacy of Transfer Learning in Mining Image-based Software Artifacts. Journal of Big Data, 2020, 7(1), 1-10. https://doi.org/10.1186/s40537-020-00335-4
14. Bhati, A., Bouras, A., Qidwai, U. A., Belhi, A. Deep Learning Based Identification of DDoS Attacks in Industrial Application. Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), July 27-28, 2021, 190-196. https://doi.org/10.1109/WorldS450073.2020.9210320
15. Bhatia, S., Behal, S., Ahmed, I. Distributed Denial of Service Attacks and Defense Mechanisms: Current Landscape and Future Directions. Versatile Cybersecurity (Springer), 2018, 55-97. https://doi.org/10.1007/978-3-319-97643-3_3
16. Bhuyan, M. H., Bhattacharyya, D. K., Kalita, J. K. Towards Generating Real-Life Datasets for Network Intrusion Detection. International Journal Network Security. 2015, 17(6), 683-701.
17. CAIDA. The CAIDA DoS Attack 2007 Dataset. Available from: https://www.caida.org/ data/passive/ddos-

20070804_dataset.xml. Accessed on November 30, 2020.

18. Catak, F. O., Mustacoglu, A. F. Distributed Denial of Service Attack Detection Using Autoencoder and Deep Neural Networks. Journal of Intelligent and Fuzzy Systems. 2019, 37 (3), 3969-3979. https://doi.org/10.3233/JIFS-190159
19. Chiba, Z., Abghour, N., Moussaid, K., Rida, M. Intelligent Approach to Build a Deep Neural Network based IDS for Cloud Environment using Combination of Machine Learning Algorithms. Computers and Security, 2019, 86, 291-317. https://doi.org/10.1016/j.cose.2019.06.013
20. CIC-DDoS2019. DDoS Evaluation Dataset (CIC-DDoS2019). Available from: https://www.unb.ca/cic/datasets/ddos-2019.html. Accessed on October 21, 2020.
21. Cui, J., Long, J., Min, E., Mao, Y. WEDL-NIDS: Improving Network Intrusion Detection using Word Embedding-based Deep Learning Method. Lecture Notes in Computer Science, 11144. Springer, Cham., 2018, 283-295. https://doi.org/10.1007/978-3-030-00202-2_23
22. CyberSecurity. 1998 DARPA Intrusion Detection Evaluation Dataset. Available from: https://www.ll.mit.edu/r-d/datasets/1998-darpa-intrusion-detection-evaluation-dataset. Accessed on November 02, 2021
23. Dantas Silva, F. S., Silva, E., Neto, E. P., Lemos, M., Venancio Neto, A. J., Esposito, F. A Taxonomy of DDoS Attack Mitigation Approaches Featured by SDN Technologies in IoT Scenarios. Sensors, 2020, 20(11), 3078. https://doi.org/10.3390/s20113078
24. 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 Transactions on Network and Service Management. 2020, 17(2), 876-889. https://doi.org/10.1109/TNSM.2020.2971776
25. Du, M., Li, F., Zheng, G., Srikumar, V. Deeplog: Anomaly Detection and Diagnosis from System Logs through Deep Learning. Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, Dallas Texas USA, October 30 - November 03, 2017, 1285-1298. https://doi.org/10.1145/3133956.3134015
26. Elsayed, M. S., Le-Khac, N. A., Dev, S., Jurcut, A. D. DDosNET: A Deep-learning Model for Detecting Network Attacks. Proceedings of IEEE 21st International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM), Cork, Ireland, August 31 - September 03, 2020, 391-396, arXiv:2006.13981. https://doi.org/10.1109/WoWMoM49955.2020.00072
27. Farahnakian, F., Heikkonen, J. A Deep Auto-encoder Based Approach for Intrusion Detection System. 20th International Conference on Advanced Communication Technology (ICACT), South Korea, February 11-14, 2018, 178-183. https://doi.org/10.23919/ICACT.2018.8323688
28. Fenil, E., Mohan Kumar, P. Survey on DDoS Defense Mechanisms, Concurrency and Computation: Practice and Experience, 2020, 32(4), e5114, https://doi.org/10.1002/cpe.5114.https://doi.org/10.1002/cpe.5114
29. Ferrag, M. A., Maglaras, L., Janicke, H., Smith, R. Deep Learning Techniques for Cyber Security Intrusion Detection: A Detailed Analysis. Proceedings of 6th International Symposium for ICS & SCADA Cyber Security Research 2019 (ICS-CSR), Athens, Greece, September 10-12, 2019, 126-136. https://doi.org/10.14236/ewic/icscsr19.16
30. Gadze, J. D., Bamfo-Asante, A. A., Agyemang, J. O., Nunoo-Mensah, H., Opare, K. A. B. An Investigation into the Application of Deep Learning in the Detection And Mitigation of DDoS Attack on SDN Controllers. Technologies, 2021, 9(1), 14. https://doi.org/10.3390/technologies9010014
31. Garber, L. Denial-of-Service Attacks Rip the Internet. Computer, 2000, 33(04), 12-17. https://doi.org/10.1109/MC.2000.839316
32. Ghanbari, M., Kinsner, W. Extracting Features from both the Input and the Output of a Convolutional Neural Network to Detect Distributed Denial of Service Attacks. Proceedings of IEEE 17th International Conference on Cognitive Informatics and Cognitive Computing (ICCI*CC), July 16 - 18, 2018, Berkeley, CA, USA2018, 138-144. https://doi.org/10.1109/ICCI-CC.2018.8482019
33. Gormez, Y., Aydin, Z., Karademir, R., Gungor, V. C. A Deep Learning Approach with Bayesian Optimization and Ensemble Classifiers for Detecting Denial of Service Attacks. International Journal of Communication Systems, 2020, 33(11), e4401. https://doi.org/10.1002/dac.4401
34. Gümüşbaş, D., Yıldırım, T., Genovese, A., Scotti, F. A Comprehensive Survey of Databases and Deep Learning Methods for Cybersecurity and Intrusion Detection Systems. IEEE Systems Journal, 2020. https://doi.org/10.1109/JSYST.2020.2992966
35. Guo, H., Fan, X., Cao, A., Outhred, G., Heidemann, J. Peek Inside the Closed World: Evaluating Autoencoder-Based Detection of DDoS to Cloud. arXiv preprint arXiv:1912.05590, 2019
36. Gurina, A., Eliseev, V. Anomaly-based Method for Detecting Multiple Classes of Network Attacks. In-

formation, 2019, 10(3), 84. https://doi.org/10.3390/info10030084

37. Hodo, E., Bellekens, X., Hamilton, A., Tachtatzis, C., Atkinson, R. Shallow and Deep Networks Intrusion Detection System: A Taxonomy and Survey. arXiv preprint arXiv:1701.02145, 2017.

38. Homayoun, S., Ahmadzadeh, M., Hashemi, S., Dehghantanha, A., Khayami, R. BoTShark: A Deep Learning Approach for Botnet Traffic Detection. Cyber Threat Intelligence (Springer, 2018), 137-153. https://doi.org/10.1007/978-3-319-73951-9_7

39. Hussain, B., Du, Q., Sun, B., Han, Z. Deep Learning-based DDoS-attack Detection for Cyber-Physical System over 5G Network. IEEE Transactions on Industrial Informatics, 2020, 17 (2), 860-870. https://doi.org/10.1109/TII.2020.2974520

40. Hussain, Y. S. Network Intrusion Detection for Distributed Denial-of-Service (DDoS) Attacks Using Machine Learning Classification Techniques, 2020.

41. 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, 2020, 8, 30387-30399. https://doi.org/10.1109/ACCESS.2020.2973023

42. Hwang, R. H., Peng, M. C., Nguyen, V. L., Chang, Y. L. An LSTM-based Deep Learning Approach for Classifying Malicious Traffic at the Packet Level. Applied Sciences, 2019, 9(16), 3414. https://doi.org/10.3390/app9163414

43. Idhammad, M., Afdel, K., and Belouch, M. Semi-supervised Machine Learning Approach for DDoS Detection. Applied Intelligence, 2018, 48(10), 3193-3208. https://doi.org/10.1007/s10489-018-1141-2

44. Imamverdiyev, Y., Abdullayeva, F. Deep Learning Method for Denial of Service Attack Detection Based on Restricted Boltzmann Machine. Big Data, 2018, 6 (2), 159-169. https://doi.org/10.1089/big.2018.0023

45. ISCXIDS2021. Intrusion Detection Evaluation Dataset (ISCXIDS2012). Available from: https://www.unb.ca/cic/datasets/ids.html. Accessed on December 04, 2021

46. Jaafar, G. A., Abdullah, S. M., Ismail, S. Review of Recent Detection Methods for HTTP DDoS attack. Journal of Computer Networks and Communications, 2019. https://doi.org/10.1155/2019/1283472

47. Johnson, K., Thongam, K., De, T. Entropy-based Application Layer DDoS Attack Detection Using Artificial Neural Networks. Entropy, 2016, 18(10), 350. https://doi.org/10.3390/e18100350

48. Kalkan, K., Gür, G., and Alagöz, F. Filtering-based Defense Mechanisms Against DDoS Attacks: A Survey. IEEE Systems Journal, 2016, 1(4), 2761-2773. https://doi.org/10.1109/JSYST.2016.2602848

49. Karim, A. M., Güzel, M. S., Tolun, M. R., Kaya, H., Çelebi, F. V. A New Generalized Deep Learning Framework Combining Sparse Autoencoder and Taguchi Method for Novel Data Classification and Processing. Mathematical Problems in Engineering, 2018. https://doi.org/10.1155/2018/3145947

50. Kasim, Ö. An Efficient and Robust Deep Learning based Network Anomaly Detection against Distributed Denial of Service Attacks. Computer Networks, 2020, 180, 107390. https://doi.org/10.1016/j.comnet.2020.107390

51. Kasongo, S. M., Sun, Y. A Deep Learning Method with Wrapper based Feature Extraction for Wireless Intrusion Detection System. Computers and Security, 2020, 92, 101752. https://doi.org/10.1016/j.cose.2020.101752

52. Kaur, P., Kumar, M., and Bhandari, A. A Review of Detection Approaches for Distributed Denial of Service Attacks. Systems Science and Control Engineering, 2017, 5(1), 301-320. https://doi.org/10.1080/21642583.2017.1331768

53. Kayacik, H. G., Zincir-Heywood, A. N., Heywood, M. I. Selecting Features for Intrusion Detection: A Feature Relevance Analysis on KDD 99 Intrusion Detection Datasets. Proceedings of Third Annual Conference on Privacy, Security and Trust, New Brunswick, Canada October 12-14, 2005, 1723-1722.

54. KDDCup. KDD Cup 1999 Data. Available from: http://kdd.ics.uci.edu/databases/kddcup99/ kddcup99.html. Accessed on November 02, 2021.

55. Khalaf, B. A., Mostafa, S. A., Mustapha, A., Mohammed, M. A., Abduallah, W. M. Comprehensive Review of Artificial Intelligence and Statistical Approaches in Distributed Denial of Service Attack and Defense Methods. IEEE Access, 2019, 7, 51691-51713. https://doi.org/10.1109/ACCESS.2019.2908998

56. Khraisat, A., Gondal, I., Vamplew, P., Kamruzzaman, J. Survey of Intrusion Detection Systems: Techniques, Datasets and Challenges. Cybersecurity, 2019, 2(1), 1-22. https://doi.org/10.1186/s42400-019-0038-7

57. Kim, J., Kim, J., Kim, H., Shim, M., Choi, E. CNN-Based Network Intrusion Detection against Denial-of-Service Attacks. Electronics. 2020, 9(6), 916. https://doi.org/10.3390/electronics9060916

58. Kim, M. Supervised Learning-based DDoS Attacks Detection: Tuning Hyperparameters. ETRI Journal. 2019, 41(5), 560-573. https://doi.org/10.4218/etrij.2019-0156

59. Ko, I., Chambers, D., Barrett, E. Feature dynamic Deep Learning Approach for DDoS Mitigation within the ISP Domain. International Journal of Information Security, 2020, 19(1), 53-70. https://doi.org/10.1007/s10207-019-00453-y

60. Kobialka D. Kaspersky Lab study. Available from : https://www.msspalert.com/cybersecurity-research/kaspersky-lab-study-average-cost-of-enterprise-ddos-attack-totals-2m/. Accessed on October 25, 2021.

61. Kolias, C., Kambourakis, G., Stavrou, A., Voas, J. DDoS in the IoT: Mirai and other Botnets. Computer, 2017, 50(7), 80-84. https://doi.org/10.1109/MC.2017.201

62. 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. Future Generation Computer Systems, 2019, 100,779-796. https://doi.org/10.1016/j.future.2019.05.041

63. Krizhevsky, A., Sutskever, I., and Hinton, G. E. Imagenet Classification with Deep Convolutional Neural Networks. Advances in Neural Information Processing Systems, 2012, 25, 1097-1105.

64. Kruse, W. G., Heiser, J. G. Computer Forensics: Incident Response Essentials. Pearson Education, 2001.

65. Kumar, C. O., Bhama, P. R. S. Detecting and Confronting Flash Attacks from IoT Botnets. The Journal of Supercomputing. 2019, 75(12), 8312-8338. https://doi.org/10.1007/s11227-019-03005-2

66. Kwon, D., Kim, H., Kim, J., Suh, S. C., Kim, I., Kim, K. J. A Survey of Deep Learning-Based Network Anomaly Detection. Cluster Computing, 2019, 22(1), 949-961. https://doi.org/10.1007/s10586-017-1117-8

67. Li, C., Wang, J., Ye, X. Using a Recurrent Neural Network and Restricted Boltzmann Machines for Malicious Traffic Detection. NeuroQuantology, 2018, 16(5). https://doi.org/10.14704/nq.2018.16.5.1391

68. Li, C., Wu, Y., Yuan, X., Sun, Z., Wang, W., Li, X., Gong, L. Detection and Defense of DDoS Attack-Based on Deep Learning in Openflow-Based SDN. International Journal of Communication Systems, 2018, 31(5), e3497 https://doi.org/10.1002/dac.3497

69. Lipton, Z. C., Berkowitz, J., Elkan, C. A Critical Review of Recurrent Neural Networks for Sequence Learning. arXiv preprint arXiv:1506.00019, 2015.

70. Liu, H., Lang, B. Machine Learning and Deep Learning Methods for Intrusion Detection Systems: A Survey. Applied Sciences, 2019, 9(20), 4396. https://doi.org/10.3390/app9204396

71. Liu, L., Lin, J., Wang, P., Liu, L., Zhou, R. Deep Learning-Based Network Security Data Sampling and Anomaly Prediction in Future Network. Discrete Dynamics in Nature and Society, 2020. https://doi.org/10.1155/2020/4163825

72. Lu, W., Traore, I. An Unsupervised Anomaly Detection Framework for Network Intrusions. Technical Report. Dept. of Electrical and Computer Engineering, University of Victoria, 2005. https://doi.org/10.1007/11599371_9

73. Manavi, M. T. Defense Mechanisms against Distributed Denial of Service Attacks: A Survey. Computers and Electrical Engineering, 2018, 72, 26-38. https://doi.org/10.1016/j.compeleceng.2018.09.001

74. Manimurugan, S., Al-Mutairi, S., Aborokbah, M. M., Chilamkurti, N., Ganesan, S., Patan, R. Effective Attack Detection in Internet of Medical Things Smart Environment using a Deep Belief Neural Network. IEEE Access, 2020, 8, 77396-77404. https://doi.org/10.1109/ACCESS.2020.2986013

75. Marcus R. Available from: https://www.hs-coburg.de/forschung/forschungsprojekte-oeffentlich/informationstechnologie/cidds-coburg-intrusion-detection-data-sets.html. Accessed on October 20, 2020.

76. McDermott, C. D., Majdani, F., Petrovski, A. V. Botnet Detection in the Internet of Things using Deep Learning Approaches. International Joint Conference on Neural Networks. Rio, Brazil, July 08-13, 2018, 1-8. ps://doi.org/ oi: 10.1109/IJCNN.2018.8489489 https://doi.org/10.1109/IJCNN.2018.8489489

77. Meidan, Y., Bohadana, M., Mathov, Y., Mirsky, Y., Shabtai, A., Breitenbacher, D., Elovici, Y. NBAIOT-Network-based Detection of IoT Botnet Attacks using Deep Autoencoders. IEEE Pervasive Computing, 2018, 17(3), 12-22. https://doi.org/10.1109/MPRV.2018.03367731

78. Meng, W., Qian, C., Hao, S., Borgolte, K., Vigna, G., Kruegel, C., Lee, W. Rampart: Protecting Web Applications from CPU-Exhaustion Denial-of-Service Attacks. Proceedings of CPU-exhaustion Denial-Of-Service Attacks (SEC 18), Baltimore, MD, USA, August 15-17, 2018, 393-410.

79. Mighan, S. N., Kahani, M. Deep Learning based Latent Feature Extraction for Intrusion Detection. Proceedings of Iranian Conference on Electrical Engineering (ICEE), Mashhad, Iran, May 08-10, 2018, 1511-1516. https://doi.org/10.1109/ICEE.2018.8472418

80. Min, E., Long, J., Liu, Q., Cui, J., Chen, W. TR-IDS: Anomaly-based Intrusion Detection Through Text-

Convolutional Neural Network and Random Forest. Security and Communication Networks, 2018

81. Mirkovic, J., Reiher, P. A Taxonomy of DDoS Attack and DDoS Defense Mechanisms. ACM SIGCOMM Computer Communication Review, 2004, 34(2), 39-53. https://doi.org/10.1145/997150.997156

82. Mirsky, Y., Doitshman, T., Elovici, Y., Shabtai, A. Kitsune: An Ensemble of Autoencoders for Online Network Intrusion Detection. arXiv preprint arXiv:1802.09089, 2018. https://doi.org/10.14722/ndss.2018.23204

83. Muraleedharan, N., Janet, B. A Deep Learning Based HTTP Slow DoS Classification Approach using Flow Data. ICT Express, 2021, 7 (2), 210-214. https://doi.org/10.1016/j.icte.2020.08.005

84. Nadav, Avishay, Johnathan, Kim. 2019 Global DDoS Threat Landscape Report. Available from: https://www.imperva.com/blog/2019-global-ddos-threat-landscape-report/. Accessed on November 04, 2021

85. NETSCOUT. NETSCOUT Threat Intelligent Report Available from: https://www.netscout.com/sites/default/files/2021-09/NETSCOUT_ThreatReport2H2021.pdf. Accessed on November 04, 2021. https://doi.org/10.1016/S1361-3723(21)00071-3. NETSCOUT. Cloud in the Crosshairs. Available from: : https://www.netscout.com/sites/default/files/2019-03/SECR_005_EN-1901-E2-WISR.pdf. Accessed on November 03, 2021

86. Nicholson P. Five Most Famous DDoS Attacks and Then Some. Available from: https://www.a10networks.com/blog/5-most-famous-ddos-attacks/. Accessed on November 3, 2020.

87. Nooribakhsh, M., Mollamotalebi, M. A Review on Statistical Approaches for Anomaly Detection in DDoS Attacks. Information Security Journal: A Global Perspective, 2020, 29(3), 118-133. https://doi.org/10.1080/19393555.2020.1717019

88. Moustafa N. The UNSW-NB15 Dataset. Available from : https://www.unsw.adfa.edu.au/unsw-canberra-cyber/cybersecurity/ADFA-NB15-Datasets/. Accessed on October 20, 2020.

89. Odusami, M., Misra, S., Adetiba, E., Abayomi-Alli, O., Damasevicius, R., Ahuja, R. An Improved Model for Alleviating Layer Seven Distributed Denial of Service Intrusion on Webserver. Journal of Physics: Conference Series, 2019, 1235(1), 012020. ,https://doi.org/10.1088/1742-6596/1235/1/012020

90. Özgür, A.,Erdem, H. A Review of KDD99 Dataset Usage in Intrusion Detection and Machine Learning between 2010 and 2015. PeerJ Preprints, 2016, 4, e1954. https://doi.org/10.7287/peerj.preprints.1954

91. Panigrahi, R., Borah, S. A. Detailed Analysis of CIC-IDS2017 Dataset for Designing Intrusion Detection Systems. International Journal of Engineering and Technology. 2018, 7(3.24), 479-482.

92. Parra, G. D. L. T., Rad, P., Choo, K. K. R., Beebe, N. Detecting Internet of Things Attacks using Distributed Deep Learning. Journal of Network and Computer Applications, 2020, 163, 102662. https://doi.org/10.1016/j.jnca.2020.102662

93. Patterson, J., Gibson, A. Deep learning: A Practitioner's Approach. O'Reilly Media, Inc., 2017.

94. Premkumar, M., Sundararajan, T. DLDM: Deep learning-based Defense Mechanism for Denial of Service Attacks in Wireless Sensor Networks. Microprocessors and Microsystems, 2020, 79, 103278. https://doi.org/10.1016/j.micpro.2020.103278

95. Priyadarshini, R., Barik, R. K. A Deep Learning based Intelligent Framework to Mitigate DDoS Attack in Fog Environment. Journal of King Saud University-Computer and Information Sciences, 2019. https://doi.org/10.1016/j.jksuci.2019.04.010

96. Qu, X., Yang, L., Guo, K., Ma, L., Sun, M., Ke, M., Li, M. A Survey on the Development of Self-Organizing Maps for Unsupervised Intrusion Detection. Mobile Networks and Applications, 2021, 26(2), 808-829. https://doi.org/10.1007/s11036-019-01353-0

97. Radford, B. J., Apolonio, L. M., Trias, A. J., Simpson, J. A. Network Traffic Anomaly Detection using Recurrent Neural Networks. arXiv preprint arXiv:1803.10769, 2018.

98. Reading D. DDoS Attacks Jump 542 from Q4 2019 to Q1 2020. Available from: https://www.darkreading.com/threat-intelligence/ddos-attacks-jump-542--from-q4-2019-to-q1-2020/d/d-id/1338208, Accessed on November 03, 2021

99. Reo J. Academic Research Reports Nearly 30,000 DoS Attacks per Day. Available from: https://www.corero.com/blog/academic-research-reports-nearly-30000-dos-attacks-per-day/. Accessed on November 01, 2021

100. Report. DDoS Attacks in Q1 2020. Available from: https://securelist.com/ddos-attacks-in-q1-2020/96837/, Accessed on November 03, 2021.

101. Report (DDoS). Q4 2017 Global DDoS Threat Landscape. Available from: https://www.incapsula.com/ddos-report/ddos-report-q4-2017.html. Accessed on November 06, 2021.

102. Robinson S. DDoS attacks on the Rise: A Closer Look at the Data. Available from : https://bigdata-madesimple.com/ddos-attacks-on-the-rise-a-closer-look-at-the-data/. Accessed on October 26, 2021.

103. Roopak, M., Tian, G. Y., Chambers, J. Deep Learning Models for Cyber Security in IoT Networks. Proceedings of IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, Nevada, United States, January 06-08, 2020, 0452-0457. https://doi.org/10.1109/CCWC.2019.8666588

104. Sabeel, U., Heydari, S. S., Mohanka, H., Bendhaou, Y., Elgazzar, K., El-Khatib, K. Evaluation of Deep Learning in Detecting Unknown Network Attacks. Proceedings of International Conference on Smart Applications, Communications and Networking (SmartNets), South Sinai Governorate, Egypt, December 17-18, 2019, 1-6. https://doi.org/10.1109/SmartNets48225.2019.9069788

105. Saied, A., Overill, R. E., Radzik, T. Detection of Known and Unknown DDoS Attacks using Artificial Neural Networks. Neurocomputing, 2016, 172, 385-393. https://doi.org/10.1016/j.neucom.2015.04.101

106. Sharafaldin, I., Gharib, A., Lashkari, A. H., Ghorbani, A. A. Towards a Reliable Intrusion Detection Benchmark Dataset. Software Networking, 2018, 9(1), 177-200. https://doi.org/10.13052/jsn2445-9739.2017.009

107. Sharafaldin, I., Lashkari, A. H., Hakak, S., Ghorbani, A. A. Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy. Proceedings of International Carnahan Conference on Security Technology (ICCST), Chennai, india, 2019, 1-8. https://doi.org/10.1109/CCST.2019.8888419

108. Shieh, C. S., Lin, W. W., Nguyen, T. T., Chen, C. H., Horng, M. F., Miu, D. Detection of Unknown DDoS Attacks with Deep Learning and Gaussian Mixture Model. Applied Sciences, 2021, 11(11), 5213. https://doi.org/10.3390/app11115213

109. Shurman, M., Khrais, R., Yateem, A. DoS and DDoS Attack Detection using Deep Learning and IDS. International Arab Journal Information Technology, 2020, 17(4A), 655-661.https://doi.org/10.34028/iajit/17/4A/10

110. Singh, K., Singh, P., Kumar, K. Application Layer HTTP-GET flood DDoS Attacks: Research Landscape and Challenges. Computers and Security, 2017, 65(C), 344-372. https://doi.org/10.1016/j.cose.2016.10.005

111. Singh, K. J., De, T. Efficient Classification of DDoS Attacks Using an Ensemble Feature Selection Algorithm. Journal of Intelligent Systems, 2020, 29 (1), 71-83. https://doi.org/10.1515/jisys-2017-0472

112. Singh, K. J., De, T. MLP-GA Based Algorithm to Detect Application Layer DDoS Attack. Journal of Information Security and Applications. 2017, 36, 145-153. https://doi.org/10.1016/j.jisa.2017.09.004

113. Sreeram, I., and Vuppala, V. P. K. HTTP Flood Attack Detection in Application Layer Using Machine Learning Metrics and Bio Inspired Bat Algorithm. Applied Computing and Informatics, 2019, 15(1), 59-66. https://doi.org/10.1016/j.aci.2017.10.003

114. Sumathi, S., Karthikeyan, N. Detection of Distributed Denial of Service using Deep Learning Neural Network. Journal of Ambient Intelligence and Humanized Computing, 2021, 12(6), 5943-5953. https://doi.org/10.1007/s12652-020-02144-2

115. Susilo, B., Sari, R. F. Intrusion Detection in IoT Networks Using Deep Learning Algorithm. Information. 2020, 11(5), 279. https://doi.org/10.3390/info11050279

116. Tama, B. A., Rhee, K. H. Attack Classification Analysis of IoT NEtwork via Deep Learning Approach. Research Briefs on Information and Communication Technology (ReBICTE), 2017, 3, 1-9.

117. Tang, D., Kuang, X. Distributed Denial of Service Attacks and Defense Mechanisms. IOP Conference Series: Materials Science and Engineering, 2019, 612, 1-6. https://doi.org/10.1088/1757-899X/612/5/052046

118. Thakkar, A., Lohiya, R. A Review of the Advancement in Intrusion Detection Datasets. Procedia Computer Science, 2020, 167, 636-645. https://doi.org/10.1016/j.procs.2020.03.330

119. Thing, V. L. IEEE 802.11 Network Anomaly Detection and Attack Classification: A Deep Learning Approach. Proceedings of IEEE Wireless Communications and Networking Conference (WCNC), San Francisco, CA, March 19-22, 2017, 1-6. https://doi.org/10.1109/WCNC.2017.7925567

120. Tripathi, N., Hubballi, N. Application Layer Denial-of-Service Attacks and Defense Mechanisms: A Survey. ACM Computing Surveys, 2021, 54(4), 1-33. https://doi.org/10.1145/3448291

121. Tripathi, N., Hubballi, N. Slow Rate Denial of Service Attacks Against HTTP/2 and Detection. Computers and Security, 2018, 72, 255-272. https://doi.org/10.1016/j.cose.2017.09.009

122. Verma, A., Ranga, V. Statistical Analysis of CIDDS-001 Dataset for Network Intrusion Detection Systems using Distance-based Machine Learning. Procedia Computer Science, 2018, 125, 709-716. https://doi.org/10.1016/j.procs.2017.12.091

123. Wang, H., Li, W. DDosTC: A Transformer-Based Network Attack Detection Hybrid Mechanism in SDN. Sensors. 2021, 21(15), 5047. https://doi.org/10.3390/s21155047

124. Wang, W., Sheng, Y., Wang, J., Zeng, X., Ye, X., Huang, Y., Zhu, M. HAST-IDS: Learning Hierarchical Spatial-Temporal Features using Deep Neural Networks to Improve Intrusion Detection. IEEE Access, 2017, 6, 1792-1806. https://doi.org/10.1109/ACCESS.2017.2780250

125. White Paper. How to Analyze the Business Impact of DDoS Attacks. Available from: https://www.a10networks.com/wp-content/uploads/A10-TPS-WP-How_to_Analyze_the_Business_Impact_of_DDoS_Attacks.pdf. Accessed on November 05, 2021

126. Wu, P., Guo, H. LuNET: A Deep Neural Network for Network Intrusion Detection. Proceedings of IEEE Symposium Series on Computational Intelligence (SSCI), Xiamen, China, December 6-9, 2019, 617-624. https://doi.org/10.1109/SSCI44817.2019.9003126

127. Xu, C., Shen, J., Du, X. Low-rate DoS Attack Detection Method Based on Hybrid Deep Neural Networks. Journal of Information Security and Applications, 2021, 60, 102879. https://doi.org/10.1016/j.jisa.2021.102879

128. Yadav, S., Subramanian, S. Detection of Application Layer DDoS Attack by Feature Learning using Stacked AutoEncoder. Proceedings of International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT), New Delhi, March 11-13, 2016, 361-366. https://doi.org/10.1109/ICCTICT.2016.7514608

129. Yao, Y., Su, L., Lu, Z. DeepGFL Deep Feature Learning via Graph for Attack Detection on Flow-based Network Traffic. Proceedings of MILCOM 2018-2018 IEEE Military Communications Conference (MILCOM). Los Angeles, CA, United States, October 29-31, 2018, 579-584. https://doi.org/10.1109/MILCOM.2018.8599821

130. Yuan, X., Li, C., Li, X. DeepDefense: Identifying DDoS Attack via Deep Learning. Proceedings of IEEE International Conference on Smart Computing (SMARTCOMP).Hong Kong, China, May 29-31,2017, 1-8. https://doi.org/10.1109/SMARTCOMP.2017.7946998

131. Zhang, H., Huang, L., Wu, C. Q., Li, Z. An Effective Convolutional Neural Network based on SMOTE and Gaussian Mixture Model for Intrusion Detection in Imbalanced Dataset. Computer Networks. 2020, 177, 107315. https://doi.org/10.1016/j.comnet.2020.107315

132. Zolotukhin, M., Hämäläinen, T., Kokkonen, T., Siltanen, J. Increasing Web Service Availability by Detecting Application-layer DDoS Attacks in Encrypted Traffic. Proceedings of 23rd International Conference on Telecommunications (ICT). Thessaloniki, Greece, May 16-18, 2016, 1-6. https://doi.org/10.1109/ICT.2016.7500408