Review of Deep Learning Architecture for Detection and Mitigation of Distributed Denial of Service Attacks

Aliyu Sulaiman Mukhtar[1*], Abubakar Tukur[1] & Amina Muhammad[2]

[1]ICT Directorate, Kaduna State University, Kaduna State, Nigeria
[2]Department of Computer Science, School of Applied Sciences, Nuhu Bamalli Polytechnic, Zaria, Kaduna State, Nigeria.
Corresponding Author's email: talk2atk@gmail.com

Abstract: With the emergence of the Corona Virus Disease code named (COVID19), it has necessitated many businesses, and institutions to move their operations and activities to the cloud, thereby making the cloud to produce large volume of data. Organizations and business require real time access to data, provide uninterrupted service to users and clients, interruption to service delivery could be very costly. Modern day attacks on networking infrastructure are growing in frequency, speed and distributed in nature which results in service interruption or denial of service (DOS), Distributed Denial of Service (DDOS). Therefore, the need to utilize Deep Learning (DL) algorithms which have the capability to compute large volume of datasets need not to be overemphasized. The DL has proven to overcome the constraint of shallow algorithms. However, there is need for a comprehensive review on the utilization of DL algorithms in the detection, mitigation and elimination of DDOS Attacks. This paper reviews the most recent research available on DL for mitigation and detection of DDOS. The review aim to provide direction for researchers interested in providing cyber security solutions, to exploit the capabilities of DL algorithms to provide solutions to wider range of domains.

Keywords: Convolutional Neural Network, Denial of Service Attacks, Distributed Denial of Service Attack, Intrusion Detection

INTRODUCTION

Numerous organizations today make use of the internet to deliver variety of services to customers and clients alike.

These services may range from sharing and receiving information, sending, and receiving emails, processing of customers request and information, provision of e-Learning Services, online banking services, entertainment, advertisement, and a host of many other services. Both confidentiality and availability of data stored and processed by servers and other network infrastructures must therefore be protected from unauthorized users and interruptions.

As new IT solutions are invented, cyber security cannot be overemphasized due to the insertion of cyber as the 5th area of combat operations and the promotion of the USA Cyber Command Haider *et al.*, (2020). Attackers launches DDOS on victims to exhaust the hardware resource, or the internet bandwidth which will result in servers not being able to respond to request and provide normal services thereby leading to huge revenue losses Hosseini & Azizi, (2019).

However, attackers possess superior computing capability to run command and control capability to dispatch instructions on vulnerable servers, and host computers to install malware that will enable the attacker to control those vulnerable machines as a result creating DDOS Aamir *et al.*, (2019). DDOS Attacks is still a security risk that is faced by mainstream service providers which amounted to 600Gbps in 2017 alone Wang *et al.*, (2020). DDoS stops the process of exchange of data between communicating devices which could result in loss of internet services like emails, online applications, or application services Saied *et al.*, (2015).

As a result of this security concerns, many solutions have been proposed to Detect, Mitigate the DDOS Attacks from compromising servers, switches, as well as the entire network infrastructure from attackers. However, despite the improvements recorded by many researchers to detect and mitigate DDoS, networking infrastructure are still vulnerable to elevated level of these attacks. Despite findings by industry experts and research from the academia to limit the rate of DDoS attack incidents, the

attacks are still growing rapidly in terms of rate of occurrence and volume of the targeted networks, computers, and many other infrastructures.

A lot of research has been conducted using machine learning algorithms to help find distinct types of attacks which will serve as a guide for network administrators to take an informed decision whenever attacks occur Yin *et al.*, (2017) argue that majority of machine learning algorithm conform to shallow learning algorithms and repeatedly give emphasis to feature engineering and selection, thereby not been able to successfully resolve the enormous task of classification of data present in real world network operating environment. Since data grow rapidly and becomes dynamic, many classifications task will produce results that are less accurate and unsuited for quick analysis and projection requirement of high dimensional learning with gigantic data obligations. Similarly, many DL solutions have been proposed to detect, mitigate DDOS which have yielded good improvements from the conventional solutions that were in existence. Recently, DL, a division of machine learning algorithms, is developing progressively popular and has been useful in finding solutions for many challenging problems which include cyber security, object detection, vehicles, smart cities, smart industries, internet of things, fog computing, cloud computing, intrusion detection, and host of many other challenging areas. Findings have indicated that Deep Learning (DL) absolutely exceeds conventional machine learning algorithms Yin *et al.*, (2017).

Presently to detect DDOS attacks efficiently the proposed solution needs to combine "intelligence" with defense mechanism, and leveraging on DL algorithm's ability to categorize and detect illegitimate or harmful network traffic. Deep Learning (DL) algorithms are highly intelligent, sophisticated, and intelligent enough to learn the fundamental data elements without the system being explicitly programmed to checkmate between usual and abnormal activities Liang & Znati, (2019).

The study aimed to deliver a review of the deep learning algorithms solutions for the detection and mitigation of DDoS attacks. The study reviews and analyses research on DDOS attacks such that comprehensible classification and identification of gap is achieved. Furthermore, the review intends to provide concise summary of deep learning adoption in providing solutions to DDOS Attacks, and to provide stakeholders with recommendation and substantial analysis of the subject matter.

The study will help in providing an understanding of the serious issues associated to this significant network security issue in order to build more comprehensive and applicable defense mechanism, as well as support researchers in the field of network security to identify potential research gap for both new researchers and experts who are fascinated to switch to this research area.

METHODS

The phrase "Deep Learning" stands as the focus of this study as well as its scope. This study adhered to the organized literature review technique.

The study considers studies that adopted DL techniques aimed at solutions to mitigation and detect DDOS Attack, the study did not consider other artificial intelligence algorithms that did not adopt Deep Learning algorithms and limited the scope to only English Literature.

The study follows the guidance provided by Jauro *et al.* (2020) and Thilakaratne *et al.* (2019). Jauro *et al.*'s (2020) work on reviewing deep learning architectures in emerging cloud computing serves as a guide for this study.

Searching the Articles

During the exploration, papers that have been found to be relevant with the selected phrase were scrutinized to pull out further relevant papers within their citations. The search was first carried out from the 8th - 25th September, 2020. The second search period was 5th - 19th October, 2020.

The third and final search that is more dominant than the rest was conducted from 5th November to 24th December 2020.

Academic Databases

The formulated keywords were used to carefully retrieve the literatures.

The study centered on articles from highly regarded peer review Journals, indexed Conference Proceedings, Relevant Thesis, and edited books.

The databases consulted to extract articles used are listed in Table 1. To determine the suitability of the chosen articles, some criteria were applied on the articles obtained from the academic databases. A total of 83 articles were used for the review out of 578,551 articles obtained. Based on

title 345,123 were eliminated. Based on abstract, and conclusion 233,345 articles were rejected.

Table 1: Academic Databases used and their Web

Acade-mic Database	Web Address
ScienceDirect	ScienceDirect
R4http://www.sciencedirect.com/	http://www.sciencedirect.com/
SpringerLink	SpringerLink
Scopus	Scopus
https://www.scopus.com/	https://www.scopus.com/

Deep Learning

DL has been utilized for the enhancement of AI in a multiplicity of domains such as image recognition and processing, pattern recognition, cloud computing development, manufacturing, and computer visualization.

It has reached a drive of extraordinary enhancement in precision of classification and forecasts in multifaceted areas of human endeavor.

DL networks have gained a drive of exceptional enhancement in precision of classification and predictions in many complex tasks. Deep Neural Networks (DNNs) have been proven to be very effective and precise than conventional machine learning techniques Diro & Chilamkurti, (2017). It has seen massive improvement over other AI techniques and machine learning algorithms because of the present-day growth in both hardware components like the Graphical Processing Unit (GPU), and more prevailing algorithms such as the DNN algorithms.

Due to the continuous growth of data and computing capacity, DL algorithms have flourished quickly, and has now been widely utilized in many areas Yin *et al.*, (2017). DL has created a new, contemporary method for image recognition and processing, as well as data analysis, with encouraging outcomes and great ability. it has successfully been used in many fields, for example in agriculture Kamilaris & Prenafeta-Boldú, (2018).

DL is a recent, and a modern method that is suitable for application in many areas, with promising results and large potential. Since the rise of deep learning, it has been successful in many domains, making it to be used for solutions in the domain of computing, trade, manufacturing agriculture and many other challenging area of machine learning such as image recognition, classification, voice recognition, communication, handwriting transcription, natural language processing and translation, self-driving cars, smart cities, cyber security, and other areas.

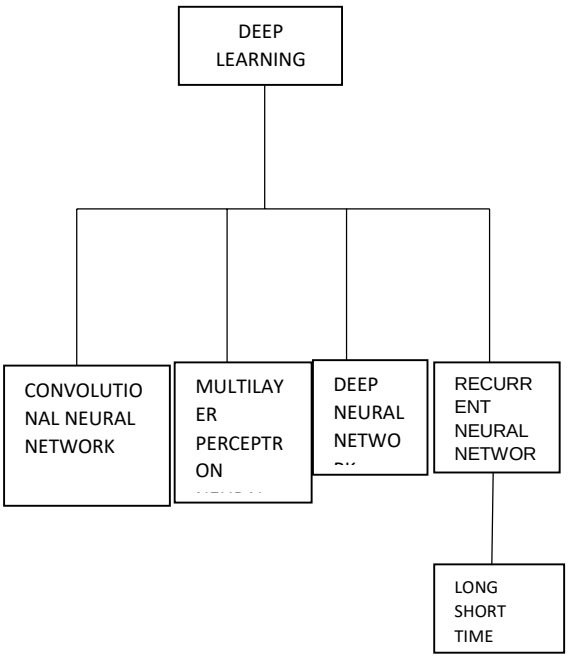


Fig 1: Taxonomy of deep learning Architecture

Deep Learning Algorithm Rudiment

This segment shows the machine learning algorithms found to be used in the literature for mitigating and detection of DDOS attacks. There are many other deep learning algorithms, but this survey only reviews those that adopted Deep Neural Network for mitigation of DDOS attack. A brief background of the algorithms is presented to expose interesting readers to how the algorithms work. Each algorithm is discussed briefly because there is a broad account of the algorithm in the existing literature.

Convolutional Neural Network

Convolutional Neural Network (ConvNet) is a special type of Artificial Neural Network (ANN) that is utilized to distinguish patterns of data efficiently in terms of memory as contrasted to the fully connected CNN (Neural Network) as a result of limited connectivity and common weights Chapaneri & Shah, (2019). ConvNet is comprised of arrangement of two processes,

namely pooling and convolution (sub-sampling), which is put on iteratively on an input of data.
ConvNet was created to in a similar way how the human's visual cortex works and it is the most suited neural network for computer vision (image recognition and processing) and video recognition Shrestha, (2019). ConvNet is a DL algorithm that involves several amounts of layers.
It is mostly suitable for handling task which include classification and recognition of images, recognition and detection of object, processing and recognition of speech, natural language processing, and data analytics, and many other exciting applications which include self driving cars project, robotics, treatments for the blind and visually impaired persons, a full ConvNet architecture is comprised of a Convolutional Layer, an Activation Function Layer (ReLu), Pooling Layer, Fully Connected Layer and a Dropout Layer Wani *et al.*, (2019). Recently CovNet architectures consist of 10 to 20 layers of ReLu, millions of weights, billions of connections that connects units. CovNet applies mathematical operation which is called Convolution. Given two Function f and g the convolution operation is perform as $(f * g)$ where both f and g are given as two different functions Lecun *et al.*, (2015). Given a domain n the result of the convolution function process is given as:

$$(f * g)(n) = \sum_{m} f(m)g(n - m) \quad \text{a)}$$

In time field functions n is replaced by t. The equation can as well be written as

$$(f * g)(n) = \sum_{m} f(n - m)g(m)$$

convolution operation could be applied to perform several alterations in image processing, for example given an input of 2D image represented as H with size of m x n represented as L, 2D feature map denoted as G, with convolutional operation is written as:

$$G(i, j) = (H * L)(i, j) \sum_{m} \sum_{n} H(m, n)L(i - m, j - n)$$

Given that the convolution operation is commutative, the above equation could be expressed as:

$$G(i, j) = (H * L)(i, j) \sum_{m} \sum_{n} H(i - m, j - n)L(m, n)$$

Compared to the input the commutative property holds when the kernel is filliped, but when the kernel is not filliped the convolution operation is exactly as cross correlation operation provided below.

$$G(i, j) = (H * L)(i, j) \sum_{m} \sum_{n} H(i + m, j + n)L(m, n)$$

The elementary structure of CovNet comprises of convolutional layer, pooling layer, input layer, output layer and fully connected layer. Its input layer is utilized to accept diverse data, and make convolution layer to mine features from the input data Jia *et al.*, (2020). Any range of features can be processed when convolution kernel is changed, with the padding parameters, and steps. The pooling layer additionally modernizes features by altering the range of the pooling layer, its steps, and the padding parameters to decrease the volume of the input. However, a fully connected layer associates the classified and mined features non-linearly, the features while the output layer produces the effects of the classification. The designing of CovNet algorithm comprises of back propagation, forward propagation, and test Jia *et al.*, (2020).
Feed forward ConvNet

Every layer of the neural network is consisting of multiple number of neurons, which is represented as follows:

$$f(\sum_{i} y_i z_i + b)$$

with f standing for the activation function, y_i standing for the weight of every neuron, and b stands for the bias of every layer within the CNN. This is done when feed forward executes a complete structure from the input to the output by readjusting CNN activation function, and parameters for the desired result.

Back Propagation
This trains the algorithm's parameters, enhances the model's accuracy. Parameters are updated using gradient decent algorithm. Using y for example parameters are updated as follows:

$$\partial L$$

$$y_{n+1} = y_n - \alpha \times \frac{\partial y}{\partial}$$

Given L as loss function and $\propto$ as the learning rate.

Within each cycle of training, the learning rate is simply the size of the increment of y and b. Nonconvergent or gradual convergence which is triggered by large or small learning rate can be solved using exponential attenuation leaning rate and training rounds to be updated dynamically.

$$\propto = \propto_0 \times \delta_d \frac{global_step}{decay_steps}$$

Given $\propto_0$ as the first value of learning rate, δ_d as attenuation coefficient, $global_step$ as present training round, and $decay_steps$ as attenuation speed.

Loss Function: The Loss Function is the representation of the difference between predictive value and actual value. When the value of the loss function is smaller, then the accuracy of the model becomes high. It is calculated as follows:

$$L = L(\hat{x} - x) + RL$$

Where $L = (\hat{x} - x)$ differentiates the predicted value and the true value. Rectified Linear Unit (ReLU) as the regularized calculation result, Regularization however, reduces overfitting problem and robustly improve the model.

Sliding Average: when the robustness of the model is to be additionally improved y and b as sliding average values are used to update the model. The sliding average will be written as follows given y.

$$f(x') = \frac{1}{1+e^{x'}}$$

$$R(x') = \max(0, x')$$

$$\bar{y} = \beta \times \bar{y} + (1+\beta) \times y$$

$$\beta = min(\beta, \frac{1 + global_step}{10 + global_step})$$

$$\bar{y}0 = y_0$$

3.3 Multilayer Perceptron Neural Network

This kind of architecture contains a single or multiples of hidden layers, output layer and single input layer. Neurons of each layer in the architecture are connecting to another neuron next to it without feedback in Computational neural network regression model for Host based Intrusion Detection System Salgado *et al.*, (2020).

Multilayer Perceptron is of two categories which include the Back Propagation Neural Network (BPNN) and Feed Forward Neural Network (FFNN) Gautam & Om, (2016). It is a NN that applies backpropagation for its training. NN models are stimulated and conceived in a comparable manner of the human brain. however, it exploits some mathematical functions to represent data as input in order to produce the desired output.

The functions work in a manner such that when data is mounted as input, the neural nodes respond by performing calculations using the activation functions through the continuous layers up until the input data is passed on to the output nodes and the outputs are then produced Alimi & Ouahada, (2019). Neural networks activation functions have sigmoid functions and Rectified Linear Units (ReLu) defined as follows.

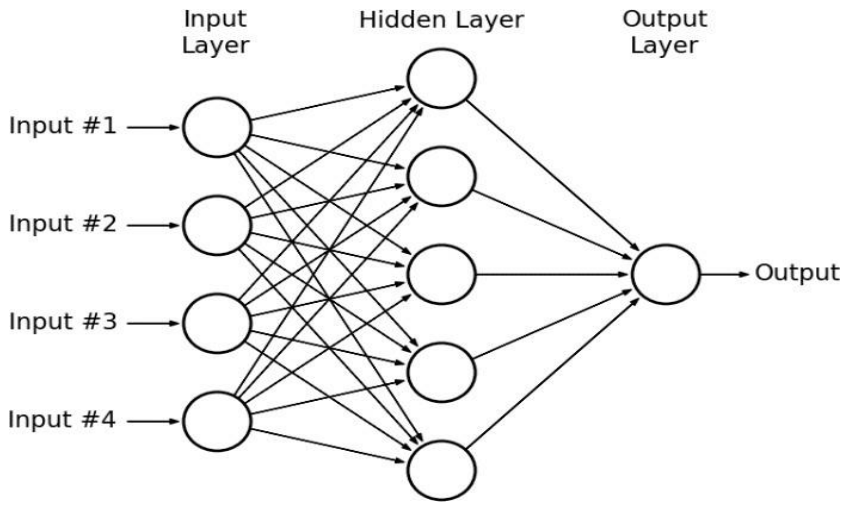


Figure 2: Multilayer Perceptron Neural Network

Deep Neural Network

DNN is the Neural Network that consist of multiple hidden layers Kim, (2018) where every layer within the network gets its input from a layer that is below it, transforms its output and then pushes it to the layer that is above it Paul, (2015).

Deep Neural networks utilizes nature of the composition of natural signals properties which is of hierarchy where features at advanced level are gotten from the lower ones Lecun *et al.*, (2015). For example, when classifying images the Deep Neural Network receives an image as input, then process it to generate vectors scores for each class of object, the object that has the largest number of scores usually belongs to the class of the image Jauro *et al.*, (2020).

However, it is worthy to note that Deep Neural networks are susceptible to overfitting problem which occurs because of a situation where a model is trained and achieves a significantly efficient result with training data, but its performance progressively degenerate when trained with a new data.

This could be solved by introducing an added layer called dropout layer whereby some neurons together with their connections and outgoing edges are selected in random to be dropped completely from the network during the training phase, so that they do not forward pass and backward propagate.

They are inputted back into the network together with their original weights after training, thereafter the overfitting is reduced significantly. The other method is known as Regularization which requires for the increase of the training data set using label preservation technique Shrestha, (2019).

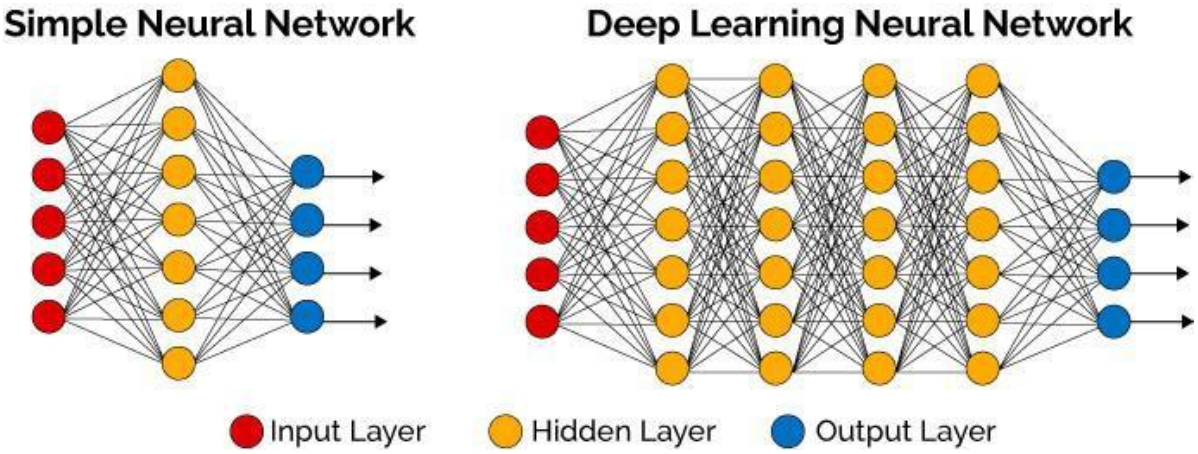


Figure 3: Deep Neural Network

Update is normally done on the weight by gradient decent optimization process at the training phase. Loss function is reduced and the weight changes iteratively using the following process Jauro *et al.*, (2020).

$$W^{t+1}_{ij} = W^{t}_{ij} - \alpha(\partial L/\partial W_{ij})$$

Given W_{ij} as the weights, α signifies the learning rate.

Recurrent Neural Network

RNN is the network whose depth may be or exceed the span of its input data arrangement, and it is trained in both unsupervised and supervised manner Deng *et al.*, (2014).

RNNs has a directional loop which keeps in memory previous information and attach it with the current output, the previous output has a relation with the existing output sequence thereby making all every node within the hidden layer connected to each other, both outputs of the last hidden layer (hidden unit act as the store of the whole network, which remember the end- to-end information) and of the input and the output serves as input to the hidden layer within the network. Pereyra, (2016) when given the sequence vectors ($X1, X2, X3, \ldots . XT$) as input, RNN produces ($h1, h2, h3, \ldots \ldots hT$) as sequence of hidden states (Yin *et al.*, 2017), it is computed at time intervals of as:

$$h_t=\emptyset(W_h\, h_{t-1} + W_x X_t)$$

where W_h represent weight matrix, W_x the input of the hidden weight matrix, and φ as arbitrary activation function.

Recurrent neural network with data from past and future times produces Bidirectional Recurrent Neural Network as follows:

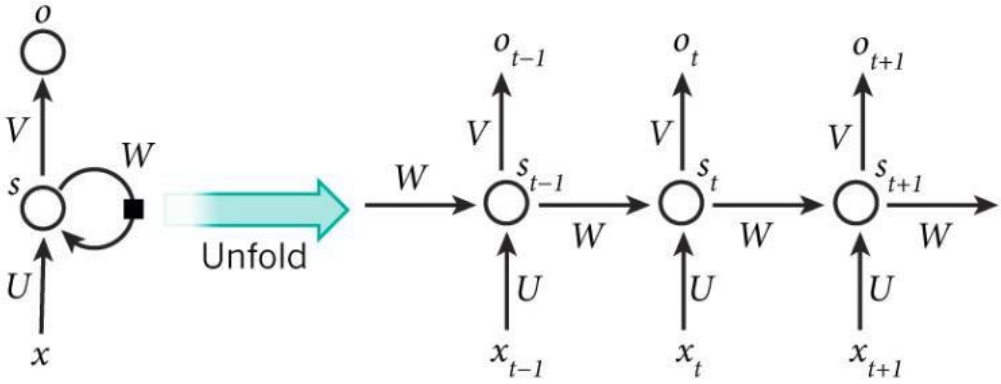
$$\overrightarrow{\overrightarrow{h}} = \emptyset(\overrightarrow{\overrightarrow{W}}\, \overrightarrow{h} + \overrightarrow{\overrightarrow{W}}\, X),$$

$x \quad t$

$$\overleftarrow{h_t} = \emptyset(\overleftarrow{W}\overrightarrow{h}_{t-1} + \overleftarrow{W} X_{x,\ t}$$

$$h_t = [\vec{h}_t : \overleftarrow{h}_t]_t$$

Figure 5: One-unit Recurrent Neural Network (RNN)



In RNN computations parameters U, V, and W are used to represent the weight of the neurons in the network, with W symbolising the weight of the neurons between hidden state S, V symbolising output O and hidden symbolizing states S, U symbolizing the weight of neurons within the inputs X and hidden states S Bediako, (2017).

Long Short Term Memory

LSTM is having the capability to unravel the Vanishing Gradient problem which is discovered regularly with Vanilla RNN by integrating gating function into its state dynamics. LSTM has hidden Vector denoted as h and cell Vector denoted as c, and time interval denoted as t responsible for states update and output to be computed as follows (Pereyra, 2016).

$$i_t = sig(W_{hi}h_{t-1} + W_{xi}X_t$$

$$f_t = sig(W_{hf}h_{t-1} + W_{hf}X_t$$

$$c_t = f_t \odot c_{t-1} + i_t \odot \tanh\,(W_{ht}h_{t-1} + W_{xc}X_t)$$

$$o_t = sig(W_{ho}h_{t-1} + W_{hx}X_t +$$
$$W_{xc}X_t\ h_t = o_t \odot \tanh\,(c_t)$$

where (·) the sigmoid is given as the logistic sigmoid function, tanh is given as the Hyperbolic tangent function, W_h given as the recurrent weight matrices and W_x as the input-to-hidden weight matrices. i_t, f_t and o_t are given respectively as the input, forget and output gates, and
c_t as the cell.

Distributed Denial of Service Attacks

DDOS Attack is a situation where network bandwidth is consumed at an alarming rate to the extent where legitimate users cannot access or make use of specific service. Distributed Denial of Service Attack is infiltrated the same way the conventional Denial of Service Attack is carried out, it usually involves according to Sumathi & Karthikeyan, (2020) an attacker to overflow the target machine with large amount of packets which will result in total exhaustion of computing power and the bandwidth in a "many to one" fashion, thereby denying legitimate users to access computing services, and making the attack complex to avoid and mitigate.

The distributed nature of these attack makes legitimate users to encounter decrease in network performance, loss of data, loss of intellectual property as well as making computer resource scarce and computing power depleted. Since the emergence of Cloud computing, it has become the standard podium for sharing and receiving large volume of data, as it provides many user-friendly features, ease of access and mobility Velliangiri *et al.*, (2020). DDOS attack has more effect on the cloud-based architecture, since cloud computing services are shared and accessed by millions of users all over the world Velliangiri & Selvam, (2018).

The emergence of the internet big tech companies such as yahoo, eBay, amazon, Facebook etc have suffered tremendous loss of revenue due to excessive DDOS attack on their network Kumar & Selvakumar, (2011). DDOS attack is among the most noteworthy problem of accessibility. The attacker aims to reduce the quality of service, or completely collapse the targeted system so that it becomes unavailable for use by legitimate system users SaiSindhuTheja & Shyam, (2021).

Frameworks/Models Adopting DDOS

This section reviews and discuss the studies that adopt DL as a solution mechanism to addressing DDOS.

Convolutional Neural Network

The CovNet has captured the attention of many interests in computer vision benchmark task such as object detection, category level object recognition, and semantic segmentation.

Overtime, it produces remarkably high amount of accuracy when used with large amount of labelled data using GPU high performance computing platforms Deng *et al.*, (2014). This algorithm has self-optimization through learning neurons just like the way it is in traditional Artificial Neural Network. Every neuron within the network gets non-linear function as an input to perform an operation Zaidan & Nan, (2019).

Assis *et al.*, (2020) proposed a Convolutional Neural Network to protect the Software Defined Network (SDN) central controller of ISP (Internet Service Provider) against internal DDoS attacks targeting an external server by analysing the flow and dimensions the IP address, leveraging the distinct features to identify a pattern connecting to the network's regular process and to detect the existence of DDoS attacks near real-time, extracting and analysing IP flow data in per second intervals.

Ghanbari & Kinsner, (2018) proposed an anomaly detection algorithm that is comprised of four stages: namely data preparing stage, data pre-processing stage, data processing stage, and data post processing stage. At the pre-processing stage both source and destination IP addresses, packet length, packet arrival time, protocol for every packet are collected and classified as normal or anomalous and passed to the next stage. Arrival time series signal that is computed at the pre-processing stage is collected and passed for feature extraction; this is done in two ways. The processing is done by the CovNet which consist of six layers, the layers are the input layer, rectified linear unit (ReLU), pooling layer, convolutional layer, normalization layer, and fully connected layer. The post processing stage is used to eliminate the duration of training the CovNet using SVM algorithm at the post processing stage.

Jia *et al.*, (2020) proposed a CovNet based solution to protect resource Adaptation Resolution Server (RARS) against DDOS in a

Smart Identifier Network (SINET). RARS is the device that is most susceptible to attack in SINET because of its comprehensive outlook of the network, which requires it to observe and gather information about the network topology, network components, and vigorously organizes service obligations with network communities. This model detects DDOS based on its characteristic such as the unpredictability of the base addresses service request packets. When suspicious connection is found, the connection is moved to a backup server which is equipped with CovNet solution so that the connection can be accurately determined to be a suspicious traffic or legitimate traffic. Chapaneri & Shah, (2019) conducted an experiment using deep CovNet architecture on the dataset UNSW-NB15 to resolve the difficulty of malicious network traffic and multi class classification of normal, the experiment was able to ascertain a significant improvement in terms of performance with deep one-dimensional CovNet architecture compared to shallow algorithms.

Shaaban *et al.*, (2019) proposed a CovNet solution to mitigate and detect DDOS attacks on Mission control Centre (MCC) which is saddle with the responsibility of controlling the spacecraft. The technique used 5 algorithms to help classify between suspicious traffic from normal. Based on their analysis and results obtained the CovNet achieved 99% accuracy compared to other classifiers used. A Deep hybrid CovNet Ensemble Framework to efficiently detect and mitigate DDOS attacks is proposed by Haider *et al.*, (2020) the authors assessed their version with other hybrid models based on flow based SDN dataset. Better accuracy of mitigation and detection of DDOS was achieved evaluated against other models.

Table 2: Summary of CovNet algorithms strength, limitations and suitability

REFERENCE	ALGORITHM(s) USED	ALGORITHM(s) COMPARED WITH	RESULT	LIMITATION
(Alguliyev *et al.*, 2019)	Improved CNN, Improved LSTM.	Classical CNN, Classical LSTM.	Outperform the compared algorithms.	the model is only trained on Twitter data.
(Chen *et al.*, 2019)	multi-channel CNN(MC-CNN).	C4.5, KNN, LSTM, CNN, SVM.	Outperform single channel CNN, LSTM, and shallow models.	Performance is limited when training data is quite deficient.
(Hwang *et al.*, 2019)	Convolutional Neural Network (CNN).	Not compared.	CovNet performed considerably well.	Difficult to measure the effectiveness of the proposed model due to lack of comparison.
(Yu *et al.*, 2021)	hierarchical packet byte-based CNN	Studies in terms of metrics and Computation time.	Outperformed the compared algorithms in terms of training with the CIC-IDS2017 and CSE-CIC-IDS2018 datasets	Evaluated to detect little sample problem On the two Datasets for intrusion detection.
(Roopak *et al.*, 2019)	CNN+LSTM, MLP (Multilayer Perceptron), 1d- CNN, LSTM.	MLP (Multilayer Perceptron), 1d- CNN, LSTM.	CNN+LSTM outperformed the compared algorithms with 9.20%.	The training was carried out on an unbalanced dataset.

Multilayer Perceptron Neural Network

The MPNN has become the frequently used neural network including the feed forward NN, this is due to its fast means of operation, requires limited number of training set, and it is easy to be implemented Orhan *et al.*, (2011).

Wang *et al.* (2020a) proposed dynamic MLP as the adopted classifier and utilised wrapper feature selection that is used to choose the optimum features which consist of three modules: Detection module, knowledge base, and feedback mechanism.
The knowledge base module consists of two labelled datasets, one consists of data sections that are used for training the detection model while the other one labels and classified the produced data by the model through the detection process. The detection model handles classifying incoming data samples as normal traffic or attack traffic. While the feedback mechanism detects considerable amount of detection errors produced by the knowledge base module.
A Multilayer Perceptron with a Genetic Algorithm (MLP-MLP-GA) proposed by Singh & De (2017) analyses the retrieving behaviour of system invaders and normal users on an application layer type of attack. The model accepts as input for classification
the four metrics which include the number of IP addresses, HTTP count, constant mapping, or concentration of the IP addresses, and frame length, and then analysed them all in perspective to attack or normal behaviour. When the model suspects an IP address to be an attack, the system confirms the IP address using the conventional CAPTCHA. Results obtained reveal that the model delivered detection accuracy of 98.04% on application layer DDoS attack, and a False Positive ratio of 2.21%.
Singh *et al.*, (2016) proposed an MLP together with Genetic Algorithm learning and trained on a dataset EPA HTTP (Environmental Protection Agency-Hypertext Transfer Protocol) to classify attackers and normal clients depending on the amount of HTTP requests, the randomness of the received packets, and change of the entropy. The model is comprised of three layers, with the input layer consisting of input pattern of 3, three hidden neurons, and output neuron. They achieved accuracy of 98.32%, sensitivity rate of 0.9962, and specificity rate of 0.0561.
Hosseini & Azizi (2019) proposed a hybrid technique that comprises Multilayer Perceptron (MLP), decision tree, naïve Bayes, and random forest, In this technique the computational loads are shared between the client and proxy sides based on their resource. The client side deals with data collection, feature extraction and divergent test. The client part can detect attacks when the divergence is bigger than the threshold, otherwise the data is pushed to the proxy side which contains the hybrid solution to effectively detect and classify the data to either attack or normal traffic, however the random forest algorithm outperformed the compared algorithms proposed.

Table 3: Summary of Multilayer Perceptron algorithms limitations, suitability and strength

REFERENCE	ALGORITHM(s) USED	ALGORITHM(s) COMPARED WITH	RESULT	LIMITATION
Maranhao *et al.*, (2021)	(MLP)	Higher Order Orthogonal Iteration (HOOI)+ MLP, Higher Order Singular Value Decomposition + MLP	Out performs the compared algorithms.	The model is more prone to false positive, thereby classifying legitimate traffic as malicious.

Moghanian *et al.*, (2020)	(MLP), Grasshopper Optimization Algorithm (GOA)	Support Vector Machine (SVM), decision tree (DT)+PSO algorithm, Random Forest.	Out performs the compared algorithms.	When the Number of grasshopper are increased the model detection is decreased.
Almeida *et al.*, (2016)	(MLP) with Limited Weights.	(MLP) with Normal Weights.	Out performs the compared algorithm.	The model consumes more ROM memory relative to the compared algorithm.
Lee *et al.* (2020)	(MLP), Convolutional NeuralNetwork (CNN), Long Short-Term Memory (LSTM) and Stacked Auto-encoder (SAE).	Convolutional Neural Network (CNN), Long Short- Term Memory (LSTM) and Stacked Auto-encoder (SAE).	Out performs the compared algorithm.	The model was trained with flow-based traffic only, it did not include any payload data.
Wang *et al.* (2020)	Dynamic multilayer perceptron (MLP).	MLP, RNN, SVM.	Outperforms the compared algorithms.	Possibility of the model to generate false positive and false positive feedbacks.

Deep Neural Network

DNN is the ideal algorithm to be used in resource constraint network, its key features include unsupervised pre-training, lack of manual feature engineering, and compression capabilities which in turn result to higher accuracy and faster processing, these has been observed in big companies which include the likes of Google and Facebook Diro & Chilamkurti, (2017).

Sumathi & Karthikeyan, (2020) proposed a deep neural network classifier that analyses both the network traffic and attack the system utilizes KDD Cup (Knowledge Discovery and Data Mining), DARPA 1999 (Defence Advanced Research Projects Agency), DARPA 2000, and CONFICKER datasets. Statistical features are obtained from the flow of the network traffic and processed within the pre-processing stage and store incoming packets into a server which will serve as input to the TCP trace. The result shows that 98.9% accuracy of detection using KDD dataset, detection accuracy on mixed dataset 98.1%, and accuracy of detection on SSE dataset 98.1%.

Asad *et al.*, (2019) proposed a model that utilises back-propagation, feed-forward architecture with 7 hidden layer to separate between normal and attack traffic, this is achieved by routing network traffic to pass through the model to enable the system mitigate against application layer DDOS. The technique achieved 98% accuracy on the Canadian dataset (Canadian Institute for Cyber) IDS 2017CIC or DDOS detection.

Table 4: Summary of Deep Neural algorithm limitations, suitability and strength,

REFERENCE	ALGORITHM(s) USED	ALGORITHM(s) COMPARED WITH	RESULT	LIMITATION
Ramesh *et al.*, (2021)	Deep Neural Network	Not compared	The DNN requires a smaller amount of time for detection.	The model was trained with datasets that only cover security surveillance areas.
Chamou *et al.*, (2019)	Deep Neural Network.	Multi-Layer Perceptron, Deep Neural Network.	Outperformed the compared algorithms.	The model does not explicitly determine the type of the attack.
Agarwal *et al.*, (2021)	(DNN), Feature Selection- Whale Optimization Algorithm (FSWOA).	(SVM), (ANN), (KNN).	Outperformed the compared algorithms.	Relatively consumes time due to encryption and decryption of sensitive data.

Makuvaza et Al., (2021)	Deep Neural Network (DNN).	Restricted Boltzmann Machine (RBM) + SVM, Gated Recurrent Unit (GRU) + Recurrent Neural Network (RNN).	Outperformed the compared algorithms	The trained data set contains big files, so requires Large RAM (Random Access Memory).
Amma & selvakumar, (2021)	Tuned vector CovNet (TVCDNN).	MLP and SVM, VCDeepFL.	Outperformed the compared algorithms.	Degree of performance is dependent on changing the structure and parameters of the algorithm.

Recurrent Neural Network

This model is unique, with features that mimics how the human brain works, it utilizes its internal memory to process arbitrary arrangements of inputs, and execute complex task which includes pattern recognition thereby making it suitable for achieving real-time leaning task considering its ability to compute time series data Thilina *et al.*, (2016).

Kim *et al.*, (2020) proposed both CovNet and RNN based intrusion detection model with focus on DDOS attack. The authors adopted KDD CUP 1999 dataset which has forty one features of traffic and one feature that will decides the location of each data item, within the forty one traffic features thirty-eight are presented in figures and 3 in symbolic features, CSE-CIC-IDS2018 data set with 78 numerical features for training the models and classified using binary and multiclass classifications.

The CovNet model achieved 99% accuracy or more with both binary and the multiclass classification, while the RNN achieved accuracy of 99% with binary classification and 93% accuracy with multiclass classification. With the CSE-CIC- IDS2018 data set the binary classification achieve 2% accuracy and multiclass classification achieve 73.5% accuracy.

SaiSindhuTheja & Shyam, (2021) proposed an RNN as model together with Oppositional Crow Search algorithm (OCSA) and Oppositional Based Learning (OBL) and used KDD cup 99 data set for the experiment. The model has three modules namely attack detection using RNN, pre-processing, feature selection using OCSA. The experiment results shows that the proposed model outperforms other techniques by 98.18%, 95.13%, 93.56%, and 94.12% relative to Precision, F-Measure, Recall, and Accuracy, respectively.

Elsayed *et al.*, (2020) designed a DDOS detection model which combines Autoencoder with Recurrent Neural network. the model was trained with the CICDDoS2019 dataset is used. All the socket features such as originating and end point IP, originating and end point port, times- tamp, and flow ID, were removed. The results obtained after training the model indicates that the model performs high in terms of recall, precision, F-score, and accuracy.

Table 5: Summary of Recurrent Neural algorithm strength, limitations and suitability

REFERENCE	ALGORITHM(s) USED	ALGORITHM(s) COMPARED WITH	RESULT	LIMITATION
Xu *et al.*, (2018)	RNN with (GRU), (MLP) and SoftMax module.	LSTM and GRU, LSTM, RNN.	Outperform the compared algorithms.	**The model could not effectively detect R2L and U2R attacks.**
Almiani *et al.*, (2020)	Recurrent Neural Network.	Not compared.	The model's performance in terms of detection rate of DoS is quite good.	**The model's detection rate of R2L attacks is quite poor.**
C. Li *et al.*, (2018)	RNN (RNN) + Restricted Boltzmann Machines (RBM).	KNN,SVM, Decision Tree, Random Forests, and Bayes.	Outperformed the compared algorithms.	**The model used DARPA1998 which does not contain modern attack signatures.**
Tang *et al.*, (2018)	(GRU-RNN).	SVM, DNN, NB Tree.	Outperformed the compared algorithms.	**The model causes an overhead on the controller.**
Dinh & park, (2021)	**Recurrent Neural Network.**	**(SVM), (NN), and 1 class SVM.**	**Outperforme d the compared algorithms.**	**The proposed model detects both YOYO and SLOWLORIS attacks with very high degree of difficulty.**

Long Short-Term Memory Neural Network

Long Short-Term Memory (LSTM) network has been established to be successful in identifying the diverse arrangements of variation of conditions over a period, by linking long time lags between related target output and input, it has theoretically been proven to be well suited and powerful architecture for classification, with applications in machine translation, natural language recognition and processing, Image processing and recognition, and so on Mcdermott *et al.*, (2018).

LSTM was invented to prevent long dependency problems which can recall extensive past information. This is achieved by examining its movement of information within an extended period, however its accuracy to detect can be improved (Y. Li & Lu, 2019).

Priyadarshini & Barik, (2019) Proposed Source based DDoS defense mechanism that may be applied to both fog environment and cloud computing in SDN (software Defined Network) environment to mitigate transport/network layer DDOS by blocking the infected packets from being spread to the server and transmission to the cloud, by doing so the entire fog network is protected, the results indicated that the LSTM achieved 98.88% accuracy on testing data set.

However, the constraint of the work is it only has two levels DDOS which are Transport and

Network were considered. Y. Li & Lu, (2019) proposed a combination of LSTM and Bayes approach to detect DDOS by examining the network traffic using probability of prediction, DDOS attacks are determined by the extent of its predictive value, while normal traffic distinguished with low predictive value, whereas the predictive values that fall in between high and low of the bayes component of the model is used to recognize the DDOS.

Zhao *et al.*, (2020) proposed Federated Learning LSTM (FL-LSTM) framework whose primary target is to check and detect substantial risk and malicious activity or behaviour ranging from directory traversal attacks, bulk uninstallation of software, simultaneously bulk reading and deleting of files on all user servers. Thereafter, each user server is trained, and its results are obtained and pushed to the central server which then performs parameters aggregation to generate a new model that is spread to individual user servers.

Gadze *et al.*, (2021) investigated a deep learning model consisting of LSTM, and CovNet. The models emphasized on ICMP flooding attacks which target the controller, TCP, and UDP attacks. This model collects information regarding source and destination IP, protocol (TCP, UDP, ICMP), number of packets of each flow, number of packets transmitted and received by each switch on the network, the model achieved 89.63 accuracy.

Liang & Znati, (2019) presented an LSTM scheme which was trained with the CICIDS 2017 datasets. This scheme detects malicious traffic by observing a modest number of sequences of packets from the network traffic, these quite small packets of the network flow serve as both input, output of the model. Results gotten from their experiment shows that the LSTM model performs better than other conventional machine learning models.

Similarly, Li & Lu, (2019) presented a DDOS detection method which combines Bayes algorithm and LSTM. Incoming data is pre-processed and sent in as input to the LSTM module to detect DDOS. However, if the prediction results obtained from the LSTM is not reliable enough the bayes algorithm is then fed with this data as input for a more comprehensive detection. The result attained from the experiment indicates that the model achieved a reliable performance compared with other methods with 98.15% accuracy.

Table 6: Summary of Long Short Term (LSTM) algorithm strength, limitations and suitability

REFERENCE	ALGORITHM(s) USED	ALGORITHM(s) COMPARED WITH	RESULT	LIMITATION
M. Kim, (2019)	LSTM,basic neural network (BNN).	Not compared.	The algorithms detect DDOS by renewing its learning parameters.	New attack component needs to be Studied in advance.
Shi *et al.*, (2019)	(LSTM).	Not compared.	The model filters abnormal traffic flow from normal traffic flow with very negligeable computational cost.	The method depends on 5 successive packets to efficiently detect DDOS attacks.

Sun *et al.*, (2019)	Bi-LSTM.	Not compared.	The method carefully mines and examine key attributes of the SDN Architecture.	The effectiveness of the model depends on changing firewall configuration.
Roopak *et al.*, (2020)	Long short-Term Memory (LSTM), CoVNet (CNN).	MLP,(SVM), Ransom Forest and Bayes algorithms.	Outperformed the compared algorithms.	The model's training time is reduced by 5 folds because of the application of feature selection before classification.
Roopak *et al.*, (2019)	MLP (Multilayer Perceptron), 1d-CNN,LSTM, CNN+LSTM.	CNN+LSTM.	CNN+LSTM performed better than other DL algorithms used.	The model does not work on unbalance dataset.
P. Singh *et al.*, (2021)	(LSTM), (GRU).	Not compared.	The model achieved a very impressive result based on the UNSW2015 dataset.	The UNSW2015 dataset is quite a small dataset. Therefore, the model could not be said to be very effective in detecting DDOS.

Hybrid Deep Leaning Algorithms to Solving Real World Problem

This section provides a summary of hybrid algorithms that have been used to develop DDOS detection and mitigation models. DL technologies are swiftly spreading due to the merging of two key reasons: improvements of modern hardware technologies, extraordinary attraction data analytics, with many DL techniques achieving unprecedented result in many research areas
Zaidan & Nan, (2019). Therefore, it is worthy to note that every algorithm has its scope, limitation, and proper area of application as regards solving real world problems as summarized below.

Table 7: Summary of Hybrid algorithms strength, limitations and suitability

REFERENCE	ALGORITHM(s) USED	ALGORITHM(s) COMPARED WITH	RESULT	LIMITATION
Saisindhuthej a & shyam, (2021)	Recurrent Neural Network (RNN) Oppositional Crow Search Algorithm OCSA and	GA+RNN based intrusion detection system, FA+RNN based intrusion detection system, and CSA+RNN based intrusion detection System	Performed significantly better with a Precision of (98.18%), Recall (95.13%), F-measure (93.56%), and Accuracy (94.12%).	The model does not provide for real time DDOS attack detection and prevention in multi-cloud environment.
Rehman *et al.*, (2021)	(RNN), (GRU) aims, Naive Bayes (NB), Sequential Minimal Optimization (SMO).	KNN, LSTM-2, MLP, PSO-DS, and SVM.	The model produced encouraging feat based on accuracy, precision, recall, and F1-score.	The study did not provide for intrusion detection, which when Included will effectively detects DDOS.
Nguyen *et al.*, (2021)	BI-LSTM (Bidirectional LSTM), Gaussian Mixture Model (GMM)	Not compared	The model performed extremely good on known attack signatures.	Capable of detecting only known attack signatures, Inability to Eliminate the need for traffic engineer's intervention, the Gaussian Mixture Model operates in a trial-and-error fashion.

Ugwu *et al.*, (2021)	LSTM, Singular Value Decomposition (SVD).	(NB), (DT), and Support Vector Machine (SVM).	Accuracy of 94.28% and 90.59% were obtained.	The model performance relative to the results obtains signifies low performance compared with shallow algorithms.
Atefinia & Ahmadi, (2021)	Deep Feed-Forward Module (DFFM), A Stacked Restricted Boltzmann Machine Module (SRBMM), long short-term memory (LSTMM).	Not compared	The model achieved an unprecedented 100% on accuracy.	Does not include Nmap or Metasploit traffic detection.
Catak & mustacoglu, (2019)	Deep Neural Network, Autoencoder.	Not compared	The model detects DDOS faster on a GPU system.	It does not consider source IP as part of detection properties.
Barati *et al.*, (2014)	Multilayer Perceptron, Genetic Algorithm (GA)	Not compared	Performed Better with remarkably high degree of attack instance detection of up to 99.98%.	The model needs to be tested on different data set to ascertain its degree of detection capability.
Wankhede & kshirsagar, (2018)	Multilayer Perceptron, Random Forest.	Random Forest, Multilayer Perceptron	Random Forest performed better than the Multilayer Perceptron algorithm.	Designed to detect application layer attacks only. Does not classify the data set into the multiple classes of attacks, of attacks, only DoS and Benign.

Liu *et al.*, (2020)	Deep Convolution Neural Network (DCNN),Deep Reinforcement LearningQ- network.	(SVM), K-means, Surface Learning Neural Network.	Takes shorter time to classify and detect attacks, efficiently. Improves DDoS attack detection in edge computing environment.	performanc e is low when the training data is a sparce data.

Challenges Of Network Attacks

With the advent of the Corona Virus pandemic code named Covid19, the need for enterprise networks, the internet, and online services to manage and create businesses has increased tremendously due to lockdowns enforced by governments, with movements of people restricted across the world, this necessitated businesses formal and informal to conduct their activities in a different way.

These activities normally conducted in office complex and open space, are now available online. Even schools, colleges and universities must have to administer lessons, lectures as well as assess students virtually, normal meetings are now held online through the popular zoom app and google meet app and host of many other meeting applications. With the vast improvement of Internet Technologies, Applications, and Protocols, analyzing legitimate and illegitimate network traffic is proving to be extremely difficult, there is need for network traffic data to be analyzed in real time to differentiate between attack, and normal network traffic Ji *et al.*, (2016).

This situation has made networks and networking infrastructure extremely vulnerable to attacks with intrusions by hackers and unauthorized users at an all-time high, therefore network security needs to evolve due to the variety of the challenges faced by network administrators and the continued varying nature of modern-day attacks.

Distributed Denial of Service Attack Data Set

This segment is intending to provide some of the best-known datasets used for the Mitigation and Detection of DDOS Attacks to help new researchers with the dataset to be used when embarking on research for this important network security area, similarly it will aide experts with variety of sources as well.

KDD CUP

The KDD CUP 99 is a standard dataset for intrusion detection produced by the MIT laboratory; it comprises four type of attacks which include DOS, R2L, Probe, and U2R and normal network connection records with each category consisting of forty-one features which is segmented into 7 characters, thirty-four number of features Zaidan & Nan, (2019).

Sumathi & Karthikeyan, (2020) utilized DARPA 1999, DARPA 2000,KDD Cup, and CONFICKER datasets. The technique achieved 98.1%, 99%, and 98.9% of detection accuracy for mixed data set, KDD dataset, and SSE dataset. Similarly, the authors (J. Kim *et al.*, 2020) used KDD CUP and CSE-CIC-IDS2018 datasets to develop their CovNet model and evaluates its performance with Recurrent Neural Network, the CovNet model achieved 99% results in binary and multiclass classifications, the RNN showed 99% accuracy in binary classification and 93% in multiclass classification.

NSL - KDD Data Set

This dataset contains forty-one features comprising three none numeric features, 38 are numeric features Kasongo & Sun, (2020). The authors Kasongo & Sun, (2020) presented a wireless intrusion detection system with deep long short-term memory-based classifier, the system achieved overall accuracy on validation data was 99.51%, the F1-Score was 99.43% and the accuracy on test data was 86.99%.

Ji *et al.*, (2016) proposed an IDS based classifier using a Deep Long Short-Term Memory, the

DLSTM IDS was compared to current methods such as DFF Neural Networks, SVM, k-Nearest Neighbors, Naïve Bayes and Random Forests. The DLSTM IDS was able to achieve data of 99.51%, F1-Score of 99.43% and the accuracy on test data was 86.99%.

CSE-CIC-IDS2018

CSE-CIC-IDS2018 dataset is a collective work between the Communications Security Establishment (CSE) and the Canadian Institute for Cyber Security (CIC) aimed to produce datasets to test, evaluate and analyze intrusion detection systems, with special attention to anomaly detectors.

CSE-CIC-IDS2018 is multi-class in nature, it has more than 16,000,000 instances, and is as well class-imbalanced. This data set also contains numerous - attack instances which includes Brute force, Botnet, DoS, DDoS, Web attack, penetration of the network from within the network Volkov & Kurochkin, (2020).

Kim *et al.*, (2020) developed a CovNet model that utilizes the more advanced DoS attacks contained in the **CSE-CIC-IDS2018** dataset, thy achieved 91.5% of accuracy on average and was compared to RNN model which attained 65% of accuracy on average. Volkov & Kurochkin, (2020) used **CSE-CIC-IDS2018** dataset to develop an LSTM based model for intrusion detection in SDN environment. An assessment was carried out to know the working effectiveness between complex and simple neural network with several parameters being put to consideration. The **CSE-CIC-IDS2018** can be found on this link https://www.unb.ca/cic/datasets/ids-2018.html.

THE DOMAİN OF APPLİCATİONS OF DL İN CYBER SECURİTY APPLİCATİONS

Cybercrime still poses an increasing task in terms of security and privacy practices. Deep Leaning has been applied in many fields such as cyber security in recent years due to its enormous ability to use input samples to obtain best feature representation.

It is found useful to be applied in several problems in cloud security such as intrusion detection, Surveillance, DDOS Attacks, Eavesdropping, malware classification, android malware detection, jamming, Anomaly Detection, Parallel Attack Detection, spam, phishing, and binary analysis. As application of deep leaning architectures in cyber security increases, many domains and sub domains will emerge.

RECOMMENDATİONS

The comprehensive review of deep learning architectures for the detection and mitigation of Distributed Denial of Service (DDoS) attacks provides valuable insights into the current state of cybersecurity in the context of cloud-based operations. To further advance this field and contribute to the ongoing efforts in securing digital infrastructures, researchers are recommended to consider the following areas for future exploration:

i. Enhanced Deep Learning Models: Investigate novel architectures and variations of deep learning models tailored specifically for DDoS detection and mitigation. Explore the integration of attention mechanisms, transfer learning, and reinforcement learning to enhance the robustness and adaptability of existing models.
ii. Real-Time Detection Mechanisms: Develop and optimize real-time DDoS detection mechanisms that can operate efficiently in dynamic cloud environments. Emphasize the reduction of false positives and negatives, ensuring timely response to emerging threats without disrupting legitimate traffic.
iii. Adaptive and Resilient Algorithms: Explore the development of adaptive algorithms that can dynamically adjust to evolving DDoS attack strategies. Consider incorporating self-learning mechanisms that enable the system to continuously adapt and enhance its resilience against sophisticated attacks.
iv. Collaborative Defense Mechanisms: Explore collaborative defense mechanisms that involve sharing threat intelligence and mitigation strategies among different entities within the cloud ecosystem. Investigate how collaborative efforts can enhance the overall resilience against large-scale DDoS attacks.

v. User-Friendly Implementation: Consider the development of user-friendly tools and platforms that enable organizations with varying technical expertise to implement deep learning-based DDoS mitigation effectively. Streamline the integration process and provide comprehensive documentation for seamless adoption.

By focusing on these areas, researchers can contribute to the evolution of effective and adaptive cybersecurity solutions, ultimately strengthening the resilience of cloud-based infrastructures against the growing threat of DDoS attacks

.

CONCLUSİON

This study analyzed and reviewed DL Architectures that have been applied in solving DDOS problem. The major DL architectures found to be widely used for solving DDOS were discussed into clear taxonomy, brief background of the algorithms is presented to expose interesting readers how the algorithms work to achieve their aim. Related works were also studied thoroughly and classified. CovNet has been found to generate a lot of interest from researchers in this field, followed by Recurrent Neural Network.

It is believed that deep learning will continue to thrive and yield significant results that will outweigh the results already gotten from the conventional machine learning algorithms because of the high interest shown by researchers in the field.

AUTHORS CONTRIBUTION

Author *1: Conceptualization, investigation, writing review and editing, methodology, resources, supervision and visualization.

Author 1: Investigation, validation, visualization, supervision, editing, project administration and funding acquisition.

Author 2: Validation, supervision, funding acquisition and methodology

REFERENCE

Aamir, M., Mustafa, S., & Zaidi, A. (2019). Clustering based semi-supervised machine learning for DDoS attack classification. *Journal of King Saud University - Computer and Information Sciences*, *xxxx*, 1319–1578. https://doi.org/10.1016/j.jksuci.2019.02.003

Agarwal, A., Khari, M., & Singh, R. (2021). Detection of DDOS Attack using Deep Learning Model in Cloud Storage Application. *Wireless Personal Communications*, *0123456789*. https://doi.org/10.1007/s11277-021-08271-z

Alguliyev, R. M., Aliguliyev, R. M., & Abdullayeva, F. J. (2019). The improved LSTM and CNN models for DDoS attacks prediction in social media. *International Journal of Cyber Warfare and Terrorism*, *9*(1), 1–18. https://doi.org/10.4018/IJCWT.2019010101

Alimi, O. A., & Ouahada, K. (2019). Real Time Security Assessment of the Power System Using a Hybrid Support Vector Machine and Multilayer Perceptron Neural Network Algorithms. *Sustainability*, *11*(13), 9. https://doi.org/doi:10.3390/su11133586

Almeida, F. M. De, Ribeiro, A. D. R. L., Moreno, E. D., & Montesco, C. A. E. (2016). Performance Evaluation of an Artificial Neural Network Multilayer Perceptron with Limited Weights for Detecting Denial of Service Attack on Internet of Things. *The Twelfth Advanced International Conference on Telecommunications II.*, *c*, 82–87.

Almiani, M., AbuGhazleh, A., Al-Rahayfeh, A., Atiewi, S., & Razaque, A. (2020). Deep recurrent neural network for IoT intrusion detection system. *Simulation Modelling Practice and Theory*, *101*, 102031. https://doi.org/10.1016/j.simpat.2019.102031

Amma, N. G. B., & Selvakumar, S. (2021). Optimization of vector convolutional

deep neural network using binary real cumulative incarnation for detection of distributed denial of service attacks. *Neural Computing and Applications*, *8*. https://doi.org/10.1007/s00521- 021-06565-8

Asad, M., Asim, M., Javed, T., Beg, M. O., Mujtaba, H., & Abbas, S. (2019). DeepDetect : Detection of Distributed Denial of Service Attacks Using Deep Learning. *The Computer Journal*, *63*(7), 938–994. https://doi.org/10.1093/comjnl/bxz064

Atefinia, R., & Ahmadi, M. (2021). Network intrusion detection using multi-architectural modular deep neural network. *Journal of Supercomputing*, *77*(4), 3571–3593. https://doi.org/10.1007/s11227-020-03410-y

Barati, M., Abdullah, A., Udzir, N. I., & ... (2014). Distributed Denial of Service detection using hybrid machine learning technique. *Biometrics and …*, 268–273. https://ieeexplore.ieee.org/abstract/document/7013133/

Bediako, P. K. (2017). *Long Short-Term Memory Recurrent Neural Network for detecting DDoS flooding attacks within TensorFlow Implementation framework* . Lule˚a University of Technology.

Catak, F. O., & Mustacoglu, A. F. (2019). Distributed denial of service attack detection using autoencoder and deep neural networks. *Journal of Intelligent and Fuzzy Systems*, *37*(3), 3969–3979. https://doi.org/10.3233/JIFS-190159

Chamou, D., Toupas, P., Ketzaki, E., Papadopoulos, S., Giannoutakis, K. M., Drosou, A., & Tzovaras, D. (2019). Intrusion detection system based on network traffic using deep neural networks. *IEEE International Workshop on Computer Aided Modeling and Design of Communication Links and Networks, CAMAD*, *2019-Septe*, 1–6. https://doi.org/10.1109/CAMAD.2019.8858475

Chapaneri, R., & Shah, S. (2019). Detection of Malicious Network Traffic using Convolutional Neural Networks. *2019 10th International Conference on Computing, Communication and Networking Technologies, ICCCNT 2019*, 6–11. https://doi.org/10.1109/ICCCNT45670.2019.8944814

Chen, J., Yang, Y. tao, Hu, K. ke, Zheng, H. bin, & Wang, Z. (2019). DAD-MCNN: DDoS attack detection via multi-channel CNN. *PervasiveHealth: Pervasive Computing Technologies for Healthcare*, *Part F1481*, 484–488. https://doi.org/10.1145/3318299.3318329

de Assis, M. V. O., Carvalho, L. F., Rodrigues, J. J. P. C., Lloret, J., & Proença, M. L. (2020). Near real-time security system applied to SDN environments in IoT networks using convolutional neural network. *Computers and Electrical Engineering*, *86*, 106738. https://doi.org/10.1016/j.compeleceng.2020.106738

Deng, L., Way, O. M., Yu, D., & Way, O. M. (2014). Deep Learning : Methods and Applications. *Foundations and Trends in Signal Processing*, *7*(2013), 197–387. https://doi.org/10.1561/2000000039

Dinh, P. T., & Park, M. (2021). R-EDoS: Robust Economic Denial of Sustainability Detection in an SDN-Based Cloud through Stochastic Recurrent Neural Network. *IEEE Access*, *9*, 35057–35074. https://doi.org/10.1109/ACCESS.2021.3061601

Diro, A. A., & Chilamkurti, N. (2017). Distributed Attack Detection Scheme using Deep Learning Approach for Internet of Things. *Future Generation Computer Systems*, *82*, 761–768. https://doi.org/10.1016/j.future.2017.08.043

Elsayed, M. S., Le-Khac, N. A., Dev, S., & Jurcut, A. D. (2020). DDoSNet: A Deep-Learning Model for Detecting Network Attacks. *Proceedings - 21st IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks, WoWMoM 2020*,

391–396. https://doi.org/10.1109/WoWMoM49955.2020.00072

Gadze, J. D., Bamfo-Asante, A. A., Agyemang, J. O., Nunoo-Mensah, H., & Opare, K. A.-B. (2021). An Investigation into the Application of Deep Learning in the Detection and Mitigation of DDOS Attack on SDN Controllers. *Technologies*, *9*(1), 14. https://doi.org/10.3390/technologies9010014

Gautam, S. K., & Om, H. (2016). Computational neural network regression model for Host based Intrusion Detection System ☪. *Perspectives in Science*, *8*, 93–95. https://doi.org/10.1016/j.pisc.2016.04.005

Ghanbari, M., & Kinsner, W. (2018). Extracting Features form both the input and the output of a Convolutional Neural Networks to Detect Distributed Denial of Service Attacks. *2018 IEEE 17th International Conference on Cognitive Informatics & Cognitive Computing*.

Haider, S., Akhunzada, A., Mustafa, I., Patel, T. B., Fernandez, A., Choo, K. K. R., & Iqbal, J. (2020). A Deep CNN Ensemble Framework for Efficient DDoS Attack Detection in Software Defined Networks. *IEEE Access*, *8*, 53972–53983. https://doi.org/10.1109/ACCESS.2020.2976908

Hosseini, S., & Azizi, M. (2019). The hybrid technique for DDoS detection with supervised learning algorithms. *Computer Networks*, *158*, 35–45. https://doi.org/10.1016/j.comnet.2019.04.027

Hwang, R. H., Peng, M. C., & Huang, C. W. (2019). Detecting IoT malicious traffic based on autoencoder and convolutional neural network. *2019 IEEE Globecom Workshops, GC Wkshps 2019 - Proceedings*, 1–6. https://doi.org/10.1109/GCWkshps45667.2019.9024425

Jauro, F., Chiroma, H., Gital, A. Y., Almutairi, M., Abdulhamid, S. M., & Abawajy, J. H. (2020). Deep learning architectures in emerging cloud computing architectures: Recent development, challenges and next research trend. *Applied Soft Computing Journal*, *96*, 106–582. https://doi.org/10.1016/j.asoc.2020.106582

Ji, S., Jeong, B., Choi, S., & Hyun, D. (2016). Journal of Network and Computer Applications A multi-level intrusion detection method for abnormal network behaviors. *Journal of Network and Computer Applications*, *62*, 9–17. https://doi.org/10.1016/j.jnca.2015.12.004

Jia, W., Liu, Y., Liu, Y., & Wang, J. (2020). Detection Mechanism Against DDoS Attacks based on Convolutional Neural Network in SINET. *Proceedings of 2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference, ITNEC 2020*, *Itnec*, 1144–1148. https://doi.org/10.1109/ITNEC48623.2020.9084918

Kamilaris, A., & Prenafeta-Boldú, F. X. (2018). Deep learning in agriculture: A survey. *Computers and Electronics in Agriculture*, *147*(February), 70–90. https://doi.org/10.1016/j.compag.2018.02.016

Kasongo, S. M., & Sun, Y. (2020). A Deep Long Short-Term Memory based classifier for Wireless Intrusion Detection System. *ICT Express*, *6*(2), 98–103. https://doi.org/10.1016/j.icte.2019.08.004

Khan, M. A. (2021). HCRNNIDS: Hybrid convolutional recurrent neural network-based network intrusion detection system. *Processes*, *9*(5). https://doi.org/10.3390/pr9050834

Kim, D. E. (2018). *Comparison of Shallow and Deep Neural Networks for Network Intrusion Detection*. 204–208.

Kim, J., Kim, J., Kim, H., Shim, M., & Choi, E. (2020). CNN-based network intrusion detection against denial-of-service attacks. *Electronics (Switzerland)*, *9*(6), 1–21. https://doi.org/10.3390/electronics9060

916

Kim, M. (2019). Supervised learning-based DDoS attacks detection: Tuning hyperparameters. *ETRI Journal*, *41*(5), 560–573. https://doi.org/10.4218/etrij.2019-0156

Kumar, P. A. R., & Selvakumar, S. (2011). Distributed denial of service attack detection using an ensemble of neural classifier. *Computer Communications*, *34*(11), 1328–1341. https://doi.org/10.1016/j.comcom.2011.01.012

Lecun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. *N A T U R E*, *521*. https://doi.org/10.1038/nature14539

Lee, T. H., Chang, L. H., & Syu, C. W. (2020). Deep learning enabled intrusion detection and prevention system over SDN networks. *2020 IEEE International Conference on Communications Workshops, ICC Workshops 2020 - Proceedings*, 2–7. https://doi.org/10.1109/ICCWorkshops49005.2020.9145085

Li, C., Wang, J., & Ye, X. (2018). Using a recurrent neural network and restricted boltzmann machines for malicious traffic detection. *NeuroQuantology*, *16*(5), 823–831. https://doi.org/10.14704/nq.2018.16.5.1391

Li, Y., & Lu, Y. (2019). LSTM-BA: DDoS Detection approach combining LSTM and bayes. *Proceedings - 2019 7th International Conference on Advanced Cloud and Big Data, CBD 2019*, *61702267*, 180–185. https://doi.org/10.1109/CBD.2019.00041

Liang, X., & Znati, T. (2019). A long short-term memory enabled framework for DDoS detection. *2019 IEEE Global Communications Conference, GLOBECOM 2019 - Proceedings*, 1–6. https://doi.org/10.1109/GLOBECOM38437.2019.9013450

Liu, Z., Yin, X., & Hu, Y. (2020). CPSS LR-DDoS Detection and Defense in Edge Computing Utilizing DCNN Q-Learning. *IEEE Access*, *8*(3), 42120–42130. https://doi.org/10.1109/ACCESS.2020.2976706

Makuvaza, A., Jat, D. S., & Gamundani, A. M. (2021). Deep Neural Network (DNN) Solution for Real-time Detection of Distributed Denial of Service (DDoS) Attacks in Software Defined Networks (SDNs). *SN Computer Science*, *2*(2), 1–10. https://doi.org/10.1007/s42979-021-00467-1

Maranhao, J. P. A., Costa, J. P. C. L. D., De Freitas, E. P., Javidi, E., & De Sousa, R. T. (2021). Noise-Robust Multilayer Perceptron Architecture for Distributed Denial of Service Attack Detection. *IEEE Communications Letters*, *25*(2), 402–406. https://doi.org/10.1109/LCOMM.2020.3032170

Mcdermott, C. D., Majdani, F., & Petrovski, A. V. (2018). Botnet Detection in the Internet of Things using Deep Learning Approaches. *2018 International Joint Conference on Neural Networks (IJCNN)*, *August*. https://doi.org/10.1109/IJCNN.2018.8489489

Moghanian, S., Saravi, F. B., Javidi, G., & Sheybani, E. O. (2020). GOAMLP: Network Intrusion Detection with Multilayer Perceptron and Grasshopper Optimization Algorithm. *IEEE Access*, *8*, 215202–215213. https://doi.org/10.1109/ACCESS.2020.3040740

Nguyen, T. T., Shieh, C. S., Chen, C. H., & Miu, D. (2021). Detection of unknown DDoS attacks with deep learning and Gaussian mixture model. *Proceedings - 2021 4th International Conference on Information and Computer Technologies, ICICT 2021*, 27–32. https://doi.org/10.1109/ICICT52872.2021.00012

Orhan, U., Hekim, M., & Ozer, M. (2011). EEG signals classification using the K-means clustering and a multilayer perceptron neural network model. *Expert Systems with Applications*, *38*(10), 13475–13481.

https://doi.org/10.1016/j.eswa.2011.04.149

Paul, S. (2015). A Review on Advances in Deep Learning. *EEE Workshop on Computational Intelligence: Theories, Applications and Future Directions (WCI*, 6. https://doi.org/https://doi.org/10.1109/WCI.2015.7495514

Pereyra, G. (2016). C ´ Universit ´ e de Montr ´ eal University of Southern California CIFAR Fellow. *2016 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 3–7.

Priyadarshini, R., & Barik, R. K. (2019). A deep learning based intelligent framework to mitigate DDoS attack in fog environment. *Journal of King Saud University - Computer and Information Sciences*, *xxxx*. https://doi.org/10.1016/j.jksuci.2019.04.010

Ramesh, S., Yaashuwanth, C., Prathibanandhi, K., Basha, A. R., & Jayasankar, T. (2021). An optimized deep neural network based DoS attack detection in wireless video sensor network. *Journal of Ambient Intelligence and Humanized Computing*, *0123456789*. https://doi.org/10.1007/s12652-020-02763-9

Rehman, S. ur, Khaliq, M., Imtiaz, S. I., Rasool, A., Shafiq, M., Javed, A. R., Jalil, Z., & Bashir, A. K. (2021). DIDDOS: An approach for detection and identification of Distributed Denial of Service (DDoS) cyberattacks using Gated Recurrent Units (GRU). *Future Generation Computer Systems*, *118*, 453–466. https://doi.org/10.1016/j.future.2021.01.022

Roopak, M., Tian, G. Y., & Chambers, J. (2020). An Intrusion Detection System Against DDoS Attacks in IoT Networks. *2020 10th Annual Computing and Communication Workshop and Conference, CCWC 2020*, 562–567. https://doi.org/10.1109/CCWC47524.2020.9031206

Roopak, M., Yun Tian, G., & Chambers, J. (2019). Deep learning models for cyber security in IoT networks. *2019 IEEE 9th Annual Computing and Communication Workshop and Conference, CCWC 2019*, 452–457. https://doi.org/10.1109/CCWC.2019.8666588

Saied, A., Overill, R. E., & Radzik, T. (2015). Neurocomputing Detection of known and unknown DDoS attacks using Arti fi cial Neural Networks. *Neurocomputing*, 0925– 2312. https://doi.org/10.1016/j.neucom.2015.04.101

SaiSindhuTheja, R., & Shyam, G. K. (2021). An efficient metaheuristic algorithm-based feature selection and recurrent neural network for DoS attack detection in cloud computing environment. *Applied Soft Computing*, *100*, 106997. https://doi.org/10.1016/j.asoc.2020.106997

Salgado, C. M., Dam, R. S. F., Salgado, W. L., Werneck, R. R. A., Pereira, C. M. N. A., & Schirru, R. (2020). The comparison of different multilayer perceptron and General Regression Neural Networks for volume fraction prediction using MCNPX code. *Applied Radiation and Isotopes*, *162*(April), 109170. https://doi.org/10.1016/j.apradiso.2020.109170

Shaaban, A. R., Abd-Elwanis, E., & Hussein, M. (2019). DDoS attack detection and classification via Convolutional Neural Network (CNN). *Proceedings - 2019 IEEE 9th International Conference on Intelligent Computing and Information Systems, ICICIS 2019*, 233–238. https://doi.org/10.1109/ICICIS46948.2019.9014826

Shi, Z., Li, J., & Wu, C. (2019). DeepDDoS: Online DDoS attack detection. *2019 IEEE Global Communications Conference, GLOBECOM 2019 - Proceedings*, 1–6. https://doi.org/10.1109/GLOBECOM38437.2019.9013186

Shrestha, A. (2019). Review of Deep Learning Algorithms and Architectures. *IEEE*

Access, *7*, 53040–53065. https://doi.org/10.1109/ACCESS.2019.2912200

Singh, K. J., & De, T. (2017). Journal of Information Security and Applications MLP-GA based algorithm to detect application layer DDoS attack. *Journal of Information Security and Applications*, *36*, 145–153. https://doi.org/10.1016/j.jisa.2017.09.004

Singh, K. J., Thongam, K., & De, T. (2016). Entropy-based application layer DDoS attack detection using artificial neural networks. *Entropy*, *18*(10). https://doi.org/10.3390/e18100350

Singh, P., Jishnu Jaykumar, P., Pankaj, A., & Mitra, R. (2021). Edge-detect: Edge-centric network intrusion detection using deep neural network. *2021 IEEE 18th Annual Consumer Communications and Networking Conference, CCNC 2021*, 1–6. https://doi.org/10.1109/CCNC49032.2021.9369469

Sumathi, S., & Karthikeyan, N. (2020). Detection of distributed denial of service using deep learning neural network. *Journal of Ambient Intelligence and Humanized Computing*, 11. https://doi.org/10.1007/s12652-020-02144-2

Sun, W., Li, Y., & Guan, S. (2019). An Improved Method of DDoS Attack Detection for Controller of SDN. *2019 IEEE 2nd International Conference on Computer and Communication Engineering Technology, CCET 2019*, 249–253. https://doi.org/10.1109/CCET48361.2019.8989356

Tang, T. A., Mhamdi, L., McLernon, D., Zaidi, S. A. R., & Ghogho, M. (2018). Deep Recurrent Neural Network for Intrusion Detection in SDN-based Networks. *2018 4th IEEE Conference on Network Softwarization and Workshops, NetSoft 2018*, *NetSoft*, 462–469. https://doi.org/10.1109/NETSOFT.2018.8460090

Thilakaratne, M., Falkner, K., & Atapattu, T. (2019). A Systematic Review on Literature- based Discovery: General Overview, Methodology, & Statistical Analysis. *ACM Computing Surveys*, *52*(6).

Thilina, A., Attanayake, S., Samarakoon, S., Nawodya, D., Rupasinghe, L., & Pathirage, N. (2016). Intruder Detection Using Deep Learning and Association Rule Mining. *2016 IEEE International Conference on Computer and Information Technology Intruder*, 10–15. https://doi.org/10.1109/CIT.2016.6

Ugwu, C. C., Obe, O. O., Popoola, O. S., & Adetunmbi, A. O. (2021). A distributed denial of service attack detection system using long short term memory with Singular Value Decomposition. *Proceedings of the 2020 IEEE 2nd International Conference on Cyberspace, CYBER NIGERIA 2020*, 112–118. https://doi.org/10.1109/CYBERNIGERIA51635.2021.9428870

Velliangiri, S., Karthikeyan, P., & Kumar, V. V. (2020). Detection of distributed denial of service attack in cloud computing using the optimization-based deep networks. *Journal of Experimental & Theoretical Artificial Intelligence*, *00*(00), 1–20. https://doi.org/10.1080/0952813X.2020.1744196

Velliangiri, S., & Selvam, R. (2018). Investigation Distributed Denial of Service Attack Classification Using MLPNN-BP and MLPNN-LM. *Journal of Computational and Theoretical Nanoscience*, *15*(9/10), 2764–2768. https://doi.org/10.1166/jctn.2018.7536

Volkov, S. S., & Kurochkin, I. I. (2020). Network attacks classification using Long Short- Term memory based neural networks in Software-Defined Networks. *Procedia Computer Science*, *178*(2019), 394–403. https://doi.org/10.1016/j.procs.2020.11.041

Wang, M., Lu, Y., & Qin, J. (2020a). A dynamic MLP-based DDoS attack detection

method using feature selection and feedback. *Computers & Security*, *88*. https://doi.org/10.1016/j.cose.2019.101645

Wani, M. A., Bhat, F. A., Afzal, S., & Khan, A. I. (2019). Advances in Deep Learning. In *Studies in Big Data* (Vol. 57). Springer Nature Singapore Pte Ltd. https://doi.org/10.1007/978-981-13-6794-6

Wankhede, S., & Kshirsagar, D. (2018). DoS Attack Detection Using Machine Learning and Neural Network. *Proceedings - 2018 4th International Conference on Computing, Communication Control and Automation, ICCUBEA 2018*. https://doi.org/10.1109/ICCUBEA.2018.8697702

Xu, C., Shen, J., Du, X., & Zhang, F. (2018). An Intrusion Detection System Using a Deep Neural Network with Gated Recurrent Units. *IEEE Access*, *6*(c), 48697–48707. https://doi.org/10.1109/ACCESS.2018.2867564

Yin, C., Zhu, Y., Fei, J., & He, X. (2017). A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks. *IEEE Access*, *5*, 21954–21961. https://doi.org/10.1109/ACCESS.2017.2762418

Yu, L., Dong, J., Chen, L., Li, M., Xu, B., Li, Z., Qiao, L., Liu, L., Zhao, B., & Zhang, C. (2021). PBCNN: Packet Bytes-based Convolutional Neural Network for Network Intrusion Detection. *Computer Networks*, *194*(March), 108117. https://doi.org/10.1016/j.comnet.2021.108117

Zaidan, A. M. A. B. B., & Nan, A. A. Z. (2019). Review of intrusion detection systems based on deep learning techniques: coherent taxonomy, challenges , motivations , recommendations , substantial analysis and future directions. *Neural Computing and Applications*, *3*. https://doi.org/10.1007/s00521-019-04557-3