University of Sindh Journal of Information and Communication Technology
(USJICT)
Volume 6, Issue 4, December 2022

ISSN-E: 2523-1235, ISSN-P: 2521-5582
Website: http://sujo.usindh.edu.pk/index.php/USJICT/
© Published by University of Sindh, Jamshoro

A CONVOLUTIONAL NEURAL NETWORK-BASED MALWARE ANALYSIS, INTRUSION DETECTION, AND PREVENTION SCHEMA

Roheen Qamar[1], Baqar Ali Zardari[2], Aijaz Ahmed Arain[1], Asadullah Burdi[3],
Dr. Kelash Kanwar[4], Engr. Fayyaz Ahmed Memon[5]

[1]Department of Computer Science, Quaid-e-Awam University of Engineering,
Science and Technology, Nawabshah, Pakistan

[2]Department of Information Technology, Quaid-e-Awam University of Engineering,
Science and Technology, Nawabshah, Pakistan

[4]Department of Electronic Engineering, Quaid-e-Awam University of Engineering,
Science and Technology, Nawabshah, Pakistan

[5]Department of computer systems engineering Quaid-e-Awam University of Engineering,
Science and Technology, Nawabshah, Pakistan

roheen.qamar04@yahoo.com[1], alizardari34@gmail.com[2,] aijaz@quest.edu.pk[1], kelashkanwar@quest.edu.pk[4],
engr_fayaz@hotmail.com[5]

Abstract: This paper explores distributed denial of service (DDoS) attacks, their current threat level, and intrusion detection systems (IDS), which are one of key techniques for mitigating them. It focuses on the problems and issues that IDS systems encounter while detecting DDoS attacks, as well as the difficulties and obstacles that they face nowadays when integrating with artificial intelligence systems. These ID systems enable the automatic and real-time identification of harmful threats. However, the network requires a highly sophisticated security solution due to the frequency with which malicious threats emerge and change. A significant amount of research is required to create an intelligent and trustworthy identification system for research purposes; numerous ID datasets are freely accessible. Due to the rapid evolution of attack detection mechanisms and the complexity of malicious attacks, publicly available Identification databases must be completely changed. on a regular basis. Due to the ever-evolving attack detection mechanism and the complexity of malicious attacks, publicly available ID datasets must frequently be modified. A Convolutional Neural Network (CNN) network was trained using four distinct training algorithms. The CICDDoS2019 dataset, which contains the most recent DDoS attack types created in CICDDoS2019, was tested, According to the analysis; the "Gradient Descent with Momentum Backpropagation" algorithm could be trained quickly. Network data attacks were correctly detected 93.1 percent of the time. The results indicate that The Convolutional Neural Network is able to successfully defend against DDoS attacks detection by using intrusion detection systems IDS, as evidenced by the high accuracy values obtained.

Keywords: Distributed DDoS (Denial of Service) Attacks, Artificial Neural Network (ANN), Intrusion Detection System, Convolutional Neural Network,CICDDoS2019 dataset, Trainrp, Traingda, Traingdm,Traincgf.
,

I. INTRODUCTION

As assaults evolve, attackers exploit undiscovered weaknesses while avoiding established signatures. An intrusion detection system is a well-known network solution (IDS). IDSs are classified into two types. Attacks are identified using known signatures in misuse detection, whereas attacks are identified using normal use patterns in anomaly-based detection. Detecting anomalies has the advantage of being able to recognize the malicious activity, whereas misuse detection makes it difficult to identify unknown assaults. Unfortunately, due to the difficulty of defining a wide range of normal use patterns, anomaly detection has a high risk of false alarms. By using a deep neural network to learn its own characteristics, Deep Learning (DL) overcomes these flaws. IDS' shortcomings can be compensated for by incorporating DL. To look at it another way, Machine Learning reduces false alarms (ML) and Deep Learning (DL) learn normal use and intrusion patterns. In this paper's IDS study, we use DL to find Denial-of-Service (DoS) attacks [1, 2] .Attacks is classified according to the CICDDoS2019 data set classification system DoS, R2L (remote to local), U2R (user to root), and probing are the four primary kinds. CICD DoS was created by injecting these types. Because IDS research frequently makes use of machine learning, many IDS studies have made use of the CICDDoS2019 data set. The majority of these studies classify the entire CICDDoS2019 data set as attack or benign using binary classification. They also divide the data set into four categories using multiclass classification. We focus on individual assaults put into CICDDoS2019 in this study. Rather of segregating assaults from benign samples or categorizing them, we employ DL to detect the smallest variations between attacks. Using only two of the four datasets, a DoS detection algorithm based on deep learning was created. Convolutional Neural Network (CNN)-based models are utilized for both binary and multiclass classification in our model [3, 4].

A) INTRUSION DETECTION

A network device is an intrusion detection system (IDS). that analyzes packets and detects threats. Threat detection, response, and network behavior preservation are among the IDS's goals.[5] The primary function of An IDS is intended to be the first line of defense in locating cyberattacks carried out over the internet. Modern Machine Learning (ML) algorithms have begun to be used by researchers to efficiently identify invaders and, as a result, safeguard the information of internet users and their faith in the general security of the internet network as a whole as infiltration strategies become increasingly complex and difficult to detect. IDS stands for An intrusion detection system is a sort of safety management. regarded as an essential component of network security systems because it can identify network intrusions. Most of the time, an intrusion detection system (IDS) looks at every packet that comes into and leaves a network to see if there is evidence of an intrusion. A well-thought-out system for detecting intrusions can catch the majority of incursion actions. a well-designed intrusion detection system that can identify the majority of intrusions and apply typical machine learning to them, either by writing to security issuing warnings [6].

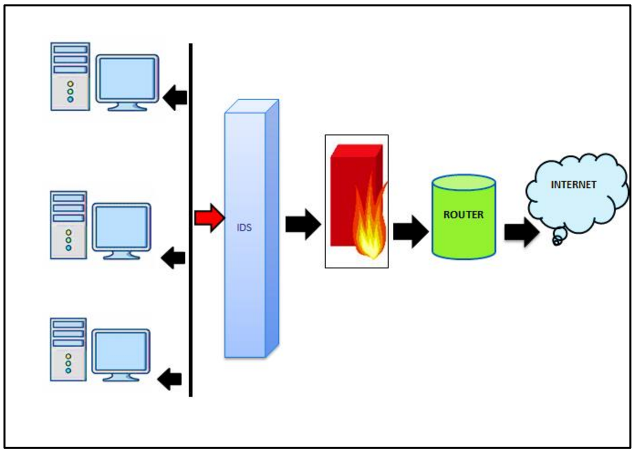


Fig 1 Instruction Detection System

B) DDOS (DISTRIBUTED DENIAL OF SERVICE)

A distributed denial of service (DDoS) assault is one carried out by a large number of internet network nodes. node agents and is a deliberate, massive attack on a victim system or program's ability to provide services. Before starting an attack, an attacker uses the internet to take control of a lot of vulnerable computer devices. The flaws in these computers are taken advantage of by the attacker through the use of malicious software or another method of cyberattack. These "zombies," also known as devices that are corrupted or vulnerable, can number in the thousands or millions. A 'spyware' is typically constructed by a swarm of zombies. The size of the botnet determines the severity of the attack; larger botnets result in a more violent attack. Well as disastrous [7], as shown in Figure 2.

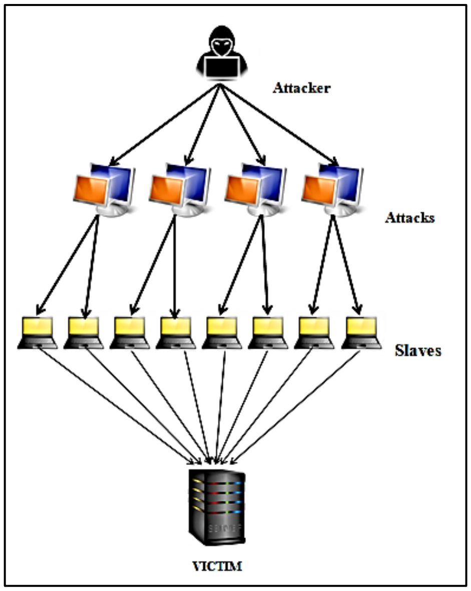


Fig 2 Distributed Denial of Service Attack

The zombies or botnet computers of a network, which are well-organized, remote-managed, and widely dispersed and send a lot of Requests for traffic or services to the target system continuously or synchronously, typically start cyberattacks.. The targeting scheme reacts slowly, becomes unusable, or crashes completely as a result of the attack. Zombies in a botnet are frequently recruited via Trojan horses, viruses, or backdoors. Because zombies controlled by the attacker via botnet use forged IP addresses, defense mechanisms have a difficult time identifying the original attacker [8].

C) NEURAL NETWORKS

The neural network is a well-known popular type of machine learning used in graphical user interfaces .The power of neural networks comes from computing units that are connected and massively parallelized and organized into distinct layers. The biological systems of the brain had an impact on the fundamental idea and motivation behind neural networks. After receiving weighted input signals from nodes, the neuron's output is sent to vertices in the subsequent layer via an activation function. Deep neural networks (ANN) are convolutional neural networks with multiple layers for advanced learning. It has been regarded as one of the most effective tools in recent decades and has been widely acknowledged in the literature for its capacity to handle massive amounts of data. Convolutional neural networks, in particular, have begun to outperform conventional methods in a number of fields [9, 10].

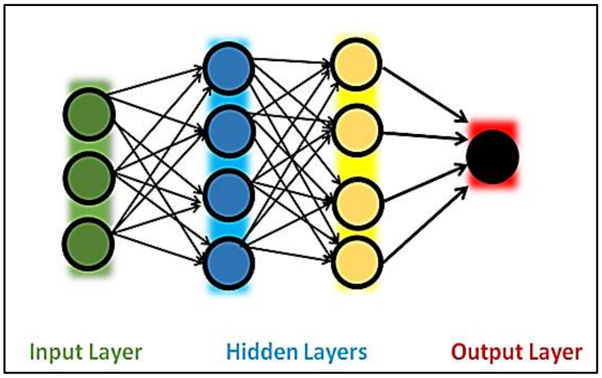


Fig 3 Artificial Neural Network Has Two Learning Procedures.

1. Supervised Learning Process

The A neural network is given a properly labeled training set and is asked to learn a mapping from inputs x to outputs y from a labeled collection of the set contains. during deep classification. The proposed method is used to train an artificial neural network (ANN), which employs supervised learning Procedures. An offline analysis method was used to detect malware with the MLP.MLP's effectiveness was compared to that of Personality Maps in a novel method for detecting network data intrusion.

2. Unsupervised Neural

The neural network is fed N xix 1 == a set of unlabeled data during this learning procedure, and you are required to find trends in the data. The proposed system, an artificial neural network (ANN), is trained using an unsupervised learning approach. That produces a Map, which is a moderate, discretized demonstration of the test set feature space [11].

D) CONVOLUTIONAL NEURAL NETWORK

A well-known The Convolutional Neural Network is the deep neural network (CNN).It gets its name from the linear mathematical procedure matrix convolution. The layer that is completely interconnected, the non-linearity layer, the pooling layer, and the convolutional layer are just a few of the many layers in a CNN. Illustration Net, the biggest picture categorization data collection, computer vision, and natural language processing (NLP) were among the memory buffer's applications and outcomes were outstanding.

A convolutional neural network with tens or hundreds of layers can learn to recognize various image features. Each convolved picture's output is used as the succeeding layer's input, and each training is processed with filters of varying resolutions. The filters can change, changing from relatively straightforward criteria like brightness and edges to properties that only describe the component [12, 13].Tens or hundreds of layers teach a To distinguish multiple visual properties, a convolutional neural network is used. The filters are applied to each training image at various resolutions, and the result of each convolved image is used as the input for the following layer. From very basic parameters like brightness and borders, the filters can go all the way up to attributes that are unique to the object [14, 15].as shown in fig 4 how CNN work.

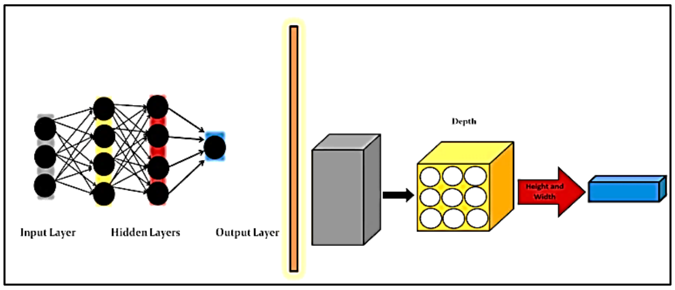


Fig 4 Convolutional Neural Network Work

II. RELATED WORK

The researchers, Engelen, Giants, and colleagues [16], uncover a variety of problems with feature extraction, labelling, traffic generation, flow construction, and traffic generation that have a negative impact on the attributes described above. We implement a more effective data processing strategy to address the majority of these flaws after investigating their underlying causes. Over a quarter of the original traffic traces have been rebuilt or relabeled as a result. Benchmarks for machine learning demonstrate significant improvements on the final dataset. Our findings demonstrate how issues with data collection can significantly affect model evaluation and offer suggestions for anticipating and avoiding them.

Various ANN models for detecting malicious activity were presented by Unsteady et al. [17]. They reduced features in the CICIDS2017 dataset using Deep Neural Networks, Shallow Neural Networks, and Auto Encoder. The precision of these models was compared. Their study found several inaccuracies, with a 98.45% accuracy rate.

Folino and co. For analyzing non-stationary data like intrusion detection system logs, a novel ensemble-based deep learning framework was created by [18]. When employing string section learners, the capacity to construct a superior detection structure is essential in order to achieve a higher detection rate, when putting together an ensemble, one of the most difficult problems is choosing from the available base classifiers and combiners.

An in-depth evaluation of Intrusion detection systems can benefit from ensemble learning by Tama and colleagues [19] The majority of traditional machine learning algorithms, on the other hand, lack formal training and place less emphasis on feature selection and engineering; They are unable to handle the enormous challenge of attack data classification in the context of a real-world network application. Multi-classification attack detection jobs are becoming more common as dataset quantities grow will become less reliable. As a result, accurate forecasting and evaluation of high learning demand with massive data volumes are incompatible with machine learning.

Kazi, Taher, and others claim that [20] when it comes to identifying network traffic; Support vector machine (SVM) is inferior to ANN-based deep learning with wrapper feature selection. The NSL-KDD dataset is used to evaluate performance by categorizing network traffic with SVM and ANN-supervised machine learning algorithms. The comparative analysis demonstrates that the suggested model has the categorizing highest accuracy rate for intrusion detection performs better than other models that are currently in use.

Oliveira et al [21] used LSTM deep learning to create an intelligent ID and classification framework. On the CIDDS-001 dataset, this framework was tested and found to be more accurate than conventional machine learning methods at identifying objects. Another well-known DL method that learns straight from the dataset, with no human feature extraction required is the convolutional neural network (CNN).Convolutional and fully linked pooling input and output layers are typical in a CNN. CNNs are frequently utilized in image identification; however, they can also be used for defense.

According to Erhan et al. [22], DDOS assaults are among the most annoying sorts of damaging online activity attacks. DDoS attacks come in two varieties: attacks on resource depletion and bandwidth depletion. The authors monitored traffic from the mirror port of the backbone router of the Bogaziçi University network and carried out DDoS attacks of the resource-depletion variety. his data set is useful for evaluating DDoS detection algorithms based on the network because it takes into account both attack and non-attack traffic. The assaults target an only one victim server connected to the campus' backbone network.

Bikram Khadka et al [23] investigate DDoS attacks and provide a DDoS detection Intrusion Detection System (IDS) based on Snort. This section describes a technique for informing network administrators about potential resource attacks and their nature. Furthermore, it temporarily disables the attacker, giving the network administrator time to devise a backup strategy. The idea was methodology mitigates the impact of DDoS assaults by identifying them early and attempting to change several factors that make the problem more visible.

Zubair Hasan and Sattar et al. [24] propose a Deep Convolution Neural Network (DCNN) model for detecting DDoS attacks on optical switching networks. DCNN was used because shallow machine learning techniques could not assess traffic in the manner intended for the smaller dataset sample. In the experiment, DCNN outperforms shallow machine learning algorithms including K-Nearest Neighbor (KNN), Support Vector Machine (SVM), and Nave Bayes, with values of 93%, 88%, and 79%, respectively.

Tang et al. [25] discovered anomalies in the stream with superior deep learning abilities. Despite this, adversarial deep learning's potential threats to the IDS system have received little attention. The use of deep learning models in large automated reviews as well as control systems that are crucial to safety and security, such as voice-controlled controllers and intrusion detection systems is restricted by the recently discovered vulnerability.

Abro, A. A., Khan et al. [26] the basic objective of this study is to give categorization and comparative analysis of data mining methods. Six supervised machine learning (ML) algorithms, C4.5 (J48), K-Nearest Neighbor (KNN), Logistic Regression (LR), Naive Bayes (NB), Support Vector Machine (SVM), and One Rule (OneR), as well as five UCI Datasets from the ML Repository, are used to demonstrate the robustness and effectiveness of various approaches. For analytical techniques, the following key factors have been considered: accuracy, Area under Curve (AUC), precision, recall, and F-measure values. As a result, the fundamental goal of this research is to acquire binary As a result; the fundamental goal of this work is to get binary classification and efficiency through performance assessment. We show experimental findings that indicate the efficacy of our strategy in comparison to well-known competing techniques.

III. EXPERIMENTATION

The training's objective is to train the system how to learn and characterize input traffic. The suggested system was trained with three distinct strategies using a recurrent neural network. For training reasons, the MATLAB 2022a simulator was employed. During the design process, clean the CICDDoS2019 dataset and provide protocol, attack, and flag values. After that, the neural network model was built and utilized to train the CICDDoS2019 dataset with ANN [27, 28]. Following training, the outcomes of DDoS attack detection were examined using the ANN toolbox in MATLAB 2022a.We assess our proposed classifier in this research using the newly available CICDDoS2019 dataset. The dataset comprises a wide number of various DDoS assaults that may be carried out utilizing TCP/UDP application layer protocols [29].

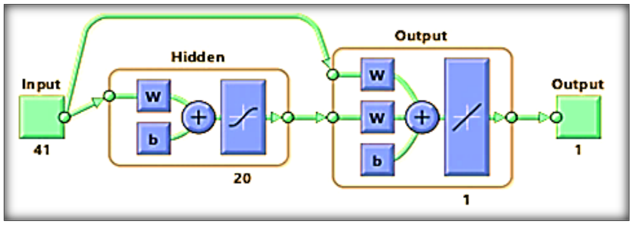


Fig 5 Neural Network of Artificial Intelligence

In this research, four algorithms have been used

1) Conjugate Gradient Backpropagation with Fletcher-Reeves Update.
2) Gradient Descent with Momentum Backpropagation.
3) Resilient Backpropagation.
4) Gradient Descent With Adaptive Learning Rate Backpropagation

IV. TRAINING ALGORITHMS

A. CONJUGATE GRADIENT BACKPROPAGATION WITH THE FLETCHER-REEVES UPDATE

All conjugate gradient algorithms look in the direction of the conjugate gradient, or the gradient's inverse, during the first iteration.

After p0=g0, a line search is done to find the shortest path in the primary search direction: Using the formula, the next search position is then determined to be adjacent to the previous ones. xk+1=xkkpk. Typically, the new gradient direction and the entire search position are combined to determine the new search direction [29].

$$pk=-gk+\beta kpk-1$$

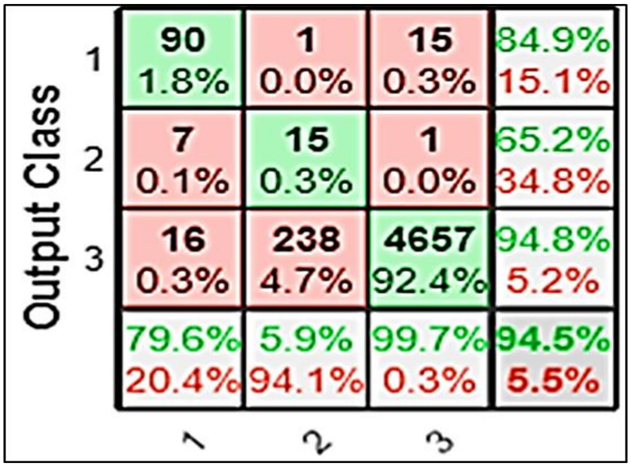
$$k=gTkgkgTk1gk1.$$

The training algorithm is used to compute performance derivatives for bias and weight variables X. The criteria that are used to adjust each variable are as follows:

$$X = X + a*dX,$$

Where dX is the search direction. dX = -gX + dX old*Z, where gX is a gradient. There are various ways to compute the parameter Z. It is calculated for the Fletcher-Reeves gradient descent variant.
Z = current norm squared/new norm squared Training is terminated if any of the following circumstances occur [29].

The convolutional neural network's classification value, which is 94.5 percent, includes a 5.5% miss classification, as shown in Figure 6.



Output Class				
1	90 1.8%	1 0.0%	15 0.3%	84.9% 15.1%
2	7 0.1%	15 0.3%	1 0.0%	65.2% 34.8%
3	16 0.3%	238 4.7%	4657 92.4%	94.8% 5.2%
	79.6% 20.4%	5.9% 94.1%	99.7% 0.3%	94.5% 5.5%
	1	2	3	

Fig 6 Using the Fletcher-Reeves Update, Conjugate Gradient Backpropagation

Figure 7 depicts the finalized neural network training. The epoch value is 29, the overall time is 12 minutes and 20 seconds, and the performance is 9.6886e-07.

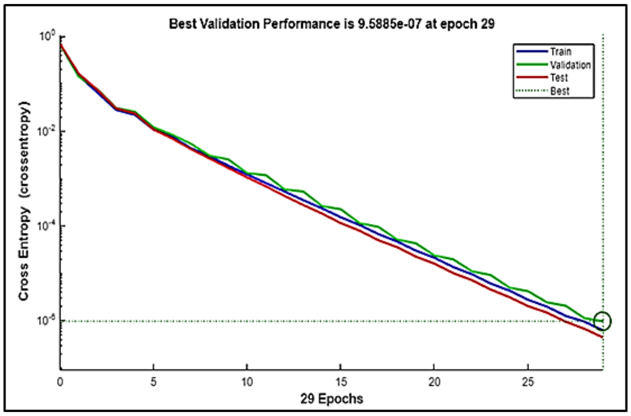


Figure 7: Fletcher-Reeves Update Validation of Conjugate Gradient Backpropagation

As shown in fig 8 Plots are then used to further analyze the results. Select Regression in the Plots section to plot the linear regression. For the training, validation, and test sets, the regression plot displays the network predictions (output) in relation to the responses (target) gradient value is 3,0051 and epoch is 11.

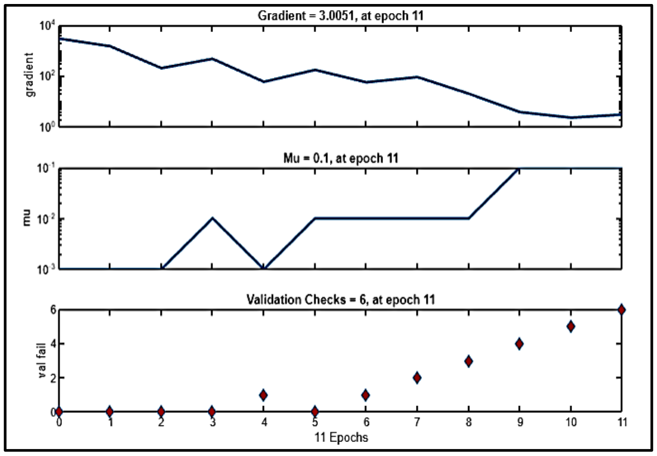


Fig 8 Plot Gradient Training Conjugate Gradient Backpropagation with Fletcher-Reeves Update

Plotting the results allows for further analysis in fig 9. R=0.8906 in the final regression plot.

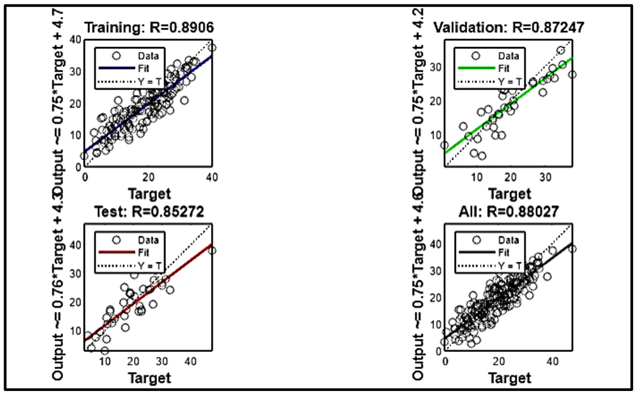


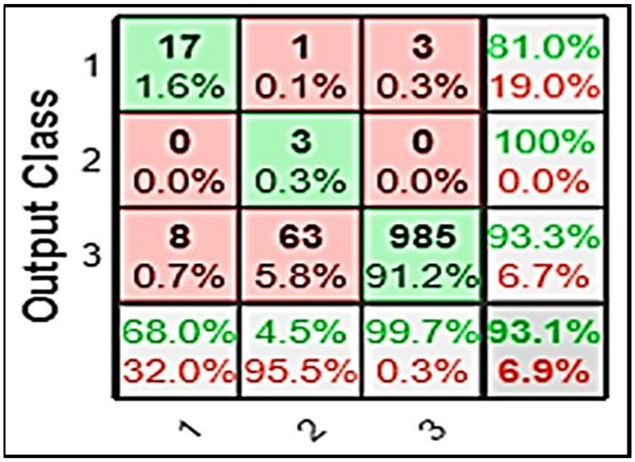
Fig 9 Plot Response Conjugate Gradient Backpropagation

B. *GRADIENT DESCENT WITH MOMENTUM BACKPROPAGATION*

Tin GDM can teach any structure using weight, net input, and transfer function derivative functions.
To compute performance derivatives for the bias and weight variables X, backpropagation is performed. Each variable is changed using gradient descent and momentum [29,30]. DX is the sum of mc*dXprev and lr*(1-mc)*dperf/dX, where dXprev represents the prior bias or weight change and dperf/dX represents the current bias or weight change. the current bias or weight change. Training is stopped if any of the following conditions are met: Figure 8 depicts the classification value for a straightforward neural network.is 93.1 percent, with a

6.9% miss classification. The epoch (repetition) limit has been reached. The time limit has expired. In order to achieve the goal, performance is reduced. The performance gradient is less than the minimum gradient [31, 32].

Figure 10 depicts the classifier value of the convolutional neural network, that is 93.1% with a miss classification rate of 6.9%.



Output Class

1	17 1.6%	1 0.1%	3 0.3%	81.0% 19.0%
2	0 0.0%	3 0.3%	0 0.0%	100% 0.0%
3	8 0.7%	63 5.8%	985 91.2%	93.3% 6.7%
	68.0% 32.0%	4.5% 95.5%	99.7% 0.3%	93.1% 6.9%
	1	2	3	

Fig 10 Confusion Matrix of Gradient Descent with Momentum Backpropagation

Figure 11 depicts the completed neural network training. The epoch value is 12, the total duration is 11 minutes and 12 seconds, and the performance is 0.031109.

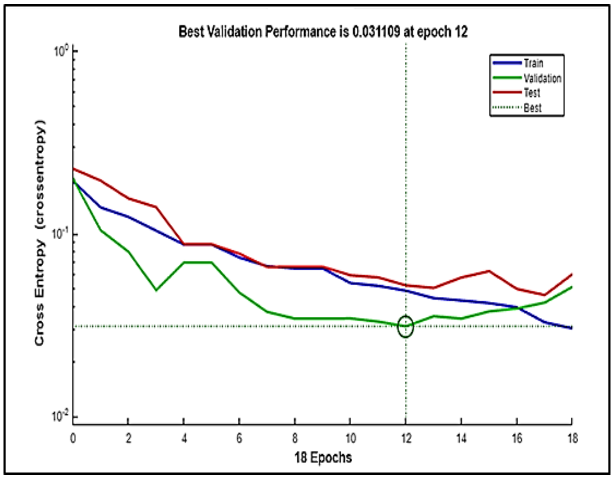


Fig 11 Validation Performance of Gradient Descent with Momentum Backpropagation

Plotting the results allows for further analysis in fig 12. R=0.88 in the final regression plot displayed at the conclusion of training indicates extremely good accuracy. However, I am unsure which scatter plot it represents.

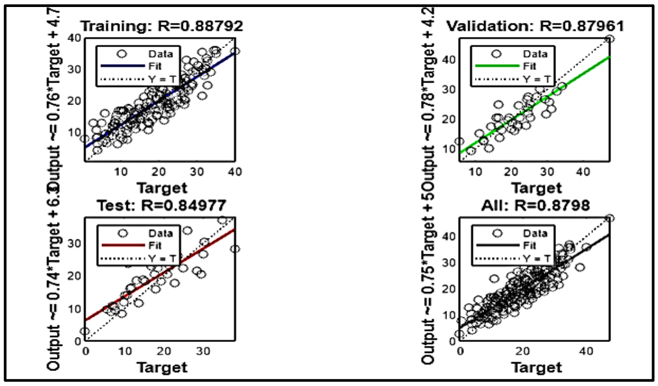


Fig 12 Gradient Descent with Momentum Backpropagation

The gradient value is 6.6284 and epoch is 17 as shown in fig 13.

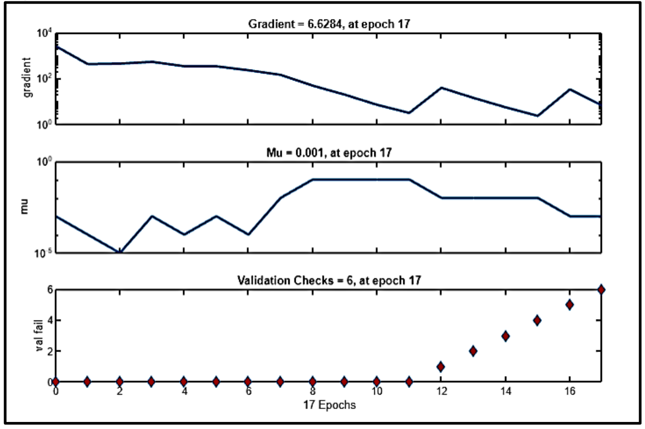


Fig 13 Visualize Impact Gradient Descent with Momentum Backpropagation

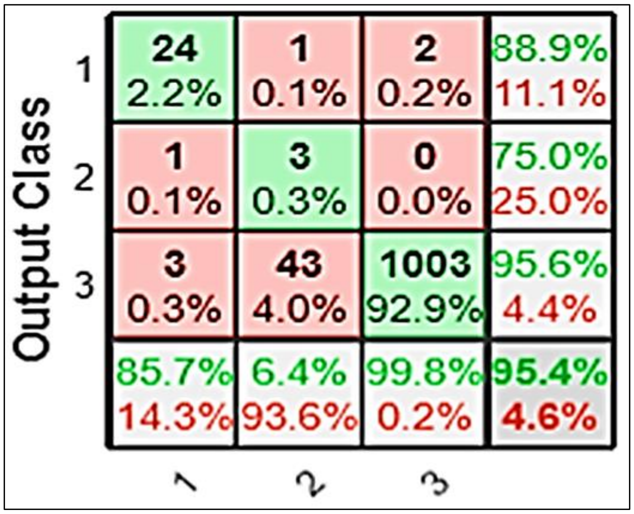
V. RESILIENT BACKPROPAGATION

Trainrp is a train neural network function that updates the bias and weight values using the resilient backpropagation method. (Rprop).The training-required starting values of the Trainrp training parameters, are listed below. Train epochs—the total number of epochs required for training The initial state is 1000.Performance performance derivatives are calculated using backpropagation in relation to the bias and weight variables X. The main parameters are used to adjust each variable.

deltaX.*sign (gX) = dX; where the gradient is gX and all deltaX elements are set to delta0. At each iteration, deltaX is changed to reflect changes in gX elements. Changes its sign between iterations, delta dec reduces the element that corresponds to deltaX.See "The RPROP Algorithm:" If an element of gX keeps the same sign from iteration to iteration, delta increases the element of deltaX that corresponds to it.M. Riedmiller and H. Braun wrote "A Direct Adaptive Method for Faster Backpropagation Learning" [33].If any of the following conditions are met, training is stopped: The number of epochs (repeats) has passed. The timeframe has expired.

1. In order to achieve the goal, performance is reduced.
2. The performance gradient is less than the minimum gradient [34, 35].

Figure 14 depicts the classification value of the convolutional neural network, which is 95.4% with a 4.6% miss classification.



Output Class	1	2	3	
1	24 2.2%	1 0.1%	2 0.2%	88.9% 11.1%
2	1 0.1%	3 0.3%	0 0.0%	75.0% 25.0%
3	3 0.3%	43 4.0%	1003 92.9%	95.6% 4.4%
	85.7% 14.3%	6.4% 93.6%	99.8% 0.2%	95.4% 4.6%

Fig 14 Confusion Matrix of Resilient Backpropagation

Figure 15 depicts the entire neural network training process. The performance is 0.058878, the epoch value is 66 iterations, and the total time is 18 minutes and 20 seconds.

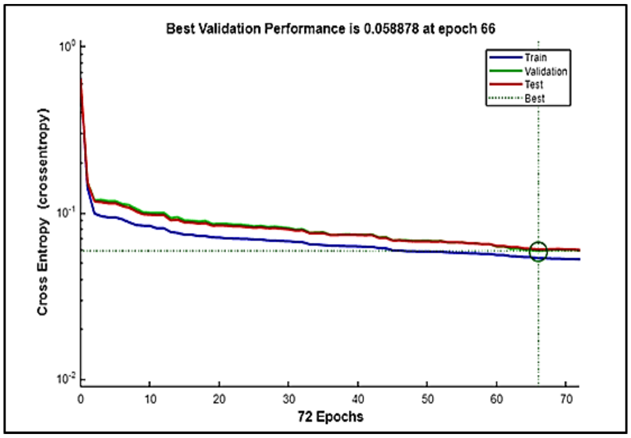


Fig 15: Validation Performance of Resilient Backpropagation

The final regression plot displayed at the end of training demonstrates very good accuracy, R0.90306

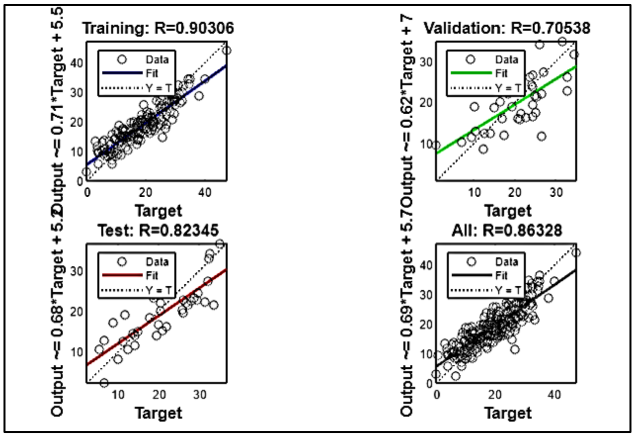


Fig 16 Linear Regression of Validation Performance of Resilient Backpropagation

The gradient value is 5.0907 and epoch is 17 as shown in Fig. 17 plots the errors between a goal time series and an output time series on the same axis.

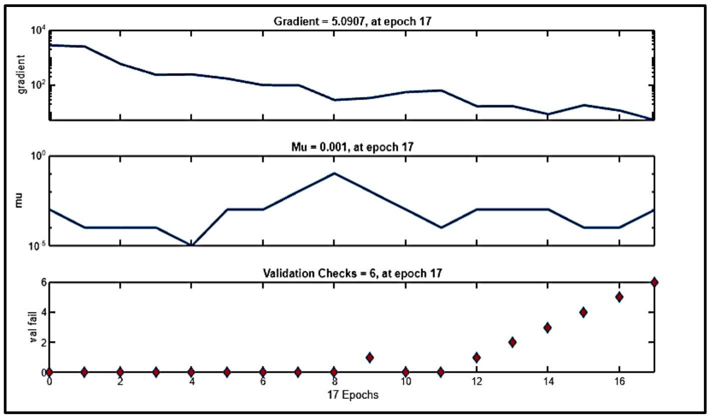


Fig 17 Graphical Response Validation Performance of Resilient Backpropagation

VI. *GRADIENT DESCENT WITH ADAPTIVE LEARNING RATE BACKPROPAGATION*

The algorithm's accuracy is mostly determined by how well the learning rate is controlled. The algorithm will vary and become unstable if the learning rate is set too high. The technique takes too long to converge if the learning rate is too low. It is hard to determine the optimal learning rate before to training since it changes as the algorithm proceeds through the performance surface. [36] Backpropagation is used to compute the performance dperf derivatives for the bias and weight variables. Each variable is changed using gradient descent: lr*dperf/dX = dX Training will be reduced. if one of the following two constraints is met: The limit on repetition, or epoch, has been reached.

1. The time limit has expired.
2. In order to reach the objective, efficiency is decreased.
3. The performance gradient is lower than the minimum performance gradient.
4. When using validation, validation performance (validation error) has increased more than the maximum fail times [37, 38].

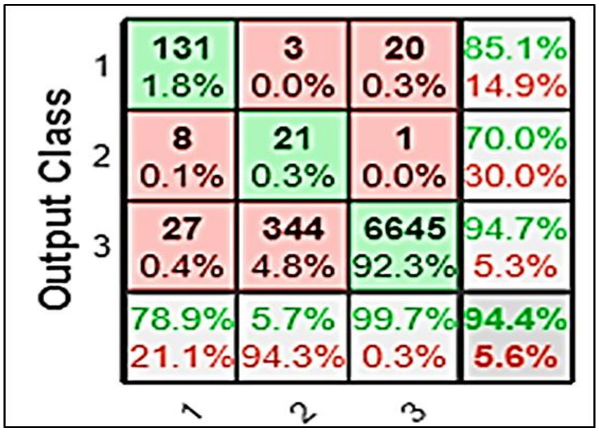


Fig 18 Confusion Matrix of Gradient Descent with Adaptive Learning Rate Backpropagation

Figure 19 depicts the completed training of a neural network. The epoch value is 24, the total duration is 15 minutes and 7 seconds, and the performance is 0.0061961.

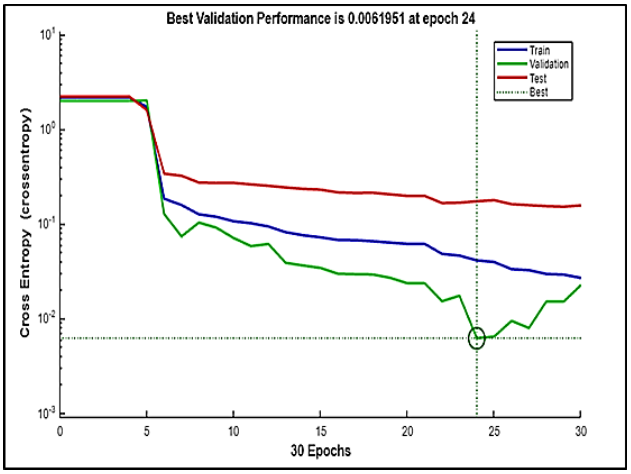


Fig 19 Gradient Descent Validation Accuracy with Adjustable Learning Rate Backpropagation

Methods like linear regression are used to create a linear model. The relationship between a dependent variable y, which is also referred to as the response, and one or more independent variables Xi, which are referred to as the predictors, is expressed in the model. A general equation for a linear regression model can be found here. At the conclusion of training, the final regression plot shows a very high level of accuracy, R0.889.However, due to the existence of multiple outputs,

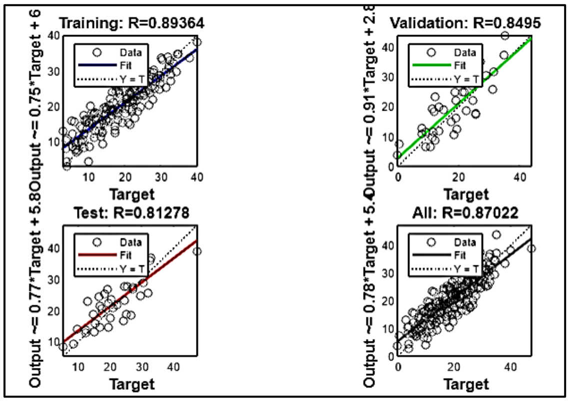


Fig 20 Linear Regression of Gradient Descent with Adaptive Learning Rate Backpropagation

The gradient value is 1.5513 and epoch is 25 as shown in fig 21.

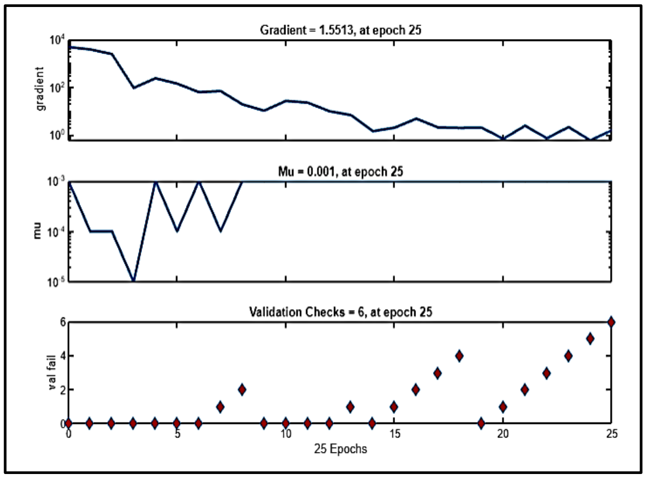


Fig 21 Sequences of events Backpropagation of Reaction Adaptive Learning Rate

The CNN training of three distinct algorithms is depicted in Table 2.The outcome demonstrates that the Gradient Descent with Momentum Backpropagation algorithm outperforms two other selected algorithms in terms of performance. The training was completed in less time, 11 minutes and 12 seconds, with a success rate (accuracy) of 93.1 percent.

TABLE 1 FINAL RESULT OF ALGORITHMS

S#	Algorithm	Success Rate	Misclassification	Timing
1.	**Conjugate Gradient Backpropagation With Fletcher-Reeves Update.**	**94.5**	**5.5**	**12 min 20 sec**
2.	**Gradient Descent With Momentum Backpropagation.**	**93.1**	**6.9**	**11 min 12 sec**
3.	**Resilient Backpropagation.**	**95.4**	**4.6**	**18 min 20 sec**
4.	**Gradient Descent With Adaptive Learning Rate Backpropagation**	**94.4**	**5.6**	**15 min 7 sec**

VII. CONCLUSIONS

Internet security is now essential for all users. Attacks known as distributed denial of service (DDoS) have a number of significant security implications for internet users. DDoS attacks prevent users from accessing services. The recurrent neural network was used for DDoS attack detection and training in this study. Four well-known algorithms were chosen by us: 1) Conjugate Gradient Backpropagation with Fletcher-Reeves Update, 2) Gradient Descent with Momentum Backpropagation, 3) and Gradient Descent with Adaptive Learning Rate Backpropagation. The article's goal was to find the optimum algorithm in terms of accuracy and training duration. The CNN neural network was used to detect DDoS attacks. The analysis showed that the "Gradient Descent With Momentum Backpropagation " algorithm in a short amount of time spent training, with a good precision performance of 93.1 percent accuracy and a training time of 11 minutes and 12 seconds. In the future, a number of approaches, models, and neural networks related to machine learning and deep learning may be utilized, and different algorithms can be used to detect which network and algorithm is best for detection of DDoS attacks

REFERENCES

[1] Yaser, Ahmed Latif, Hamdy M. Mousa, and Mahmoud Hussein. "Improved DDoS Detection Utilizing Deep Neural Networks and Feedforward Neural Networks as Autoencoder." Future Internet 14, no. 8 (2022): 240.

[2] Asharf, J.; Moustafa, N.; Khurshid, H.; Debie, E.; Haider, W.; Wahab, A. A Review of Intrusion Detection Systems Using Machine and Deep Learning in Internet of Things: Challenges, Solutions and Future Directions. Electronics 2020, 9, 1177.

[3] Wang, Jiushuang, Ying Liu, and Huifen Feng. "IFACNN: efficient DDoS attack detection based on improved firefly algorithm to optimize convolutional neural networks." Mathematical Biosciences and Engineering 19, no. 2 (2022): 1280-1303.

[5] Fouladi, Ramin Fadaei, Orhan Ermiş, and Emin Anarim. "A Novel Approach for distributed denial of service defense using continuous wavelet transform and convolutional neural network for software-Defined network." Computers & Security 112 (2022): 102524.

[6] Kanna, P. Rajesh, and P. Santhi. "Hybrid Intrusion Detection using MapReduce based Black Widow Optimized Convolutional Long Short-Term Memory Neural Networks." Expert Systems with Applications 194 (2022): 116545.

[7] Alharbi, Yasser, Ali Alferaidi, Kusum Yadav, Gaurav Dhiman, and Sandeep Kautish. "Denial-of-Service Attack Detection over IPv6 Network Based on KNN Algorithm." *Wireless Communications and Mobile Computing* 2021 (2021).

[8] S ur Rehman, Saif, Mubashir Khaliq, Syed Ibrahim Imtiaz, Aamir Rasool, Muhammad Shafiq, Abdul Rehman Javed, Zunera Jalil, and Ali Kashif Bashir. "DIDDOS: An approach for detection and identification of Distributed Denial of Service (DDoS) cyberattacks using Gated Recurrent Units (GRU)." Future Generation Computer Systems 118 (2021): 453-466.

[9] Altikat, A. A. A. G. S., A. Gulbe, and S. Altikat. "Intelligent solid waste classification using deep convolutional neural networks." International Journal of Environmental Science and Technology 19, no. 3 (2022): 1285-1292.

[11] Jmj, A. 5 Industries That Heavily Rely on Artificial Intelligence and Machine Learning. Available online: https://medium.com/datadriveninvestor/5-industries-that-heavily-rely-on-artificial-intelligence-and-machine-learning-53610b6c1525 (accessed on 10 November 2020).

[12] Lent, Daniel M. Brandão, Matheus P. Novaes, Luiz F. Carvalho, Jaime Lloret, Joel JPC Rodrigues, and Mario Lemes Proença. "A Gated Recurrent Unit Deep Learning Model to Detect and Mitigate Distributed Denial of Service and Portscan Attacks." IEEE Access 10 (2022): 73229-73242.

[13] Malliga, Subramaniam, P. S. Nandhini, and Shanmuga Vadivel Kogilavani. "A Comprehensive Review of Deep Learning Techniques for the Detection of (Distributed) Denial of Service Attacks." Information Technology and Control 51, no. 1 (2022): 180-215.

[14] Ghimire, Deepak, Dayoung Kil, and Seong-heum Kim. "A Survey on Efficient Convolutional Neural Networks and Hardware Acceleration." Electronics 11, no. 6 (2022): 945.

[15] Tulbure, Andrei-Alexandru, Adrian-Alexandru Tulbure, and Eva-Henrietta Dulf. "A review on modern defect detection models using DCNNs–Deep convolutional neural networks." Journal of Advanced Research 35 (2022): 33-48.

[16] Engelen, Gints, Vera Rimmer, and Wouter Joosen. "Troubleshooting an intrusion detection dataset: the CICIDS2017 case study." In *2021 IEEE Security and Privacy Workshops (SPW)*, pp. 7-12. IEEE, 2021.

[17] S. Ustebay, et al., "Cyber Attack Detection by Using Neural Network Approaches: Shallow Neural Network, Deep Neural Network and Auto Encoder," in International Conference on Computer Networks, pp. 144-155, 2019.

[18] Folino, F.; Folino, G.; Guarascio, M.; Pisani, F.; Pontieri, L. On learning effective ensembles of deep neural networks for intrusion detection. Inf. Fusion 2021, 72, 48–69.

[19] Tama, B.A.; Lim, S. Ensemble learning for intrusion detection systems: A systematic mapping study and cross-benchmark evaluation. Computer. Sci. Rev. 2021, 39, 100357.

[20] Taher, Kazi Abu, Billal Mohammed Yasin Jisan, and Md Mahbubur Rahman. "Network intrusion detection using supervised machine learning technique with feature selection." In 2019 International conference on robotics, electrical and signal processing techniques (ICREST), pp. 643-646. IEEE, 2019.

[21] Oliveira, N.; Praça, I.; Maia, E.; Sousa, O. Intelligent Cyber Attack Detection and Classification for Network-Based Intrusion Detection Systems. Appl. Sci. 2021, 11, 1674.

[22] Erhan, D.; Anarım, E. Bogˇaziçi University distributed denial of service dataset. Data Brief 2020, 32, 106187

[23] Bikram Khadka, Chandana Withana, Abeer Alsadoon, Amr Elchouemi, 2015. Distributed Denial of Service attack on Cloud Detection and Prevention. School of Computing and Mathematics, Charles Sturt University, Sydney, Australia Hewlett Packard. 2015 International Conference (pp. 1-5). IEEE.

[24] Zahid Hasan, Md., Zubair Hasan, K. M., & Sattar, Abdus (2018). Burst header packet flood detection in optical burst switching network using deep learning model. Procedia Computer Science, 143, 970–977.

[25] T. A. Tang, L. Mhamdi, D. McLernon, S. A. R. Zaidi, and M. Ghogho, "Deep learning approach for network intrusion detection in software defined networking," in 2016 international conference on wireless networks and mobile communications (WINCOM), 2016, pp. 258–263.

[26] Abro, A. A., Khan, A. A., Talpur, M. S. H., Idrissa Kayijuka, & Erkan Yaşar. (2021). Machine Learning Classifiers: A Brief Primer. *University of Sindh Journal of Information and Communication Technology, 5*(2), 63-68.

[27] I. Sharafaldin, A. H. Lashkari, S. Hakak, and A. A. Ghorbani, ''Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy,'' in Proc. Int. Carnahan Conf. Secur. Technol. (ICCST), Oct. 2019, pp. 1–8.

[28] Almiani, Muder, Alia Abughazleh, Yaser Jararweh, and Abdul Razaque. "Resilient Back Propagation Neural Network Security Model for Containerized Cloud Computing." *Simulation Modelling Practice and Theory* 118 (2022): 102544.

[29] Qamar, R., Zardari, B. A., Arain, A. A., Khoso, F. H., & Jokhio, F. A. (2021). Detecting Distributed Denial of Service attacks using Recurrent Neural Network. *University of Sindh Journal of Information and Communication Technology , 5*(2), 86-94

[30] Zhu, Hongfei, Jorge Leandro, and Qing Lin. "Optimization of Artificial Neural Network (ANN) for Maximum Flood Inundation Forecasts." Water 13, no. 16 (2021): 2252.

[31] Bayrak, Sengul, Eylem Yucel, Hidayet Takci, and Ruya Samli. "Classification of epileptic electroencephalograms using time-frequency and back propagation methods." *Cmc-Computers Materials & Continua* (2021).

[32] Qamar, R., Zardari, B., Arain, A., Hussain, Z., & Burdi, A. (2022). A Comparative Study of Distributed Denial of Service Attacks on The Internet Of Things By Using Shallow Neural Network. *Quaid-E-Awam University Research Journal of Engineering, Science & Technology, Nawabshah. 20*(01), 61-73.

[33] Trivedi, Udai Bhan, and Priti Mishra. "Improving Steepest Descent Method by Learning Rate Annealing and Momentum in Neural Network." In Evolving Technologies for Computing, Communication and Smart World, pp. 181-194. Springer, Singapore, 2021.

[33] Pan, Li, and Qian Zhang. "Face Recognition Algorithm Comparison based on Backpropagation Neural Network." In Journal of Physics: Conference Series, vol. 1865, no. 4. IOP Publishing, 2021

[34] Vinothkumar, V., and R. Kanimozhi. "Power quality improvement by PV integrated UPQC using multi-level inverter with resilient back propagation neural network approach." *Journal of Intelligent & Fuzzy Systems* Preprint (2022): 1-18.

[35] Gupta, Rahul, and P. C. Gupta. "Implementation of cognitive radio networks for optimum spectrum utilization through feed forward backpropagation artificial neural network." *Materials Today: Proceedings* (2022).

[36] Liang, Jinxiu, Yong Xu, Chenglong Bao, Yuhui Quan, and Hui Ji. "Barzilai–Borwein-based adaptive learning rate for deep learning." *Pattern Recognition Letters* 128 (2019): 197-203.

[37] Yuberta, Andre. "Jaringan Syaraf Tiruan dengan Algoritma Backpropagation dalam Memprediksi Hasil Asesmen Nasional Berbasis Komputer (ANBK) SMP Se Kota Sawahlunto." *Jurnal Informasi dan Teknologi* (2022).

[38] Liu, Xia, and Gang Bai. "Research on Intelligent Algorithm of the AC Motor Speed Regulation System Based on the Neural Network." *Mobile Information Systems* 2022 (2022).