SSRG International Journal of Computer Science and Engineering
ISSN: 2348 – 8387 / https://doi.org/10.14445/23488387/IJCSE-V10I3P102

Volume 10 Issue 3, 11-16, March 2023

Original Article

Gradient Fuzzy based Cyberattack Detection

R. Surendiran[1], S. Veerapandi[2]

[1]*School of Information Science, Annai College of Arts and Science, Tamilnadu, India.*
[2]*Department of Computer Science, Mannar Thirumalai Naicker College, Tamilnadu, India.*

[1]*Corresponding Author : surendiranmca@gmail.com*

Received: 19 January 2023 Revised: 02 March 2023 Accepted: 13 March 2023 Published: 28 March 2023

Abstract *- Cloud computing is the need-based supply of computer system resources, particularly processing power and data storage, without necessitating direct and active monitoring by users. Numerous sites, each of which is a data centre, frequently host large cloud operations. A cloud assault is a cyberattack that targets a platform of cloud-based services, including hosted apps in PaaS or SaaS frameworks, storage services, and computer services. In this paper, a novel Gradient Fuzzy based Cyberattack detection in healthcare environment technique has been proposed to detect and recover the attacker. To preprocess the input NSL KDD dataset utilized for normalization and data cleaning methods to select the features extraction via CNN. Fuzzy K means clustering uses the features acquired via CNN is used for creating bounding boxes for extracted features. To identify the attack and to classify the type of attack by means of the Mobile Net technique. MATLAB implemented the simulation result. The efficiency of the suggested methodology is analyzed using the parameters like precision, Specificity, Accuracy, and recall. The performance analysis of the proposed is calculated based on the parameters like accuracy. The proposed achieves an accuracy range of 97.95%. The result shows that the proposed enhances the overall accuracy better than 37.45 %, 22.85%, and 17.07% in TPA, ITA, and EDoS.*

Keywords *- Fuzzy K means clustering, Preprocessing, MATLAB, Cyberattack detection, Convolution Neural Network.*

1. Introduction

A network-based system known as cloud computing focuses on offering virtualized resources to its users on a pay-for-uses basis [1]. It is a cutting-edge information system architecture seen as the direction of computing technologies by fusing cutting-edge technologies like virtualization and service-oriented architecture (SOA) [2,3].

A DoS attack may be defined as an attempt to temporarily stop a cloud computing service or resource from offering its regular services [4]. DoS assaults, which frequently target the connection or capacity of computer networks, jeopardize the availability of cloud resources and services [5,6].

One source of Cyber-attack can easily reduce the severity of the attacks because the defenders can block the network traffic from attacker sources. However, it is challenging to recognize and defend against attacks on different attack systems [7,8]. So, it is very difficult to detect the difference between malicious packets and legitimate internet traffic [9,10]. The major contributions of the proposed technique are given below:

- Initially, the preprocessing input NSL KDD Dataset utilized normalization and Data cleaning methods.
- Then select the features extraction via Convolution Neural Network.
- Fuzzy K means clustering uses the features acquired via CNN is used for creating bounding boxes for extracted features.
- To identify the attack, classify the type of attack using the Mobile Net technique.

The remainder of the analysis is organized as shown below. The literature review is thoroughly explained in Section II. The suggested approach is described in Section III. Section IV presents the results, while Section V presents the conclusions.

2. Literature Review

In 2020, Virupakshar, K.B., et al. [1] suggested a cloud operating system with a built-in firewall, DDoS detection software, an Open Stack integrated firewall, and raw socket programming for network traffic monitoring. The dataset DNN, KNN, and Decision Tree algorithms are used in DDoS attacks. DDoS attacks are discovered as a result of the experiment, and the private cloud administrator is contacted.

In 2020, Saxena, R. and Dey, S. [2] suggested a packet traceback system based on a third-party auditor (TPA), which is used to determine where the DDoS attack originated. Because of its powerful identification element, which is dependent on the vulnerabilities the intruder left behind, it offers an effective and fruitful solution. The experimental findings are presented to demonstrate the

efficacy of the suggested approach for DDoS attack mitigation and prevention.

In 2022 Liu, D. and Hu [3] suggested a brand-new Imperceptible Transfer Attack (ITA), a 3D point cloud assault from two fresh and difficult angles are offered. Numerous tests show that our ITA assault is stealthy and more transferrable than state-of-the-art, confirming our defensive plan's supremacy.

In 2022 Aldhyani, T.H. and Alkahtani, H. [4] offered a successful strategy for reducing EDoS assaults in cloud computing. Methods for identifying such widespread assaults on various cloud computing smart grids have been proposed as mitigation measures. The suggested algorithms' findings revealed that the RF method had a binary classification accuracy of 98%, and the SVM model had a multi-classification accuracy of 97.54%.

In 2022 Kautish, S. et al. [5] presented a cutting-edge DDoS defence plan for the hybrid cloud setting. The proposed SDMTA mitigation architecture incorporates integrated network monitoring to support detection methods—the expected detection rates over the input dataset for the proposed and current state-of-the-art models. The system's accuracy, specificity, and sensitivity were determined to be 99.7%, 98.32%, and 99.92%, respectively, compared to the current state-of-the-art model.

3. Proposed Methodology

In this paper, a novel gradient fuzzy-based cyberattack detection in healthcare environment technique has been proposed to detect and recover the attacker. To preprocess the input NSL KDD dataset utilized for normalization and data cleaning methods to select the features extraction via CNN. Fuzzy K means clustering uses the features acquired via CNN is used for creating bounding boxes for extracted features. To identify the attack and classify the type of attack using the Mobile Net technique. The overall workflow of the proposed methodology is shown in Figure 1.

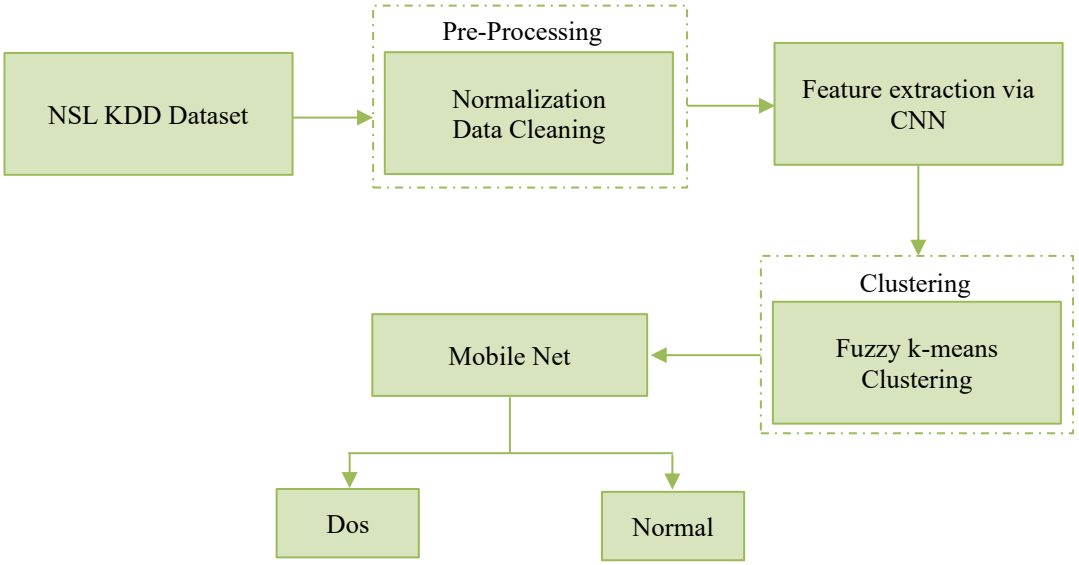

Fig. 1 Overall proposed diagram

3.1. Preprocessing

It is preprocessed to eliminate duplicate and redundant instances and to tidy up missing data. The dataset can be standardized and cleaned during the preprocessing stage. The z-score is obtained as the initial stage in the normalization procedure. The Z-score will be represented by Equation 1

$$A=[(Y-\mu)/\sigma] \quad (1)$$

Where μ is the mean of the patient population, and σ is the SD of the dataset.

3.2. Feature Extraction Via CNN

After the feature extraction phase, the input is fed into optimized CNN. The convolutional, pooling, and completely connected layers are the three significant layers that makeup CNN in general. The basic building block of the CNN architecture, the convolution layer, extracts various simple visual features from the input image. Convolution operation and activation function, respectively, reflect the linear and nonlinear operations it carries out. Different features from the input image are extracted by sequentially applying kernel (filter) using the linear convolution procedure. By convolving (sliding) the kernel across the full input image, the kernel is sequentially applied to the input map.

3.3. Fuzzy K-Means Clustering

Fuzzy K-means clustering is a significant clustering technique for unsupervised learning tasks. The proposed EC-DRE method utilizes the k-means clustering algorithm to perform clustering. By reducing the objective function

based on a Squared-Error-Function (SEF), this technique seeks to locate the optimal cluster centroid. The clusters have a better formation when using the K-means algorithm when the average distance between each cluster node is reduced. It is more effective to evenly distribute the nodes across clusters and balance the network's load. This method is quite helpful for creating clusters for various WSN applications. The K-means algorithm's objective function is defined as:

$$K = \sum_{x=1}^{m} \sum_{y=1}^{l} dis(a_x, a_z)^2 \quad x = 1,2,\dots,m, y = 1,2,\dots,l \qquad (2)$$

Where $dis(a_x, a_z)^2$ is the Euclidean distance calculated between node a_{ji} and its cluster centroid zy, where x represents the number of nodes and y represents the number of clusters. This algorithmic process comprises several parts.

Phase 1: Find the L centroid points in the space that the data set represents, where L is a predetermined number.
Phase 2: Each data point should be assigned to the appropriate cluster with the closest centroid distance.
Phase 3: Recalculate the L centroids' locations after all the data points have been clustered.
Phase 4: Repeat Phases 2 and 3 until there is no discernible change in the centroids' positions.

3.4. Mobile Net

Features from preprocessed assaults are extracted using MobileNet. We present depth-separable filters, the foundation of MobileNet, in this section. Before examining the resolution and width multipliers, the two hyperparameters that minimize the model, let's first speak about MobileNet. This network uses depth-wise separable convolution (DSConv) instead of regular convolution as in conventional networks. A MobileNet network based on DSConv can perform the same feature extraction function as a regular convolution network with fewer model parameters. As a result, network resource restrictions on hardware can be reduced. A depthwise separable convolution combines pointwise convolution (PWConv) and depthwise convolution (DWConv).

In DWConv, each convolution kernel only handles one channel, with no multidimensional convolution kernels. The channels cannot be increased after DWConv. Furthermore, since each convolution operation is carried out sequentially between channels, employing the feature data from many channels at the same spatial location is impossible. In order to produce new feature maps, the feature maps produced by DWConv must be combined using PWConv. The convolution kernel size is 1x1, which differentiates PWConv from ordinary convolution. In the basic model, there are a number of levels of abstraction, a combination of various convolutions with rectified linear units (ReLUs). Using the resolution multiplier variable ω for the internal portrayal of each layer of the input image reduces its dimensionality and internal portrayal with the identical variable of the input images. The size of the feature vector map $f_m * f_m$ and the kernel is of size $k_s * k_s$ the input variable is referred to as x, and the output variable is represented as y. The following Equation (4) can be used to evaluate the overall computation efforts C_{eff} for the central abstract layers of the network.

$$C_{eff} = k_s * k_s * \omega * \alpha f_m + \omega * \rho * \alpha f_m * \alpha f_m \qquad (3)$$

The multiplier value is explicit for context, and for the resulting breakdown in weed classification, the value of multiplier ω is considered as the range from 1 to n. The variable resolution multiplier is recognized by α, and the value is estimated as 1. The computational efforts are identified with the variable $cost_{eff}$ and it is evaluated using Equation (4),

$$cost_{eff} = k_s * k_s * \omega * \rho * f_m * f_m \qquad (4)$$

MobileNet integrates with the DWConv, PWConv are limited in the reduction variable recognized by the variable D that is similar to Equation (5),

$$D = \frac{f_s * f_s * \omega * \alpha f_m + \omega * \rho * \alpha f_m * \alpha f_m}{f_s * f_s * \omega * \rho * f_m * f_m} \qquad (5)$$

In different situations, the width multiplier and resolution multiplier helps to adjust the window size for accurate prediction.

3.5. Dataset

To solve some of the noted issues with the KDD'99 data set inherent issues, the NSL-KDD data collection was suggested. This upgraded version of the KDD dataset is a good benchmark dataset to enable researchers to evaluate different intrusion detection approaches, although some of McHugh's corrected difficulties persist due to the lack of publicly available datasets for network-based IDS.

3.5.1. Accuracy

overall dataset's percentage of samples that were properly categorized.

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN} \qquad (6)$$

3.5.2. Precision

Proportion of accurately categorized positive sample data.

$$\text{Precision} = \frac{TP}{TP+FP} \qquad (7)$$

3.5.3. Recall

Proportion of positively predicted samples over all samples in the relevant class that were correctly predicted.

$$\text{Recall} = \frac{TP}{TP+FN} \qquad (8)$$

3.5.4. F1 Score

Harmonic average of recall and precision

$$\text{F1} = \frac{2\,X\,TP}{2\,X\,TP+FN+FP} \qquad (9)$$

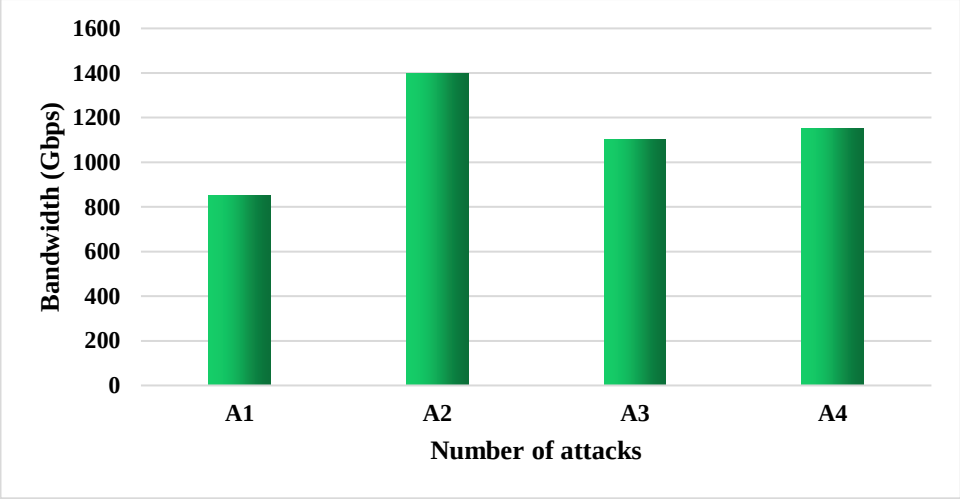

Fig. 2 shows an overall decline in attack frequency and shows that attack sizes have grown considerably

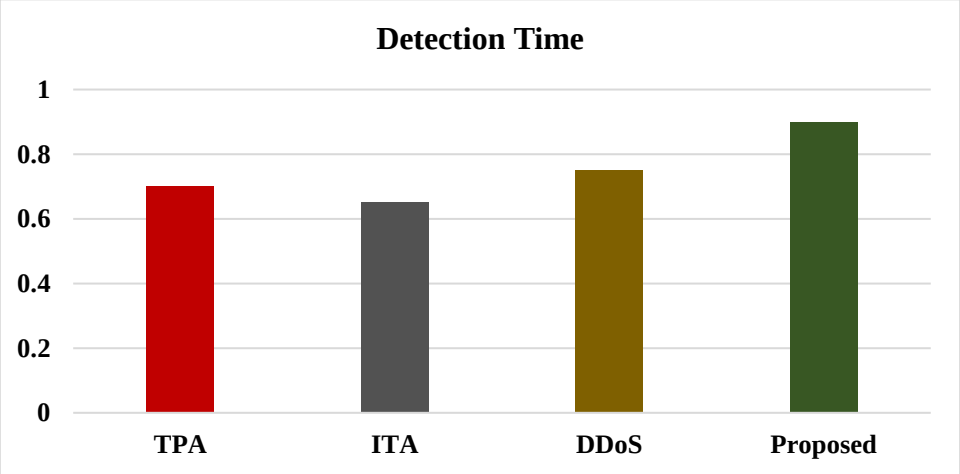

Fig. 3 Detection Time

Attack detection time is the total amount of time needed to identify the attacker's IP address, identify susceptible behaviour, and contact the coordinator to validate other properties. Fig. 3 displays the average amount of time needed to identify a single attack. Compared to existing approaches, the proposed has the quickest attack detection time and is more effective than the TPA, ITA, and DDoS.

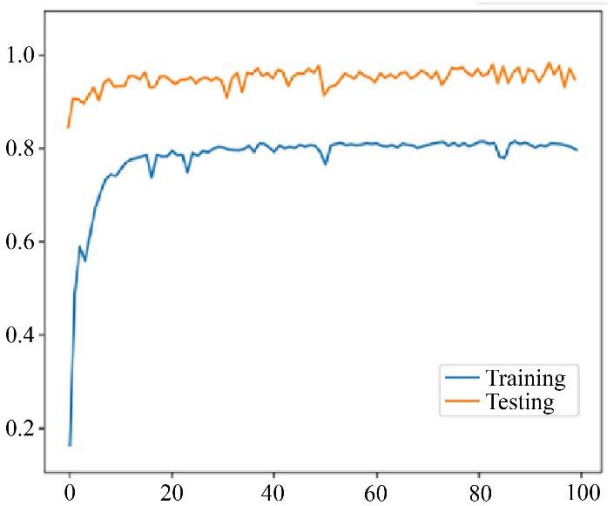

Fig. 4 Training and testing accuracy of the proposed method

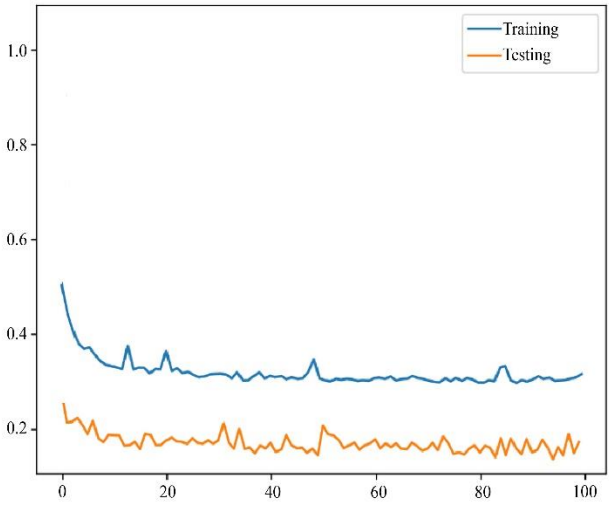

Fig. 5 Training and testing loss of the proposed method

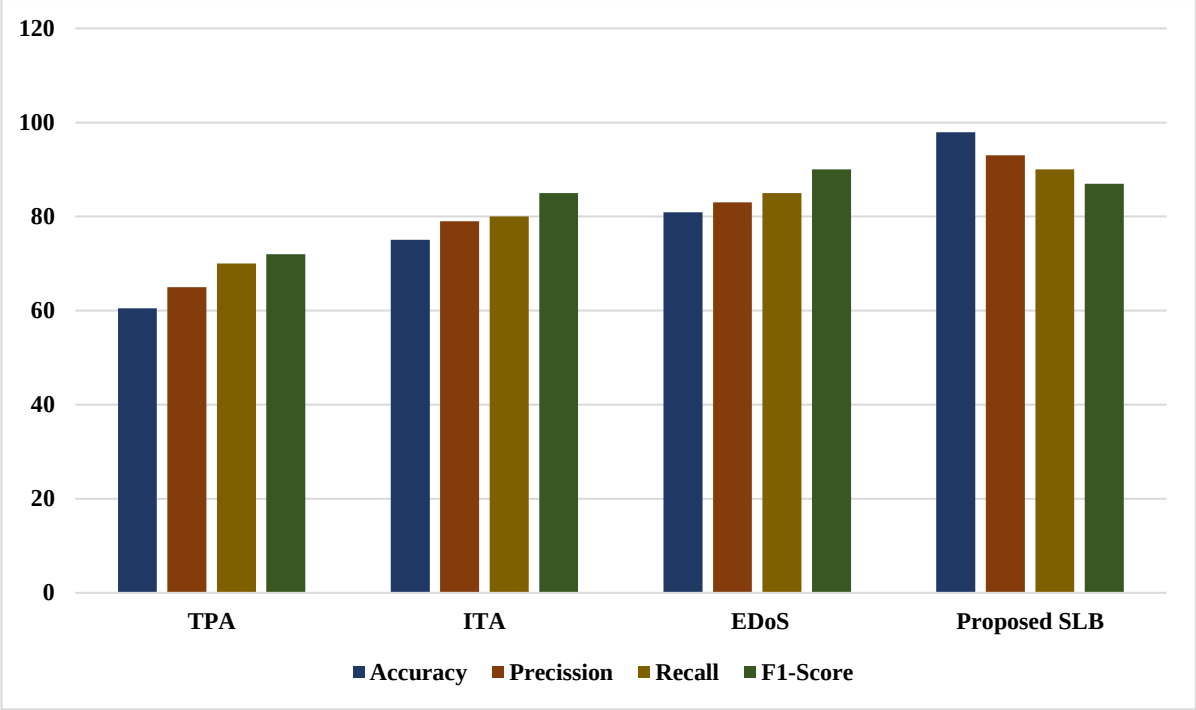

Fig. 6 Comparison with performance metrics

Figure. 4 shows the accuracy curve with epochs and accuracy on both vectors; the method accuracy increases with increasing epochs. The epoch versus loss curve in Figure 5 demonstrates how the model loss decreases as epochs are improved.

Fig 6 depicts the accuracy, Precision, Recall and F1Score among the suggested method and existing methods. From the observations, it is proved that the Precision, Specificity, accuracy, and recall of the suggested method are greater than the existing methods. A comparison analysis is carried out between the suggested method. In order to demonstrate that the outcome of the suggested strategy is more effective, the performance of existing methods was compared using Accuracy, Specificity, Precision and Recall.

4. Conclusion

In this paper, a novel Gradient Fuzzy based Cyberattack detection in healthcare environment technique has been proposed to detect and recover the attacker. To preprocess the input NSL KDD Dataset utilized normalization and Data cleaning methods to select the feature extraction via CNN. Fuzzy K means clustering uses the features acquired via CNN is used for creating bounding boxes for extracted features. To identify the attack and classify the type of attack using the Mobile Net technique. MATLAB implemented the simulation result. The efficiency of the suggested methodology is analyzed using the parameters like precision, Specificity, Accuracy, and recall. The performance analysis of the proposed is calculated based on the parameters like accuracy. The proposed achieves an accuracy range of 97.95%. The result shows that the proposed enhances the overall accuracy better than 37.45 %, 22.85%, and 17.07% in TPA, ITA, and EDoS.

References

[1] Waqas Ahmad et al., "Cyber Security in IoT-Based Cloud Computing: A Comprehensive Survey," *Electronics*, vol. 11, no. 1, p. 16, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[2] Sangwon Hyun et al., "Interface to Network Security Functions for Cloud-Based Security Services," *IEEE Communications Magazine*, vol. 56, no. 1, pp. 171-178, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[3] Isaac Odun-Ayo et al., "Cloud-Based Security Driven Human Resource Management System," *Advances in Digital Technologies*, pp. 96-106, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[4] Alaeddine Mihoub et al., "Denial of Service Attack Detection and Mitigation for Internet of Things Using Looking-Back-Enabled Machine Learning Techniques," *Computers & Electrical Engineering*, vol. 98, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[5] Xia Chen et al., "Distributed Resilient Control Against Denial of Service Attacks in DC Microgrids with Constant Power Load," *Renewable and Sustainable Energy Reviews*, vol. 153, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[6] Ammarah Cheema et al., "Prevention Techniques against Distributed Denial of Service Attacks in Heterogeneous Networks: A Systematic Review," *Security and Communication Networks*, vol. 2022, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[7] Hammond Pearce et al., "FLAW3D: A Trojan-Based Cyber Attack on the Physical Outcomes of Additive Manufacturing," *IEEE/ASME Transactions on Mechatronics*, vol. 27, no. 6, pp. 5361-5370, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[8] V. Bolbot et al., "*Identification of Cyber-Attack Scenarios in a Marine Dual-Fuel Engine*," Trends in Maritime Technology and Engineering, CRC Press, vol. 1, pp. 503-510, 2022. [Google Scholar] [Publisher Link]

[9] Hashim Albasheer et al., "Cyber-attack Prediction Based on Network Intrusion Detection Systems for Alert Correlation Techniques: A Survey," *Sensors*, vol. 22, no. 4, p. 1494, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[10] Jie Yang et al., "A Robust Active Distribution Network Defensive Strategy against Cyber-Attack Considering Multi-Uncertainties," *IET Generation, Transmission & Distribution*, vol. 16, no. 8, pp. 1476-1488, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[11] Karan B. Virupakshar et al., "Distributed Denial of Service (DDoS) Attacks Detection System for Openstack-Based Private Cloud," *Procedia Computer Science*, vol. 167, pp. 2297-2307, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[12] Rajat Saxena, and Somnath Dey, "DDoS Attack Prevention using Collaborative Approach for Cloud Computing," *Cluster Computing*, vol. 23, no. 2, pp. 1329-1344, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[13] Daizong Liu, and Wei Hu, "Imperceptible Transfer Attack and Defense on 3D Point Cloud Classification," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 45, no. 4, pp. 4727-4746, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[14] Theyazn H. H. Aldhyani, and Hasan Alkahtan, "Artificial Intelligence Algorithm-Based Economic Denial of Sustainability Attack Detection Systems: Cloud Computing Environments," *Sensors*, vol. 22, no. 13, p .4685, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[15] Sandeep Kautish, A. Reyana, and Ankit Vidyarthi, "SDMTA: Attack Detection and Mitigation Mechanism for DDos Vulnerabilities in Hybrid Cloud Environment," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 9, pp. 6455-6463, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[16] G. P. Dimf, P. Kumar, and K. Paul Joshua, "CNN with BI-LSTM Electricity Theft Detection based on Modified Cheetah Optimization Algorithm in Deep Learning," *SSRG International Journal of Electrical and Electronics Engineering,* vol. 10, no. 2, pp. 35-43, 2023. [CrossRef] [Publisher Link]

[17] Sheetakshi Shukla, and Tasneem Bano Rehman, "VAPT & Exploits, along with Classification of Exploits," *SSRG International Journal of Computer Science and Engineering*, vol. 9, no. 3, pp. 1-4, 2022. [CrossRef] [Publisher Link]

[18] S. Kannan, and T. Pushparaj, "Creation of Testbed Security using Cyber-Attacks," *SSRG International Journal of Computer Science and Engineering*, vol. 4, no. 11, pp. 4-14, 2017. [CrossRef] [Publisher Link]

[19] G. P. Dimf, P. Kumar, and K. Paul Joshua, "CNN with BI-LSTM Electricity Theft Detection based on Modified Cheetah Optimization Algorithm in Deep Learning," *SSRG International Journal of Electrical and Electronics Engineering,* vol. 10, no. 2, pp. 35-43, 2023. [CrossRef] [Publisher Link]

[20] Sabita Nayak, and Amit Kumar, "An Intelligent CSO-DBNN Based Cyber Intrusion Detection Model for Smart Grid Power System," *International Journal of Engineering Trends and Technology,* vol. 68, no. 6, pp. 50-57, 2020. [Google Scholar] [Publisher Link]