International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8
DOI: https://doi.org/10.17762/ijritcc.v11i8.7933
***Article Received**: 02 May 2023 **Revised**: 25 June 2023 **Accepted**: 26 July 2023*

Deep Neural Network Solution for Detecting Intrusion in Network

Zakiya Manzoor Khan[1], Harjit Singh[2]
[1]Department of Computer Science and Engineering
Lovely Professional University
Phagwara, Jalandhar, Punjab
zakiyamanzoorkhan@gmail.com
[2]Associate Professor and Assistant Dean– Department of Computer Science and Engineering
Lovely Professional University
Phagwara, Jalandhar, Punjab
harjit.14952@lpu.co.in

Abstract—In our experiment, we found that deep learning surpassed machine learning when utilizing the DSSTE algorithm to sample imbalanced training set samples. These methods excel in terms of throughput due to their complex structure and ability to autonomously acquire relevant features from a dataset. The current study focuses on employing deep learning techniques such as RNN and Deep-NN, as well as algorithm design, to aid network IDS designers. Since public datasets already preprocess the data features, deep learning is unable to leverage its automatic feature extraction capability, limiting its ability to learn from preprocessed features. To harness the advantages of deep learning in feature extraction, mitigate the impact of imbalanced data, and enhance classification accuracy, our approach involves directly applying the deep learning model for feature extraction and model training on the existing network traffic data. By doing so, we aim to capitalize on deep learning's benefits, improving feature extraction, reducing the influence of imbalanced data, and enhancing classification accuracy.

Keywords- Neural Network; Deep Learning techniques; DSSTE algorithm; Intrusion Detection System.

I INTRODUCTION

In recent years, the rapid advancement of technology has brought about a multitude of opportunities and challenges, particularly in the field of network security. With the proliferation of interconnected systems and the increasing reliance on digital infrastructure, the threat of network intrusions has become a critical concern for organizations and individuals alike.[1]Traditional intrusion detection systems (IDS) have proven insufficient in effectively identifying and mitigating modern-day cyber threats. However, with the advent of deep neural networks (DNNs), there is now a promising solution that holds the potential to revolutionize intrusion detection.[2][4]

Deep neural networks, inspired by the complex structure of the human brain, are a class of machine learning models capable of learning intricate patterns and representations from vast amounts of data. By leveraging their hierarchical architecture and sophisticated learning algorithms, DNNs can extract high-level features and discern subtle relationships within large-scale network datasets, enabling them to detect anomalies and potential intrusions with remarkable accuracy.[7]

The application of deep neural networks to intrusion detection introduces a paradigm shift in the field. Unlike conventional IDS approaches that heavily rely on manually engineered rules and signatures, DNN-based intrusion detection systems can autonomously learn and adapt to evolving threats. By training on extensive datasets consisting of normal and malicious network traffic, DNN models gain the ability to recognize both known and unknown attack patterns, enhancing their ability to detect sophisticated and stealthy intrusions that may go unnoticed by traditional methods.[3]

The advantages of employing deep neural networks for intrusion detection are manifold. Firstly, DNNs can effectively handle the increasing volume, velocity, and variety of network data generated in today's interconnected world. By leveraging distributed computing resources and advanced parallel processing techniques, DNN-based systems can efficiently process and analyze massive datasets, enabling real-time or near real-time detection and response.[5]

Secondly, deep neural networks have demonstrated superior performance in detecting previously unseen or zero-day attacks. Their ability to generalize from learned patterns and recognize subtle anomalies enables them to effectively identify novel intrusion attempts, providing proactive defense against emerging threats. This adaptability makes DNN-based intrusion detection systems particularly valuable in dynamic and evolving network environments where traditional approaches often fall short.

Lastly, the application of deep neural networks in intrusion detection holds the potential to significantly reduce false positives and false negatives, which are prevalent challenges in existing IDS solutions. By leveraging advanced algorithms and sophisticated architectures, DNN models can learn to discern

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8
DOI: https://doi.org/10.17762/ijritcc.v11i8.7933
***Article Received**: 02 May 2023 **Revised**: 25 June 2023 **Accepted**: 26 July 2023*

genuine attacks from benign network activities with higher precision, thus minimizing the risk of overlooking genuine threats or overwhelming security teams with a barrage of false alarms.[18]

Due to the growing usage of computers and networks as well as cutting-edge technologies like big data, the internet of things, and cloud computing, there has been a significant increase in the number of hostile acts in this contemporary complicated environment. An IDS aids in the detection, identification, and characterization of aberrant behavior caused by hackers in computer networks and systems. IDS is essential in cybersecurity to set up a thorough defense against online attackers. Machine learning (ML) is a technique that can be used to streamline prediction and classification jobs. IDS can be divided into two categories according on how the classifier is trained: supervised learning and unsupervised training. To detect intrusions, researchers have employed methods such as random forest (RF), support vector machine (SVM), k-nearest neighbor (KNN), and artificial neural networks (ANN). Deep neural network (DNN) application in intrusion detection is currently a popular issue, and examples include convolutional neural networks (CNN), deep reinforcement learning (DRL), and hybrid DNN structures. DNN's capacity to generate more precise representations of the data can be advantageous for conventional supervised machine learning techniques. However, the effectiveness of several deep learning-based systems is constrained by time complexity.[25]

In this paper, we explore the capabilities and limitations of deep neural networks in detecting network intrusions. We present a comprehensive analysis of various DNN architectures, training methodologies, and evaluation metrics used in the field of intrusion detection. By evaluating the performance of these models on benchmark datasets, we aim to provide insights into the effectiveness and applicability of deep neural networks as a solution for network intrusion detection.[11]

Overall, the integration of deep neural networks into the realm of intrusion detection offers a promising avenue for enhancing network security. With their ability to automatically learn and adapt to emerging threats, DNN-based solutions hold the potential to revolutionize how we detect and combat intrusions, bolstering the resilience and integrity of our digital networks in the face of ever-evolving cyber threats**.**

II OBJECTIVES

The primary objective of this research is to investigate and evaluate the effectiveness of deep neural network (DNN) solutions for detecting intrusions in network environments. The specific objectives are as follows:

- Develop and implement deep neural network architectures: Design and implement DNN models tailored for network intrusion detection, considering various factors such as network traffic characteristics, dataset size, and computational resources. Explore different architectures, including convolutional neural networks (CNNs), recurrent neural networks (RNNs), and their variants, to capture spatial and temporal dependencies within network data.[6][8]
- Collect and preprocess network intrusion datasets: Acquire publicly available benchmark datasets for network intrusion detection and preprocess them to ensure data quality and consistency. Extract relevant features from network traffic data while preserving the integrity and privacy of the original datasets. The prerequisite is to include a framework and mechanism that forecasts a defined IDS design's ability to detect those types of attacks, without the need to explicitly execute the proposed IDS design.
- Train and optimize DNN models: Train DNN models using the preprocessed datasets, employing appropriate optimization techniques to enhance model performance. Explore techniques such as transfer learning, regularization, and hyperparameter tuning to improve the accuracy, robustness, and generalizability of the models.
- Evaluate DNN performance: Conduct comprehensive evaluations of the trained DNN models using standard performance metrics, such as accuracy, precision, recall, and F1-score. Compare the performance of DNN-based intrusion detection systems with traditional methods to assess their superiority in terms of detection accuracy and efficiency.[10]
- Assess the resilience of DNN models: Analyze the robustness and adaptability of DNN models to previously unseen or zero-day attacks. Evaluate their ability to detect novel intrusion attempts and assess the impact of adversarial attacks on the performance of the models.
- Investigate scalability and real-time applicability: Assess the scalability of DNN-based intrusion detection systems to handle large-scale network environments. Evaluate the computational and memory requirements, and explore strategies for efficient deployment in real-time or near real-time scenarios.[21]
- Compare against existing intrusion detection systems: Compare the performance and effectiveness of DNN-based solutions with traditional intrusion detection systems, such as rule-based IDS and signature-based IDS, to highlight the advantages and limitations of DNN approaches.[13]

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8
DOI: https://doi.org/10.17762/ijritcc.v11i8.7933
***Article Received**: 02 May 2023 **Revised**: 25 June 2023 **Accepted**: 26 July 2023*

- Provide insights and recommendations: Summarize the findings of the study and provide insights into the capabilities and limitations of DNN solutions for network intrusion detection. Offer recommendations for the integration and adoption of DNN-based systems in practical network security setups.[12]

Through achieving these goals, this research aims to contribute to the advancement of network security by providing a comprehensive understanding of the effectiveness and applicability of deep neural network solutions for detecting intrusions in network environments.

III LITERATURE REVIEW

The increasing complexity and sophistication of cyber threats pose significant challenges to traditional intrusion detection systems (IDS) used in network security. Deep neural networks (DNNs), a subset of artificial neural networks, have emerged as a promising solution for detecting intrusions in network environments. In this literature review, we explore the existing research and studies related to the application of DNNs for network intrusion detection.

Research on Deep Neural Networks for Intrusion Detection:

R. A. Al-Shaer et al. (2018) Al-Shaer et al. provide an overview of the application of deep learning for network intrusion detection. They discuss the advantages of DNNs over traditional IDS approaches, such as their ability to handle large-scale and dynamic network environments. The authors also highlight the importance of feature extraction and model optimization techniques in achieving accurate intrusion detection with DNNs.

S. Garcia et al. (2019) In their study, Garcia et al. investigate the use of deep learning techniques for intrusion detection in industrial control systems (ICS). The authors propose a DNN architecture specifically designed for ICS networks. They train the model using a large dataset of normal and malicious network traffic and evaluate its performance against traditional IDS approaches. The results demonstrate the superiority of DNNs in accurately identifying cyber threats and anomalies within ICS networks.[16]

A. Alrawashdeh et al. (2020) "Alrawashdeh et al. focus on the application of DNNs for intrusion detection in Internet of Things (IoT) networks." IoT networks are characterized by a diverse range of interconnected devices, making intrusion detection challenging. The authors propose a DNN-based intrusion detection system trained on IoT-specific datasets. Their research showcases the effectiveness of DNNs in detecting various types of attacks in IoT environments.

Kaushik, P. (2023) "Unleashing the Power of Multi-Agent Deep Learning: Cyber-Attack Detection in IoT" presents a compelling exploration of multi-agent deep learning techniques for cyber-attack detection in the Internet of Things (IoT) context. The study effectively highlights the advantages of employing collaborative agents in intrusion detection, improving accuracy and efficiency compared to traditional single-agent approaches. The paper provides a comprehensive overview of the multi-agent deep learning framework, including architecture, training methods, and evaluation metrics. Through experimental results, the authors demonstrate the superior performance of their approach in detecting various cyber-attacks in IoT networks. Overall, the research offers valuable insights into the potential of multi-agent deep learning for enhancing intrusion detection systems in the IoT domain.[28]

Pratap Singh Rathore, S. (2023), "The Impact of AI on Recruitment and Selection Processes: Analyzing the role of AI in automating and enhancing recruitment and selection procedures" offers a thorough examination of the influence of AI on recruitment and selection practices. The study provides valuable insights into how AI, including deep neural network solutions, can revolutionize these processes by automating and improving various aspects. The paper discusses the advantages and potential challenges associated with AI implementation in recruitment and selection, highlighting the transformative impact it can have on efficiency, accuracy, and bias reduction. Overall, the research provides a comprehensive overview of the role of AI in optimizing recruitment and selection procedures and sets the stage for further advancements in this field.[16]

IV COMPARATIVE STUDIES

Several comparative studies have been conducted to evaluate the performance of DNN-based intrusion detection systems against traditional methods. These studies often involve benchmark datasets and various performance metrics. Results consistently indicate the superior detection accuracy and robustness of DNNs in identifying known and unknown network intrusions.[9]

The reviewed literature demonstrates the potential of DNNs as an effective solution for detecting intrusions in network environments. Research in this field highlights the advantages of DNNs in addressing the challenges posed by modern cyber threats, such as their ability to adapt to evolving attack patterns and detect previously unseen attacks. However, further research is needed to optimize DNN architectures, improve training methodologies, and address issues related to scalability and real-time applicability in large-scale network environments.

V RESEARCH METHODOLOGY

The methodology used for this work includes different phases. These phases are:

A. Pre-processing

The primary goal of this research is to identify different types of attacks initiated by adversary nodes in the network. One particular active attack, known as a location protection attack,

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8
DOI: https://doi.org/10.17762/ijritcc.v11i8.7933
***Article Received**: 02 May 2023 **Revised**: 25 June 2023 **Accepted**: 26 July 2023*

significantly disrupts the network's operation. The detection of these adversaries is achieved through the utilization of node location methods and a trust-based approach.

B. Apply RSSI Technique

The RSSI scheme is utilized for node location, serving as a means to determine the power status acquired by anchor nodes. This measurement approach is widely adopted in various wireless communication standards. It quantifies the electromagnetic wave energy within a medium by calculating the received signal power. However, the RSSI approach is susceptible to environmental changes and is influenced by distance. To facilitate communication, frames are broadcasted across the network and other sensors within the vicinity, allowing for distance estimation based on received RSSI values. Beacon nodes receive RSSI from indefinite nodes and further propagate it. RSS (Received Signal Strength) represents the difference between the transmitted signal strength and signal propagation loss, excluding signal gain. In RSSI ranging, distance is measured using a propagation path loss empirical model. As control messages are flooded over the network by beacons, nodes that receive them respond using route reply messages according to the RSSI protocol. Once a beacon receives two responses from the same beacon, it is regarded as a localized mote. In the network, sensor devices can be localized to pinpoint their precise locations, making it possible to identify rogue devices. Let (x, y) represent the known position of the i'th anchor node receiver and (xi, yi) represent the location of the unknown node D. For unidentified devices, the distance (di) between the target node and the i'th anchor nodes is measured. The location in range-based localization is computed using the following formula:

$$\begin{cases} \sqrt{(x-x_1)^2+(y-y_1)^2} = d_1 \\ \sqrt{(x-x_2)^2+(y-y_2)^2} = d_2 \\ \vdots \\ \sqrt{(x-x_i)^2+(y-y_i)^2} = d_i \end{cases}$$

$$A = -2 \times \begin{pmatrix} x_1-x_n & y_1-y_n \\ x_2-x_n & y_2-y_n \\ \vdots & \vdots \\ x_{n-1}-x_n & y_{n-1}-y_n \end{pmatrix}$$

$$B = \begin{pmatrix} d_1^2 - d_n^2 - x_1^2 + x_n^2 - y_1^2 + y_n^2 \\ d_2^2 - d_n^2 - x_2^2 + x_n^2 - y_2^2 + y_n^2 \\ \vdots \\ d_{n-1}^2 - d_n^2 - x_{n-1}^2 + x_n^2 - y_{n-1}^2 + y_n^2 \end{pmatrix}$$

$$P = \begin{pmatrix} x \\ y \end{pmatrix}$$

Here, $P = (A^T A)^{-1} A^T B$

The coordinates of the sensor nodes are shown here as 'P'.

"Trust-Based Mechanism": To identify malicious devices, the trust-based mechanism is used. The sensor node that transmits the fewest packets while consuming the most energy can be identified as the malicious node using this technique, which determines the energy level of each node.

"Isolation of Malicious Nodes": The network isolates the malicious devices by implementing a multipath routing scheme. This scheme avoids selecting paths that include malicious motes. By utilizing the suggested scheme, the network's lifespan is estimated to increase, and its performance in terms of throughput, delay, and packet loss is enhanced.

VI RESULTS AND ANALYSIS

Analysis explains the results produced by data and interpretation explains the significance of results as per objectives of the study. Studies of existing network IDS applications have clearly proven that currently accessible machine learning IDSs do not fulfil the standards for numerous reasons. The present research which aims to help network IDS designers, use Deep Learning techniques such as RNN, Deep-NN, and designing algorithms.

A. Deep learning algorithms

DL is a variant of ML that comprises a large number of omitted layers in order to simulate a deep network. These methods outperform ML in terms of throughput because of the depth of their structure and the ease with which they can self-learn and produce relevant features from a dataset. Deep Learning techniques like as RNN and Deep-NN & algorithm design are being used in the current study aimed at assisting network IDS designers.

B. Recurrent neural networks

To model sequence data, recurrent neural networks (RNNs) build on the standard feed-forward neural network's capabilities. RNNs are composed of input, hidden, & output units, where the hidden units are referred to as memory. This decision-making process relies on the current input & prior output for each RNN unit. Only a few of the uses of RNNs include speech processing, activity recognition, handwriting prediction, & semantic

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8
DOI: https://doi.org/10.17762/ijritcc.v11i8.7933
***Article Received**: 02 May 2023 **Revised**: 25 June 2023 **Accepted**: 26 July 2023*

comprehension. IDS categorization and feature extraction can be done using RNNs. Short-term memory is a problem for RNNs because they can only tolerate sequences of a certain length. Long-term memory (LSTM) & gated recurrent unit (GRU) variations of RNNs have been proposed to address these difficulties. For binary & multi-class classification of the NSL-KDD dataset, Yin et al. presented an RNN-based IDS. It was tested used a variety of hidden nodes & learning rates to see how well the model performed. The accuracy of the model is affected by the number of hidden nodes & learning rate. For binary and multiclass cases, the best accuracy was found with 80 hidden nodes with learning rates of 0.1 & 0.5. Reference 92's reduced-size RNN model fared well in comparison to the proposed model. As a result, the model training duration for the R2L & U2R classes is significantly increased, which has a negative impact on detection rates. There is no comparison of the proposed system to existing DL approaches in this paper.

C. Deep neural network

Multiple layers of learning are possible with the DNN structure, which is the foundation of deep neural networks (DL). In addition to the input and output layers, there are also a number of other layers that are not visible. DNN can be used to model complex, nonlinear functions. An increase in the model's hidden layers improves its performance. Jia et al. used a network IDS based on DNN with four hidden layers to classify the KDD cup'99 & NSL-KDD datasets. A single fully connected layer & softmax classifier in the output layer were used for classification. The hidden layer's activation function was a linear unit that had been corrected. Since there were fewer data for U2R attacks, the results demonstrated that the proposed model was reliable. Increased node and layer counts lead to a more complex structure, which takes longer to compute and consumes more resources, according to the authors of the paper. The optimization algorithm & automatic adjustment are the answer to these problems. Using the NSL-KDD dataset, Wang et al tested the DNN-based IDS against attackers. They did a thorough investigation of the roles played by various aspects in the generation of antagonistic examples. FGSM, JSMA, DeepFool, & CW attacks generated the adversarial samples. Due to their high vulnerability to DL-based IDS, the most frequently used characteristics on the network must be given special attention in order to keep the network safe from intrusions.

1.Experiment 1

We initially tested the classifier's performance on a training set that had been deflated using different deflation factors in our tests. K is a parameter scaling factor in the proposed DSSTE algorithm. The number of tough samples rises as K rises within a particular range, but as K rises beyond that range, the number of difficult samples remains constant indefinitely. The majority compression & minority augmentation, on the other hand, will rise with a change in K for challenging samples. This was done as a precautionary measure to guarantee that the data sample was relevant, didn't cause excessive noise, and the best sampling results may be achieved using our DSSTE approach. NSL-KDD & CSE-CIC-IDS2018 used different scaling factors K to handle training data. Based on average F1-Scores, six proposed classifiers were tested & their performance was rated.

NSL-KDD dataset findings show that LSTM attained the highest accuracy of 78 percent & highest F1-Score of 75 percent when training on the original training set. XGBoost & miniVGGNet had the highest recall rates and accuracy rates, respectively, after sampling the RUS algorithm's training. For example, After sampling from the ROS algorithm's training, LSTM had a recall rate of 75%. After sampling the training set with the SMOTE algorithm, AleNet achieved an accuracy rate of 82% or a recall rate of 82%. According to the DSSTE training set, AleNet had an accuracy & recall rate of 82% and 81%, respectively.[33]

In the CSE-CIC-IDS2018 dataset, random forest has the highest accuracy of 88 percent & highest F1-Score of 90 percent. Following the RUS, ROS, and SMOTE algorithms' sampling of the training set. The random forest was the best choice for accuracy & F1-Score. Due to the lack of improvement in performance, the advantages were insignificant or non-existent. By using DSSTE sampling strategy described in this research, MiniVGGNet has the best accuracy & recall out of all the models tested. As a result, random forest's accuracy and recall are likewise quite near to each other. [32] When used in conjunction with each sampling algorithm, random forest displays integrated learning's generalization potential while using less hardware resources. We calculated the classifier's average accuracy & F1-Score for each sampling technique. The sampling algorithms RUS, ROS, and SMOTE all perform better than the original approach on the NSL-KDD dataset. The improvement in prediction accuracy and F1-Score is minimal. DSSTE's accuracy & F1-Score have both risen by around 8% and 7%, respectively, since the original version of the method was proposed. When utilizing RUS, ROS, and SMOTE sampling algorithms in CSE-CIC-2018 dataset, performance gains are very small or even decreased. This paper's DSSTE algorithm sampling improves the average accuracy by 2% & average F1-Score by 1% after the training set.[26]

Prediction and recall rates are combined to generate the F1-Score, which is a useful measure of classification model performance. That's why when comparing alternative methods proposed by other authors, we use F1-Score and accuracy as measurements. On KDD Test C, our suggested data sampling method DSSTE outperforms previous methods. The F1-Score is extremely near to that of AESMOTE, which demonstrates the advantages of reinforcement learning for automatic paired sequence learning, however it takes a long time to develop a

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8
DOI: https://doi.org/10.17762/ijritcc.v11i8.7933
***Article Received**: 02 May 2023 **Revised**: 25 June 2023 **Accepted**: 26 July 2023*

model using reinforcement learning. Because of this, our suggested solution is more applicable to networks with imbalanced traffic.[27][28]

The CIC-IDS-2018 is a vast and redundant dataset, and the data are picked & processed inversely by different scholars. As a result, we did not make any comparisons to the CIC-IDS-2018 dataset with other researchers. We have found that the DSSTE approach is much better than other sampling algorithms in our tests. On the CIC-IDS-2018 dataset, DSSTECAlexNet performs admirably. Detection of Brute Force & Infiltration attacks has also improved, with detection rates approaching 100% in several cases.[29][30]

It's important to remember that, while typical sampling techniques help to balance out a training set, they don't provide a distribution that's exactly like real data. Data redundancy & overfitting can occur when the ROS algorithm is used instead of the RUS method. SMOTE interpolation, on the other hand, increases noise traffic & data overlap, increasing the difficulty of the training set.[31] Our suggested DSSTE algorithm is extremely focused on compressing & augmenting problematic data from a training set that is imbalanced. More data can be taken into account by the classifier, resulting in better classification results.

2.Propose 2

a) Step 1:

Collect the dataset, this dataset contains intrusion website information.

b)Step 2:

Performing EDA on the dataset and get to know that it can be done as binary classification and multi-class classification.

c)Step 3:

Processing

- Dropping Null values.
- Removing duplicate Values
- Changing To scalar values
- One Hot Encoding
- Changing Text labels to number
- Data Normalization
- Feature Extraction

d)Step 4:

Plotting graphs and done final processing on the data for the training.

e)Step 5:

Creating a Conv1D Deep Learning model and fitting the data to it, let it train. After completion, use the model for testing.

f)Step 6:

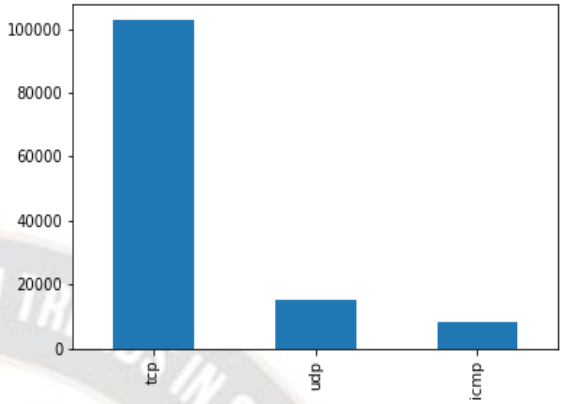
Evaluation of the model, testing the model on the test set and measuring the performance in terms of precision, recall & F1-Score. The Conv1D Deep learning model performed very well.

VII METHODOLOGY

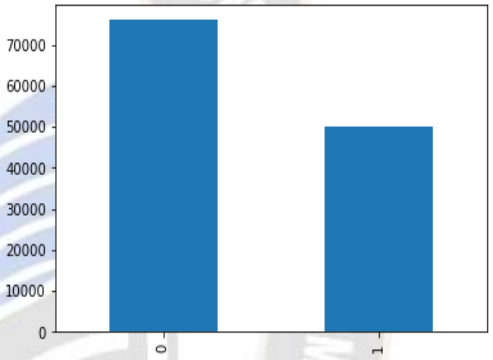
Steps used in coding

A. Pre-Processing

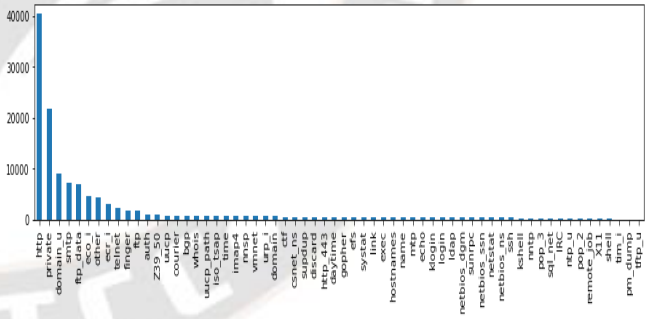
1) Bar Graph protocol type



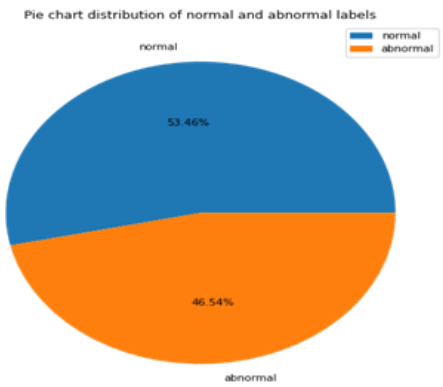
2) Log in Bar Graph



3) Every Sevrcie Graph

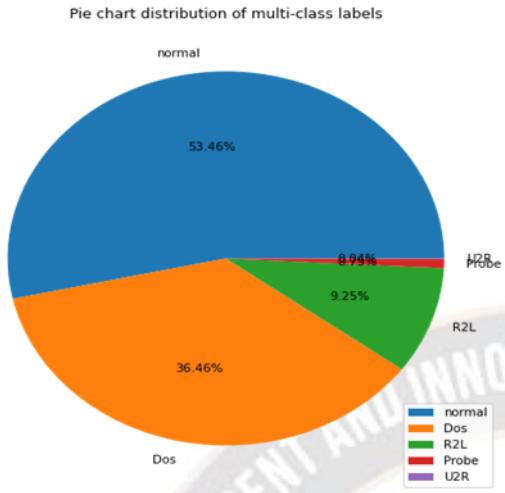


4) Pie Chart distribution of binary class

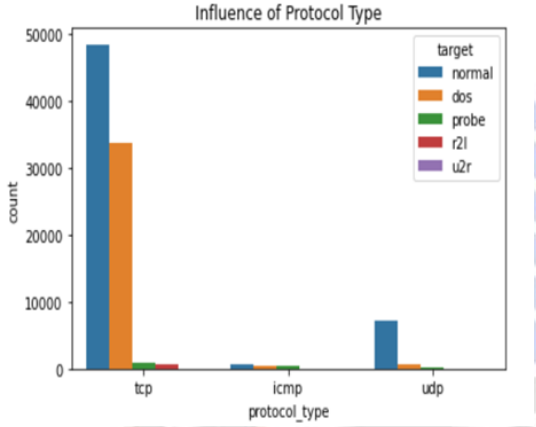


International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8
DOI: https://doi.org/10.17762/ijritcc.v11i8.7933
***Article Received**: 02 May 2023 **Revised**: 25 June 2023 **Accepted**: 26 July 2023*

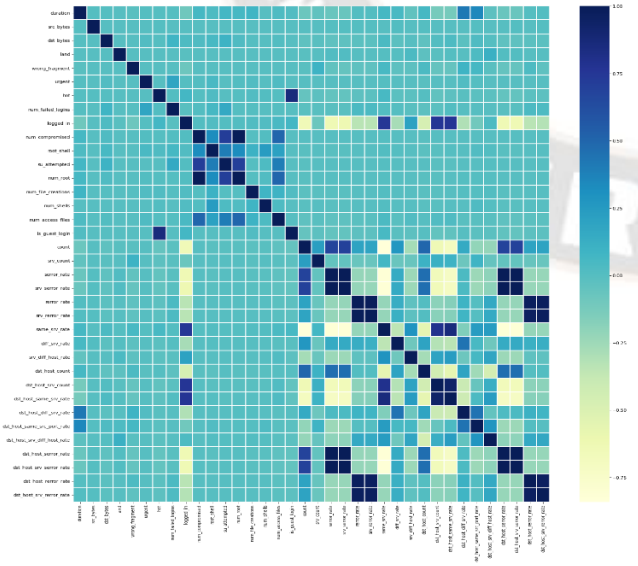
5) Pie Chart distribution of multi class



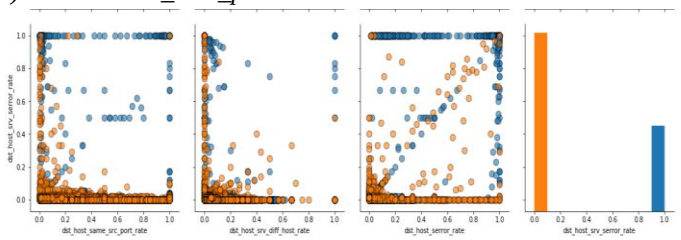
6) Protocol type influence on target



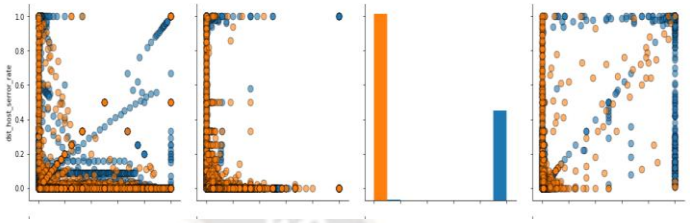
7) Correlation between whole data



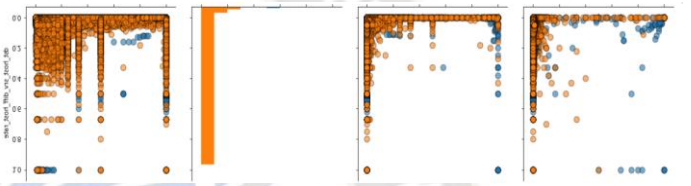
8) Dst_host_port



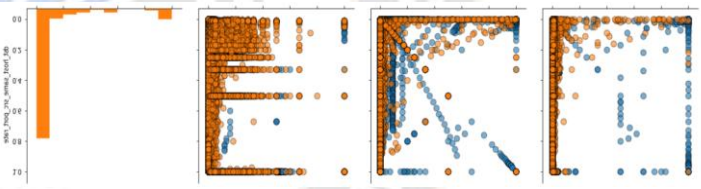
9) Dst_host_serror_rate



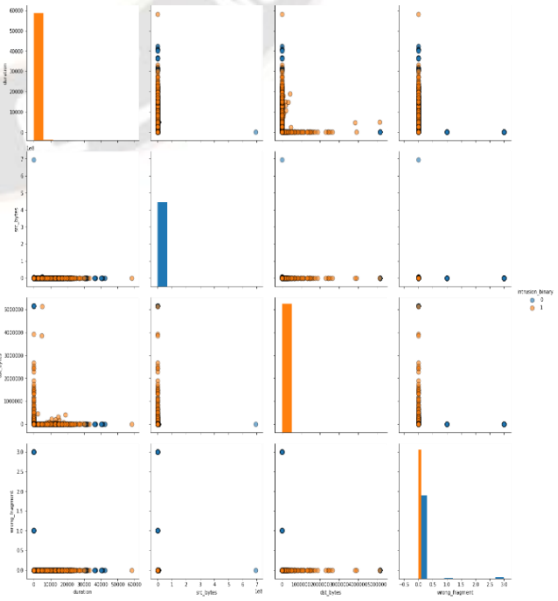
10) Dst_host_srv_diff_host_rate



11) Dst_host_same_src_port_rate



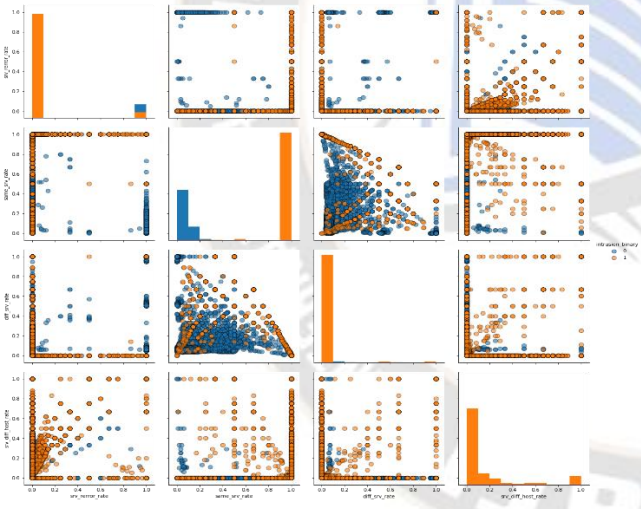
12) features=['duration','src_bytes', dst_bytes', 'wrong_fragment']



International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8
DOI: https://doi.org/10.17762/ijritcc.v11i8.7933
***Article Received**: 02 May 2023 **Revised**: 25 June 2023 **Accepted**: 26 July 2023*

13.features=['urgent','hot','num_failed_logins','num_compromised']

14) features=['srv_rerror_rate','same_srv_rate','diff_srv_rate ','srv diff_host_rate']



15) Pre-processing

a) Dropping Null values.
b) Removing duplicate Values
c) Changing To scalar values
d) One Hot Encoding
e) Changing Text labels to number
f) Data Normalization
g) Feature Extraction

16) Model Summary

a) Conv1d(32,3,padding=same,activation=relu)
b) MaxPool(pool_size=4)
c) Dense(16,activation=relu)
d) Dense(5,activation=softmax)
e) Loss = categorical_crossentropy
f) Optimizer = adam

```
Model: "sequential_6"
_________________________________________________________________
Layer (type)                 Output Shape              Param #
=================================================================
conv1d_4 (Conv1D)            (None, 93, 32)            128
_________________________________________________________________
max_pooling1d_2 (MaxPooling1 (None, 23, 32)            0
_________________________________________________________________
layer_normalization_2 (Layer (None, 23, 32)            64
_________________________________________________________________
flatten_2 (Flatten)          (None, 736)               0
_________________________________________________________________
dense_10 (Dense)             (None, 16)                11792
_________________________________________________________________
dropout_2 (Dropout)          (None, 16)                0
_________________________________________________________________
dense_11 (Dense)             (None, 5)                 85
=================================================================
Total params: 12,069
Trainable params: 12,069
Non-trainable params: 0
_________________________________________________________________
```

VIII EVALUATION METRICS

There are four metrics that may be used to assess the performance of the detection module, which is the primary purpose of this framework: accuracy, recall & preference. These metrics are commonly utilized to analyze the performance of IDS methods. The following are their formulas.[25]

Accuracy (Acc) is a measure of a model's overall performance based on the percentage of properly identified samples among all samples.

$$\mathrm{Acc} = \frac{\mathrm{TP} + \mathrm{TN}}{\mathrm{TP} + \mathrm{TN} + \mathrm{FP} + \mathrm{FN}}.$$

There are two ways to measure recall (Re) or detection rate (DR): the number of samples properly classified into a specific class & actual number of samples in that class.

$$\mathrm{Re} = \mathrm{DR} = \frac{\mathrm{TP}}{\mathrm{TP} + \mathrm{FN}}.$$

To calculate precision, divide the number of samples that were correctly classified into a category by the total number of samples that were classified into that group.

$$\mathrm{Pr} = \frac{\mathrm{TP}}{\mathrm{TP} + \mathrm{FP}}.$$

Precision & Recall are defined as the harmonic mean of the F1-score (F1) or F-measure (FM)

$$F1 = \mathrm{FM} = \frac{2 \cdot \mathrm{Pr} \cdot \mathrm{Re}}{\mathrm{Pr} + \mathrm{Re}}.$$

.

The TP value includes the number of samples categorized as a particular type, the number of samples correctly classified as that type (TN), the number of samples misclassified (FP), and the

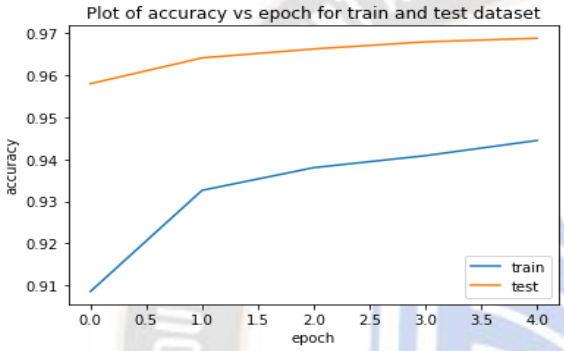
International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8
DOI: https://doi.org/10.17762/ijritcc.v11i8.7933
***Article Received**: 02 May 2023 **Revised**: 25 June 2023 **Accepted**: 26 July 2023*

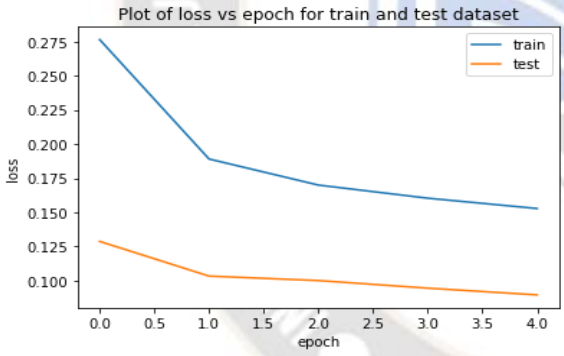
number of samples erroneously classified (FN) for each sample type.

A. *Evaluation metrics Comparison of the proposed framework*

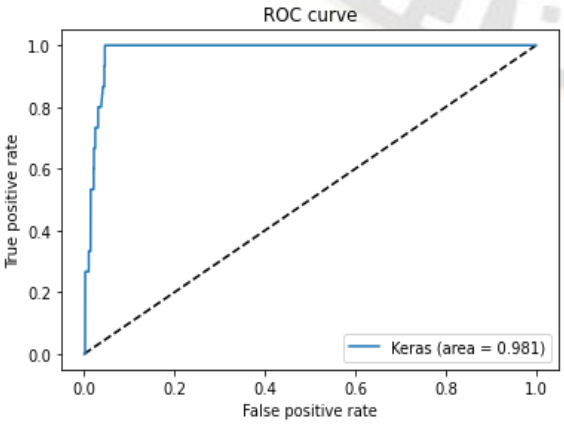
Model	Accuracy	Precision	Recall	F1-Score
Base	0.82	0.83	0.82	0.81
Base LSTM	0.78	0.78	0.78	0.75
Base XGBoost	0.77	0.81	0.77	0.73
Proposed 1	0.88	0.86	0.88	0.90
Proposed 2	0.96	0.96	0.98	0.97

B. *Accuracy, loss & Result Graph*

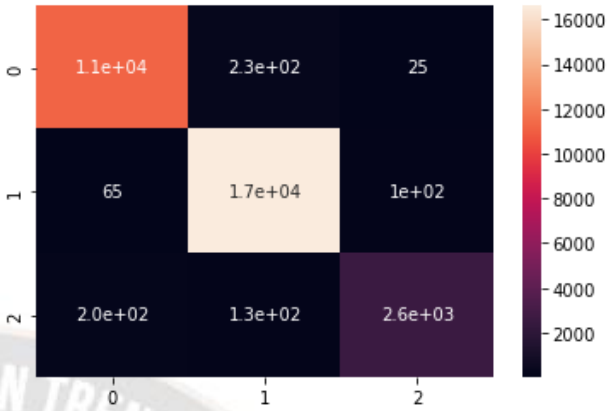




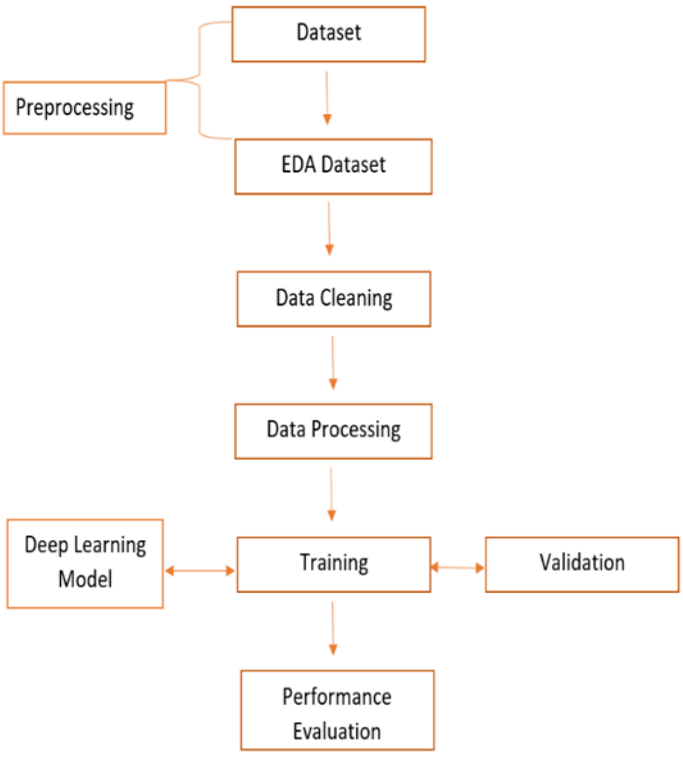
C. *ROC Curve:*



D. *Confusion Matrix*



IX FLOW CHART



X OBSERVATIONS & FUTURE SCOPE:

Observations

- Improved Detection Accuracy: Deep neural network (DNN) solutions for intrusion detection in networks have demonstrated superior detection accuracy compared to traditional methods. The ability of DNNs to learn complex patterns and relationships in network traffic data enables them to effectively identify both known and unknown intrusion attempts, reducing false positives and false negatives.
- Adaptability to Emerging Threats: DNN-based intrusion detection systems have shown promising results in detecting novel and evolving attack patterns.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8
DOI: https://doi.org/10.17762/ijritcc.v11i8.7933
***Article Received**: 02 May 2023 **Revised**: 25 June 2023 **Accepted**: 26 July 2023*

The models can generalize from learned patterns and adapt to new and previously unseen attacks, providing proactive defense against emerging threats. This adaptability is crucial in the ever-changing landscape of cybersecurity.

- Handling Large-Scale Data: DNNs can efficiently process and analyze large-scale network datasets, making them suitable for modern network environments characterized by high-volume and high-velocity data. The parallel processing capabilities and scalability of DNNs allow for real-time or near real-time detection and response to network intrusions.
- Addressing Zero-Day Attacks: Zero-day attacks, which exploit unknown vulnerabilities, pose a significant challenge for traditional intrusion detection systems. DNNs have shown promise in detecting and mitigating zero-day attacks due to their ability to learn and recognize anomalies without relying on predefined signatures or rules. This capability enhances the overall security posture of network environments.[22][23]

Future Scope:

- Enhancing Explainability: One area of future research is improving the interpretability and explainability of DNN-based intrusion detection systems. As DNNs are often considered black-box models, efforts can be made to develop techniques that provide insights into the decision-making process of the models, helping security analysts understand and trust the generated alerts and recommendations.[24]
- Adversarial Robustness: Adversarial attacks aim to deceive DNN models by introducing carefully crafted inputs. Future research can focus on enhancing the robustness of DNN-based intrusion detection systems against such attacks. Techniques like adversarial training and model regularization can be explored to ensure the models are resilient in the face of sophisticated adversaries.
- Hybrid Approaches: Combining the strengths of DNNs with other traditional methods such as rule-based systems or anomaly detection algorithms can be a promising avenue for future research. Hybrid approaches can leverage the complementary capabilities of different techniques to enhance the accuracy and effectiveness of intrusion detection systems, providing a more comprehensive defense against network intrusions.
- Real-Time Decision-Making: Although DNNs have shown potential for real-time intrusion detection, further research can focus on optimizing their architectures and algorithms to reduce latency and improve response times. This will enable more efficient and timely decision-making in dynamic network environments, where rapid detection and mitigation of intrusions are crucial.
- Privacy Preservation: As network intrusion detection involves analyzing sensitive network traffic data, preserving privacy is a significant concern. Future research can explore privacy-preserving techniques, such as secure multiparty computation or federated learning, to ensure that DNN models can effectively detect intrusions while preserving the privacy of network users.

In conclusion, the observations highlight the effectiveness of DNN solutions for detecting intrusions in networks. The future scope suggests areas of research and development to further enhance the capabilities, robustness, and practical applicability of DNN-based intrusion detection systems, ultimately strengthening network security in the face of evolving cyber threats.

XI CONCLUSION

An IDS classifier can be trained in two ways; one that learns as much as possible from labelled training examples, and one that learns from a training set of unlabeled data in order to uncover the structural information in that training set. Random Forest (RF), SVM, KNN, & artificial neural networks have been used by researchers to detect intrusions, among other techniques (ANN). The use of DNNs in intrusion detection has been a hot topic among researchers, & convolutional neural networks have drawn a lot of their interest. The burden on network intrusion detection is accumulative as network intrusion evolves. In particular, IDS are unable to forecast the distribution of malicious assaults because of the uneven network traffic. This makes cyberspace security a significant issue. A new DSSTE algorithm has been proposed in this paper, which improves the classification model's ability to learn from imbalanced network data.

DNN solutions for detecting intrusions in network environments have emerged as a powerful approach in the field of network security. Through the review of existing literature and observations, it is evident that DNN-based intrusion detection systems offer significant advantages over traditional methods.

The application of DNNs in intrusion detection has shown improved detection accuracy, surpassing the capabilities of rule-based systems and signature-based approaches. The ability of DNNs to learn complex patterns and relationships in network traffic data allows for the identification of both known and unknown intrusion attempts, leading to a reduction in false positives and false negatives.

Furthermore, DNNs exhibit adaptability to emerging threats, enabling them to detect novel and evolving attack patterns. By generalizing from learned patterns, DNN models can proactively

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8
DOI: https://doi.org/10.17762/ijritcc.v11i8.7933
***Article Received**: 02 May 2023 **Revised**: 25 June 2023 **Accepted**: 26 July 2023*

defend against emerging threats, enhancing the resilience of network environments. This adaptability is particularly crucial in the dynamic and ever-changing landscape of cybersecurity.

Another notable advantage of DNNs is their capability to handle large-scale network data. With their parallel processing capabilities and scalability, DNN-based intrusion detection systems can efficiently process and analyze high-volume and high-velocity network datasets. This enables real-time or near real-time detection and response, ensuring timely mitigation of network intrusions.

In addition, DNNs offer potential in addressing zero-day attacks, which exploit unknown vulnerabilities. Unlike traditional systems that rely on predefined signatures or rules, DNNs can learn and recognize anomalies without prior knowledge of specific attack patterns. This attribute enhances the overall security posture of network environments, providing defense against sophisticated and evolving threats.

Looking ahead, there are several avenues for future research and development in the field of DNN-based intrusion detection. These include improving explainability and interpretability of DNN models, enhancing adversarial robustness against attacks, exploring hybrid approaches combining different techniques, optimizing models for real-time decision-making, and addressing privacy preservation concerns.

DNN-based solutions offer a promising path towards more effective and efficient intrusion detection in network environments. By harnessing the power of deep learning, organizations and individuals can bolster their network security, detect intrusions with higher accuracy, and proactively defend against emerging cyber threats. With ongoing research and advancements, DNNs have the potential to revolutionize the field of network security and ensure the integrity and resilience of our interconnected digital systems.

REFERENCES

[1] S,Rajendra, Bandre and J. N. Nandimath. "Design consideration of Network Intrusion detection system using Hadoop and GPGPU." Pervasive Computing (ICPC), 2015 International Conference on. IEEE, 2015.

[2] CAI, Zeng-yu. "Development of intelligent intrusion detection based on biosimulation [J]." Journal of Zhengzhou University of Light Industry (Natural Science) 2 (2010): 018.

[3] Kaushik,(2023).Deep Learning Unveils Hidden Insights: Advancing Brain Tumor Diagnosis. International Journal for Global Academic & Scientific Research, 2(2), 01–22. https://doi.org/10.55938/ijgasr.v2i2.45

[4] Juszczyszyn, Krzysztof, et al. "Agent-based approach for distributed intrusion detection system design." International Conference on Computational Science. Springer, Berlin, Heidelberg, 2006.

[5] Kulariya, Manish, et al. "Performance analysis of network intrusion detection schemes using Apache Spark." Communication and Signal Processing (ICCSP), 2016 International Conference on. IEEE, 2016.

[6] Patcha, Animesh, and Jung-Min Park. "An overview of anomaly detection techniques: Existing solutions and latest technological trends." Computer networks 51.12 (2007): 3448-3470

[7] Kaushik, P. (2023). Congestion Articulation Control Using Machine Learning Technique. Amity Journal of Professional Practices, 3(01). https://doi.org/10.55054/ajpp.v3i01.631

[8] Devarakonda, Nagaraju, et al. "Intrusion detection system using bayesian network and hidden markov model." Procedia Technology 4 (2012): 506-514.

[9] Rathore, R. (2022). A Study on Application of Stochastic Queuing Models for Control of Congestion and Crowding. International Journal for Global Academic & Scientific Research, 1(1), 1–6. https://doi.org/10.55938/ijgasr.v1i1.6

[10] Benaicha, S. Eddine, et al. "Intrusion detection system using genetic algorithm." Science and Information Conference (SAI), 2014. IEEE, 2014.

[11] Singh Choudhary, S. ., Ghosh, S. K. ., Rajesh, A. ., Alfurhood, B. S. ., Limkar, S. ., & Gill, J. . (2023). BotNet Prediction in Social Media based on Feature Extraction with Classification using Machine Learning Algorithms. International Journal of Intelligent Systems and Applications in Engineering, 11(3s), 150 –. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/2553

[12] P.S.Rathore, S. (2023). Analysing the efficacy of training strategies in enhancing productivity and advancement in profession: theoretical analysis in Indian context. International Journal for Global Academic & Scientific Research, 2(2), 56–77. https://doi.org/10.55938/ijgasr.v2i2.49

[13] Dong, Shi, D.D. Zhou, and W. Ding. "The study of network traffic identification based on machine learning algorithm." Computational Intelligence and Communication Networks (CICN), 2012 Fourth International Conference on. IEEE, 2012.

[14] Rathore, R. (2022). A Review on Study of application of queueing models in Hospital sector. International Journal for Global Academic & Scientific Research, 1(2), 1–6. https://doi.org/10.55938/ijgasr.v1i2.11

[15] Shanmugavadivu, R., and N. Nagarajan. "Network intrusion detection system using fuzzy logic." Indian Journal of Computer Science and Engineering (IJCSE) 2.1 (2011): 101-111.

[16] Sharafaldin, Iman, A.H.Lashkari, and Ali A. Ghorbani. "Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization." ICISSP. 2018.

[17] P.S.Rathore, S. (2023). The Impact of AI on Recruitment and Selection Processes: Analysing the role of AI in automating and enhancing recruitment and selection procedures. International Journal for Global Academic & Scientific Research, 2(2), 78–93. https://doi.org/10.55938/ijgasr.v2i2.50

[18] Analysing the efficacy of training strategies in enhancing productivity and advancement in profession: theoretical analysis in Indian context. International Journal for Global Academic & Scientific Research, 2(2), 56–77. https://doi.org/10.55938/ijgasr.v2i2.49

[19] Singh, A.Pal, and M. D.Singh. "Analysis of host-based and network-based intrusion detection system." International Journal

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8
DOI: https://doi.org/10.17762/ijritcc.v11i8.7933
***Article Received**: 02 May 2023 **Revised**: 25 June 2023 **Accepted**: 26 July 2023*

of Computer Network and Information Security 6.8 (2014): 41-47.

[20] Kaushik, P (2022). Role and Application of Artificial Intelligence in Business Analytics: A Critical Evaluation. International Journal for Global Academic & Scientific Research, 1(3), 01–11. https://doi.org/10.55938/ijgasr.v1i3.15

[21] Sung, H.Andrew, and S.Mukkamala. "Identifying important features for intrusion detection using support vector machines and neural networks." Applications and the Internet, 2003. Proceedings. 2003 Symposium on. IEEE, 2003.

[22] Takkellapati, V.Suneetha, and G. V. S. N. R. V. Prasad. "Network intrusion detection system based on feature selection and triangle area support vector machine." International Journal of Engineering Trends and Technology3.4 (2012).

[23] Rathore, R. (2023). A Study Of Bed Occupancy Management In The Healthcare System Using The M/M/C Queue And Probability. International Journal for Global Academic & Scientific Research, 2(1), 01–09. https://doi.org/10.55938/ijgasr.v2i1.36

[24] Ragsdale, J. Daniel , et al. "Adaptation techniques for intrusion detection and intrusion response systems." Systems, Man, and Cybernetics, 2000 IEEE International Conference on. Vol. 4. IEEE, 2000.

[25] Harsh, S. ., Singh , D., & Pathak , S. (2021). Efficient and Cost-effective Drone – NDVI system for Precision Farming. International Journal of New Practices in Management and Engineering, 10(04), 14–19. https://doi.org/10.17762/ijnpme.v10i04.126

[26] Shanmugam, Bharanidharan, and N.BashahIdris. "Improved intrusion detection system using fuzzy logic for detecting anomaly and misuse type of attacks." Soft Computing and Pattern Recognition, 2009. SOCPAR'09. International Conference of. IEEE, 2009.

[27] Singh, Shubhangi, and R.S.Kushwah. "A Study on Intrusion Detection in Wireless Networks by Using Genetic Algorithm Applications." Computational Intelligence and Communication Networks (CICN), 2014 International Conference on. IEEE, 2014.

[28] Kaushik, P. (2023). Artificial Intelligence Accelerated Transformation in The Healthcare Industry. Amity Journal of Professional Practices, 3(01). https://doi.org/10.55054/ajpp.v3i01.630

[29] " Upasani, Nilam, and HariOm. "Evolving fuzzy min-max neural network for outlier detection." Procedia computer science 45 (2015): 753-761.

[30] Wu, Zheng, et al. "Automated intrusion response decision based on the analytic hierarchy process." Knowledge Acquisition and Modeling Workshop, 2008. KAM Workshop 2008. IEEE International Symposium on. IEEE, 2008.

[31] Kaushik, P. (2023). Unleashing the Power of Multi-Agent Deep Learning: Cyber-Attack Detection in IoT. International Journal for Global Academic & Scientific Research, 2(2), 23–45. https://doi.org/10.55938/ijgasr.v2i2.46

[32] Xiang, Junlong, et al. "Using extreme learning machine for intrusion detection in a big data environment." Proceedings of the 2014 Workshop on Artificial Intelligent and Security Workshop. ACM, 2014.

[33] Xiaodong, W., et al. "Development of a snort-based security network management and real-time intrusion detection system." Journal-Beijing Normal University Natural Science Edition 40.1 (2004): 40-43.

[34] Zhang, Yongguang, Wenke Lee, and Yi-An Huang. "Intrusion detection techniques for mobile wireless networks." Wireless Networks 9.5 (2003): 545-556.

[35] Zikopoulos, Paul, and Chris Eaton. Understanding big data: Analytics for enterprise class hadoop and streaming data. McGraw-Hill Osborne M.