University of Ibadan
Journal of Science and Logics in ICT Research

Deep Learning Algorithms for Multiple Cyberattacks Detection

[1]✉ Nureni A. Azeez, [2]Emman-Ugheoke Osatsoghena and [3]Joy Nneka Ojuro.

[1,2]Department of Computer Sciences, Faculty of Science, University of Lagos.
[3]University of louisiana Lafayette, USA
[1]nurayhn1@gmail.com; [2]osaoshione@gmail.com. [3]Ojurojoy@gmail.com

Abstract

Data is pervasive and accessible through the internet. The proliferation of smart devices worldwide, such as computers and mobile phones, has led to a significant increase in internet usage. Consequently, this surge has also given rise to a corresponding increase in cyberattacks, which are a prevalent issue faced by internet users. To address this problem, it is crucial to have an effective cyberattack detection mechanism in place to safeguard computer networks, systems, and data. While intrusion detection systems (IDS) play a significant role in this regard, they do have their limitations. Therefore, in this research, two deep learning algorithms, namely Multilayer Perceptrons (MLPs) and Recurrent Neural Networks (RNN), have been proposed. The NSL-KDD and CIC-IDS-2017 datasets were utilized for this project. When using the NSL-KDD dataset, the MLP algorithm achieved an accuracy of 99.44% with a false positive rate of 0.52%, whereas the RNN algorithm achieved an accuracy of 98.02% with a false positive rate of 2.21%. On the other hand, when employing the CIC-IDS-2017 dataset, the MLP algorithm achieved an accuracy of 99.98% with a false positive rate of 2.06%, while the RNN algorithm achieved an accuracy of 99.09% with a false positive rate of 39.65%. Furthermore, various metrics such as precision, recall, F1-score, error rate, and others were calculated and compared for both models. The obtained results clearly indicate that the MLP algorithm outperformed the RNN algorithm in terms of performance when applied to both datasets.

Keywords: *cyber-attacks, deep-learning, detection, intrusion, comparison*

1. INTRODUCTION

According to the International Telecommunication Union (ITU), as of 2021 there were approximately 4.9 billion people who were using the internet which is about 65% of the world's population [15]. There is a strong relationship between the use of computers and the use of the internet because the internet is often accessed through computers. The internet has become a vital aspect of life and computers are the most common tool used to access the internet. Therefore as the use of computers increase so does the use of the internet and vice versa.

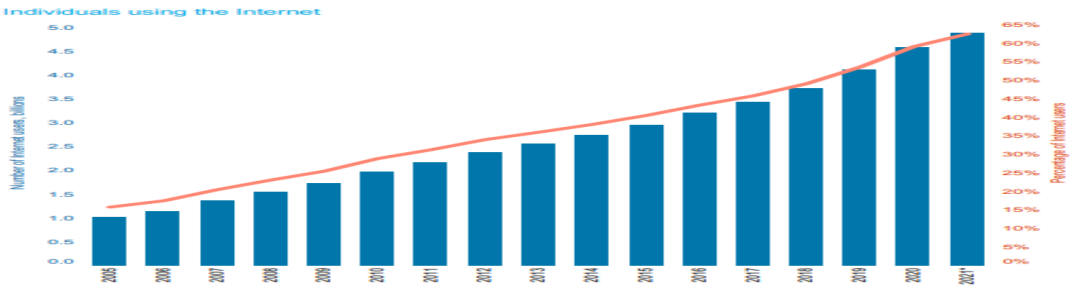


Figure 1:The use of the internet from 2005 to 2021 [15]

Internet is used for almost everything and in almost every industry or sector in this 21st century. It could be used for projects, research,

Nureni A. Azeez, Emman-Ugheoke Osatsoghena and Joy Nneka Ojuro (2024). Deep Learning Algorithms for Multiple Cyberattacks Detection. *University of Ibadan Journal of Science and Logics in ICT Research (UIJSLICTR)*, Vol. 11 No. 2, pp. 71 - 84

communications, social media, applications, transfer of money, ordering of food, sharing pictures with loved ones, organizations, etc. The uses of the internet is endless and the use increases daily. One can say, the internet is a way of life. The internet cuts across all sectors/industries in life [16]. A lot of data are stored in the internet both confidential and non-confidential information. Almost all companies/sectors have information that shouldn't be available to the general public. For example, the salaries of different employees or the information of clients or the diagnosis of patients in the hospital. Let's come down to the school setting, majority of students won't be happy if their CGPA or grades were available to the general public or lecturer's salaries known by all. Once the security is breached, a lot of things and activities are affected. This is just a few of the possible disasters that can occur when a system is not secured. When a system is attacked, it could lead to breach of confidentiality, availability and integrity. It could also lead to theft of service and denial of service (DOS) [24] and this are serious issues that we need to prevent. As the use of the internet increases, so does cyberattack [20].

Cyberattack is the attack over the internet. It is a malicious attempt to gain unauthorized access to computer systems, networks and data. i.e. it is an attempt to breach security over the internet. It can even lead to damage in some cases [27]. Cyberattack is one of the most common issues faced while using the internet. Since more than half of the population uses the internet, then the issue is one that cannot be ignored. As new ways or type of cyberattack emerges daily, the need of cyberattack detection is very vital.

Cyberattack detection can be defined as the process of identifying threats and responding to threats that are targeted towards computer networks, systems and data. It is very essential for safeguarding networks, systems and data from malicious activities [18].

As the use of the internet increases daily, the network traffic increases, so does the complexity and diversity of the cyberattacks. The Intrusion Detection System (IDS) may struggle to accurately and efficiently identify complex and varied network attacks, particularly those that occur infrequently [21]. Against this backing, finding a solution to this seemingly challenge is highly essential. There is need for a faster and more accurate way of identifying and detecting sophisticated attacks to solve the problem, therefore, more advanced Deep learning algorithms like MLPs and RNN are used to solve the problem.

2. RELATED WORKS

A framework called DFEL was used to detect internet intrusions in IoT environments. It addresses security challenges and improves classifier accuracy while reducing detection time. However, it requires a large amount of training data and has complex models [38].

The authors emphasized the need to identify cybercrime culprits and understand their tactics for effective prediction and prevention. They proposed using machine learning models to analyze cybercrimes and predict the impact of features on detecting attack methods and perpetrators. Their study found that the Support Vector Machine Linear model achieved 95.02% accuracy in detecting attack methods, while Logistic Regression achieved 65.42% accuracy in identifying attackers. However, the solution is limited in identifying attackers, doesn't consider an increase in perpetrators, and may not perform well with noisy data. It performs better with clean and well-separated data [6].

An efficient deep-learning-based system called IoT-IDCS-CNN was developed to detect and classify cyber-attacks in IoT communication networks. It utilized convolutional neural networks and consisted of three sub-systems for feature engineering, feature learning, and traffic classification. The system outperformed other machine-learning-based systems in terms of effectiveness. However, it requires a significant amount of labeled data for training, which can be challenging to acquire and hinders practical implementation. Additionally, the system is computationally intensive and may require expensive computing resources [2].

A proposed architecture for intrusion detection and classification in IoT networks using non-traditional machine learning methods addresses the growing number of attacks on

IoT systems. The architecture is efficient and flexible, adaptable to various IoT cyber-attack datasets. It comprises feature engineering, feature learning, and detection and classification subsystems, utilizing deep learning models to accurately detect subtle variations in attacks within IoT networks. However, a drawback is the difficulty in handling complex and high-dimensional data [1].

The proliferation of IoT devices has raised security concerns for big companies and smart towns. To automatically detect suspicious activities on these devices, a framework utilizing classification-based methods (SVM, GBDT, RF) was proposed. The RF algorithm achieved the highest accuracy (85.34%) when tested on the NSL KDD dataset. However, a major limitation is the resource and time-intensive training required for the models [4].

The authors explored the use of deep reinforcement learning, specifically the deep Q-learning algorithm, for detecting and preventing cyberattacks. While these methods show promise in real-time network intrusion detection, they have limitations due to evolving attack scenarios and the need for abundant training data. To overcome these challenges, the authors propose DAEQ-N, which combines a deep auto-encoder and a Q-network. This approach continuously learns from behavior patterns for improved accuracy. However, the requirement for large amounts of data remains a potential limitation, particularly in scenarios with limited data availability [19].

The research proposes using deep learning (DL) to enhance cybersecurity in the social Internet of Things (IoT). Comparing DL to traditional machine learning, the study finds that DL performs better in attack detection. Additionally, distributed attack detection systems utilizing DL outperform centralized systems. However, a drawback is the need for large amounts of labeled training data, which can be challenging to obtain in real-world environments [13].

The authors developed a new approach using deep reinforcement learning to detect phishing websites by analyzing harmful URLs. This method adapts to changing phishing behavior and learns the key characteristics for detection. However, a major drawback is the need for a significant amount of labeled data, which is often difficult to obtain specifically for phishing websites [9].

The research focused on identifying and mitigating vulnerabilities in cloud computing platforms. Machine learning techniques, including CNN, Logistic Regression, and SVM, were used to detect specific cyber attacks such as XSS, SQLI, and phishing. The CNN approach achieved 98.59% accuracy in detecting XSS attacks, Logistic Regression had 92.85% accuracy for SQLI, and SVM achieved 85.62% accuracy for phishing detection. Other methods like Decision Tree Classifier, Bayesian Network, and K-Nearest Neighbors also showed high accuracies for intrusion detection. However, a significant amount of labeled data is required for training, and overfitting is a potential concern [5].

The study explores the use of deep neural networks (DNNs) for developing an intrusion detection system capable of timely and automated detection of cyberattacks. DNNs outperform classical machine learning classifiers in detecting and classifying attacks at both network and host levels. The proposed scale-hybrid-IDS-AlertNet, a hybrid DNN framework, effectively monitors network traffic and host-level events for proactive detection. However, a limitation is that DNNs can overfit when trained on small datasets, leading to poor performance [36].

The study introduced a framework for detecting phishing websites using a deep learning approach called multilayer perceptron (MLP). This was particularly relevant during the COVID-19 pandemic when remote work increased the risk of cybercrime. While existing tools exist, attackers continually find new ways to exploit vulnerabilities. The proposed model achieved high training and test accuracies of 95% and 93%, respectively, using a dataset of 10,000 webpages. However, the MLP method has a high computational cost and is prone to overfitting [29].

The study proposes an intrusion detection system approach using machine learning models to detect anomalies in network traffic data. The LSTM model demonstrates exceptional performance in detecting

sequential patterns, achieving a high accuracy of 99.94% and an f1-score of 91.66% on the CIDDS-001 dataset. However, the approach is computationally intensive. This research addresses the growing concern of cyberattacks on sensitive data shared over networks [23].

The study investigates the use of a Multilayer Perceptron (MLP) neural network algorithm for network intrusion detection in cybersecurity. It demonstrates the algorithm's efficiency on low-power minicomputers, achieving a high scan rate of over 226,000 packets per second and an accuracy of over 99% while consuming only 5W of power. However, a significant amount of labeled data is required for training. This research emphasizes the potential of MLP in securing interconnected microprocessors in household devices [10].

The study focuses on the vulnerability of Industrial Internet of Things (IIoT) systems to cyberattacks and proposes a method for detecting these attacks using HDRaNN approach. The HDRaNN combines a deep random neural network and a multilayer perceptron with dropout regularization. Testing on IIoT security datasets demonstrates high accuracy, reaching 98% and 99% respectively, outperforming other attack detection algorithms. However, a drawback is the need for a large amount of labeled data for training, and the method can be computationally expensive [14].

The study investigates the use of Multilayer Perceptron (MLP) for intrusion detection using the KDD dataset. It shows that the algorithm effectively reduces errors during training and achieves high classification accuracy by adjusting the configuration of hidden layers and neurons. The proposed system achieves an impressive accuracy rate of 99.99% and a false positive rate of about 10% after applying output bias. However, limitations include the need for a large amount of labeled data for training and the tendency to overfit. This research demonstrates the potential of MLP in intrusion detection [26].

The article addresses the challenges faced by the manufacturing industry with IoT and CPS technologies, highlighting the need for effective defense techniques against cyberattacks. The authors propose a cyberattack detection method using Simple RNN and LSTM architectures. The method successfully detects all considered attacks without false positives when tested with real-world data. However, implementing the method may require substantial computational resources. Overall, the study offers valuable insights into improving cybersecurity in the manufacturing industry [23].

The study emphasizes the need for effective cyber-attack detection and proposes the use of Generative Adversarial Networks (GANs) as a solution. GANs can generate virtual data to address challenges related to imbalanced data in traditional techniques like Machine Learning and Deep Learning. However, implementing GANs requires substantial computational resources and can be challenging to train and fine-tune. The study provides valuable insights into overcoming the limitations of existing detection methods [32].

The study explores the use of Artificial Neural Networks (ANN) for detecting malicious users accessing high-security servers. Different ANN models, including Shallow Neural Network (SNN), Deep Neural Network (DNN), and Auto Encoder, were compared using the CICIDS2017 dataset. These models achieved an impressive accuracy rate of 98.45% in accurately classifying server connection requests as normal or malicious. However, the approach requires a significant amount of labeled data and may be susceptible to overfitting [34].

3. METHODOLOGY

Algorithms, Datasets, Architecture and Requirement analysis are the proposed methodology for the project.

3.1 Multilayer Perceptrons (MLPs)

Multilayer perceptrons are a type of artificial neural network that can be used for cyberattack detection. An MLP consists of multiple layers of interconnected "neurons," which process and transmit information. The input layer receives the data, and each subsequent layer processes the data and passes it on to the next layer until it reaches the output layer, which produces a result based on the input data.

To train an MLP for cyberattack detection, the network is typically fed a large dataset of labelled network traffic examples, where each example is labelled as either normal or abnormal (e.g., an attack). The MLP then uses this labelled dataset to learn the characteristics of normal and abnormal traffic. Once trained, the MLP can be used to classify new, unseen network traffic as normal or abnormal.
Generally, an MLP for cyberattack detection will have:

- The input layer would typically accept a set of features extracted from network traffic, such as packet size, destination IP address, protocol, etc.
- The hidden layers would use a set of weights and biases to transform the input data. The number of hidden layers can vary depending on the complexity of the task and the amount of data available. Each hidden layer typically consists of several artificial neurons.
- The output layer would produce a binary value (e.g. 1 for attack, 0 for normal) or a probability value between 0 and 1 indicating the likelihood of the input data being an attack [28].

The mathematical formula for using a Multi-Layer Perceptron (MLP) in cyberattack detection would involve using the model to compute a set of outputs, y, from a set of input features, x, using the following general form:

$$y = f(W\_n * f(W\_\{n-1\} * \ldots f(W\_2 * f(W\_1 * x + b\_1) + b\_2) \ldots) + b\_n)$$

------- *1*

Where W_1, W_2, ..., W_n are the weight matrices for each layer of the MLP,

b_1, b_2, ..., b_n are the bias vectors for each layer,

And f is the activation function [12].

The activation function f could be a sigmoid, ReLU, or other common activation function used in neural networks.
The final output is typically a probability value between 0 and 1 for each class. The class with the highest probability is chosen as the output.
The training process of the MLP would involve adjusting the weights and biases to minimize the error between the predicted outputs and the true labels of the training data. This is typically done using an optimization algorithm such as gradient descent.

3.2 Recurrent Neural Network (RNNs)

Recurrent Neural Networks (RNNs) are a type of neural network that are particularly well suited for processing sequential data, such as time series data. In the context of cyberattack detection, RNNs can be used to analyze log files or network traffic data in order to identify patterns that may indicate the presence of an attack. RNNs can also be used to learn from labelled examples of attacks in order to improve their ability to detect future attacks.

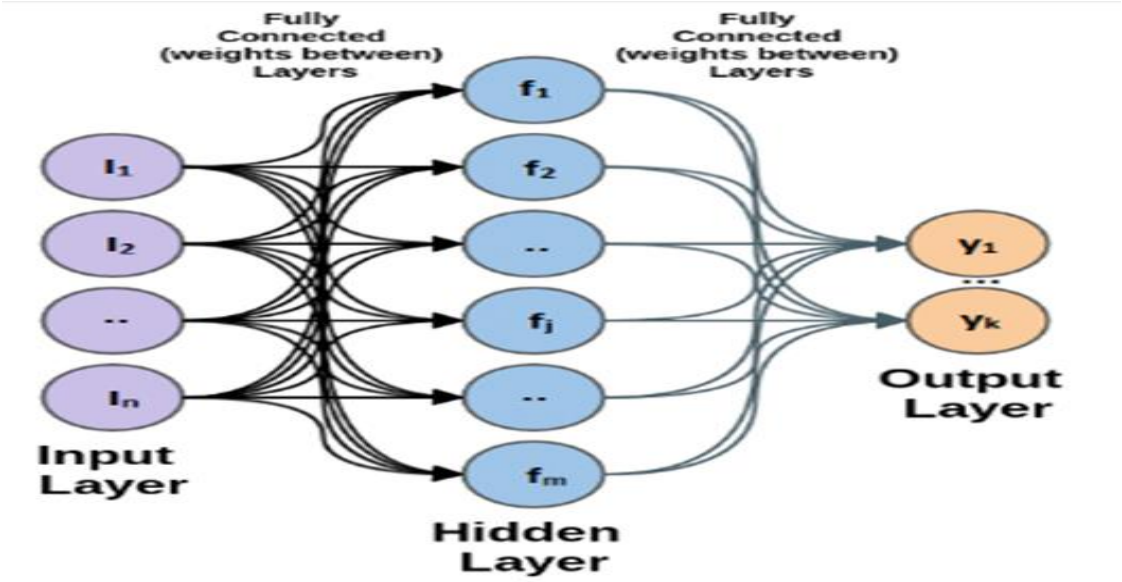


Figure 2: Multilayer Perceptron Architecture [26]

One of the key features of RNNs is that they have "memory," meaning that they can use information from previous time steps to inform their processing at the current time step. This allows them to effectively process data with temporal dependencies, such as the words in a sentence or the frames in a video.Recurrent Neural Networks (RNN) are more frequently used in cyberattack detection due to their capability to deal with high dimensional and temporal data. Unlike traditional neural networks, which are designed to process fixed-sized inputs and produce fixed-sized outputs, RNNs have the ability to process input of any length and to maintain a state that can be passed from one input to the next. This allows them to capture dependencies between input elements and to process sequences of data in a meaningful way.

A typical RNN for cyberattack detection would have an input layer, one or more recurrent layers (such as LSTM or GRU layers), and an output layer. The input layer takes in a sequence of data, such as network traffic or log data. The recurrent layers process the input sequence and maintain a hidden state that captures information about the previous input. This allows the RNN to learn temporal dependencies in the data. The output layer produces a prediction or classification of the input sequence, indicating whether it represents normal or attack traffic [28].

Mathematically, an RNN can be represented as a dynamic system of equations that update the state of the network based on the current input and the previous state. One of the most common mathematical representation of an RNN is th following:

$h\_t = f(W\_hh\_t - 1 + W\_xx\_t + b)$-------- *2*

$y\_t = g(W\_y * h\_t + b\_y)$ ---------- *3*

Where:

h_t is the hidden state at time step t, it captures the information from the previous inputs.

x_t is the input at time step t.

W_h, W_x, W_y are the weight matrices for the hidden state, input and output respectively.

b, b_y are the bias terms.

f(.) and g(.) are the non-linear activation functions such as sigmoid, tanh or ReLU [8].

The above equation describes how the hidden state of the network is updated at each time step, based on the current input and the previous hidden state. The output of the network is then computed by applying a second function g(.) to the hidden state.

In cyberattack detection, the input to the RNN can be a sequence of network traffic or log data, and the output can be a binary label indicating whether the input sequence is normal or an attack. During the training phase, the RNN is fed with the input X and its corresponding label Y, and the weights and biases are adjusted to minimize the difference between the predicted label and the true label.

3.3 Datasets

3.3.1 NSL-KDD dataset

The NSL-KDD dataset is a commonly used benchmark for intrusion detection in the field of network security. It is an improved version of the KDD Cup 99 dataset and addresses the issue of record redundancy. It is widely used as a benchmark dataset to compare different cyberattack detection methods. The dataset includes a training set (KDDTrain+) and two test sets (KDDTest+ and KDDTest-21), with the latter being more challenging to classify due to the presence of unknown attack types. It includes five categories of network traffic data: normal, denial of service (DoS), probe, user to root (U2R), and remote to local (R2L) with different number and percentage of records for each category. Each record in the dataset includes 41 features and a corresponding classification label, which are divided into four parts: basic,

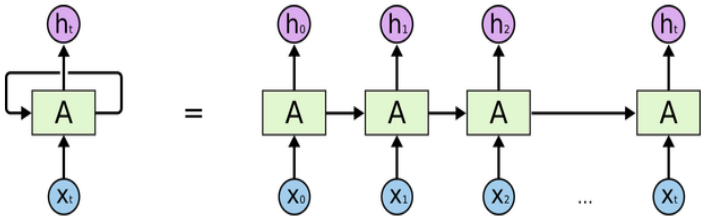


Figure 3: Basic Architecture of Recurrent Neural Networks [21]

content, time-based network traffic statistics, and host-based network traffic statistics [37].

3.3.2 CIC-IDS-2017

CIC-IDS-2017 is a publicly available dataset for intrusion detection in industrial control systems (ICS). It was created by the Canadian Institute for Cybersecurity (CIC) and contains network traffic data captured from various ICS environments. The dataset includes a wide range of attack types, including data exfiltration, reconnaissance, and control-layer attacks. The dataset contains the following types of network traffic: normal, benign and malicious, which includes different types of attacks such as Brute Force, DDoS, DoS, Infiltration, Botnet and Web Attack. The dataset consists of two parts: the training set, containing about 2.5 million flows, and the test set, containing about 0.5 million flows. Each flow in the dataset contains 81 features, which are a combination of both basic and advanced features. This dataset can be used to evaluate and compare different machine learning models for intrusion detection in ICS environments [33].

Table 1: Sources of Dataset

Dataset	Name	URL	Source
Dataset 1	**NSL-KDD**	**https://www.kaggle.com/datasets/hassan06/nslkdd**	**Kaggle**
Dataset 2	**CIC-IDS-2017**	**https://www.kaggle.com/datasets/cicdataset/cicids2017**	**Kaggle**

3.4 Architecture

The three deep learning algorithms used in this project have similar steps for cyberattack detection. The steps are:

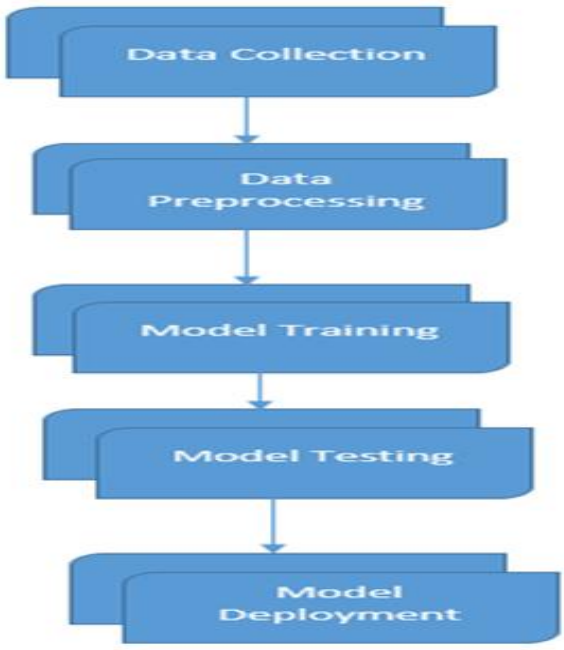


Figure 4: Steps for training the model for cyberattack detection

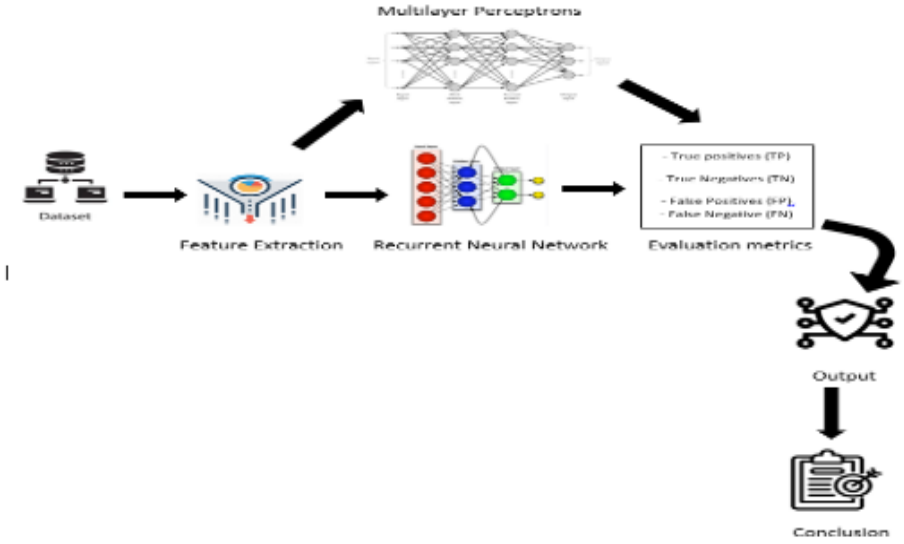


Figure 5: Proposed architecture for multiple cyber-attack detection [13]

The proposed architecture for multiple cyber-attack detection is illustrated in Figure 5. The process begins by obtaining the datasets, followed by performing feature extraction to extract the relevant features. Subsequently, the models are trained using each dataset. Their performances are then evaluated using various evaluation metrics, including accuracy, precision, recall, and others. The results obtained from this evaluation process are presented, and conclusions are drawn based on the findings.

4. RESULTS AND DISCUSSION

4.1 Results

NSL-KDD and CIC-IDS-2017 were the two datasets used in this project. They were both obtained from Kaggle. The NSL-KDD training dataset contains 125,972 rows and 42 columns while CIC-IDS-2017 training dataset contains 225,711 rows and 79 columns. The datasets were split into features and labels. NSL-KDD had two labels namely Normal and anomaly while CIC-IDS-2017 has benign and DDOS.

The categorical features in the dataset were encoded into numerical values using LabelEncoder from scikit-learn.

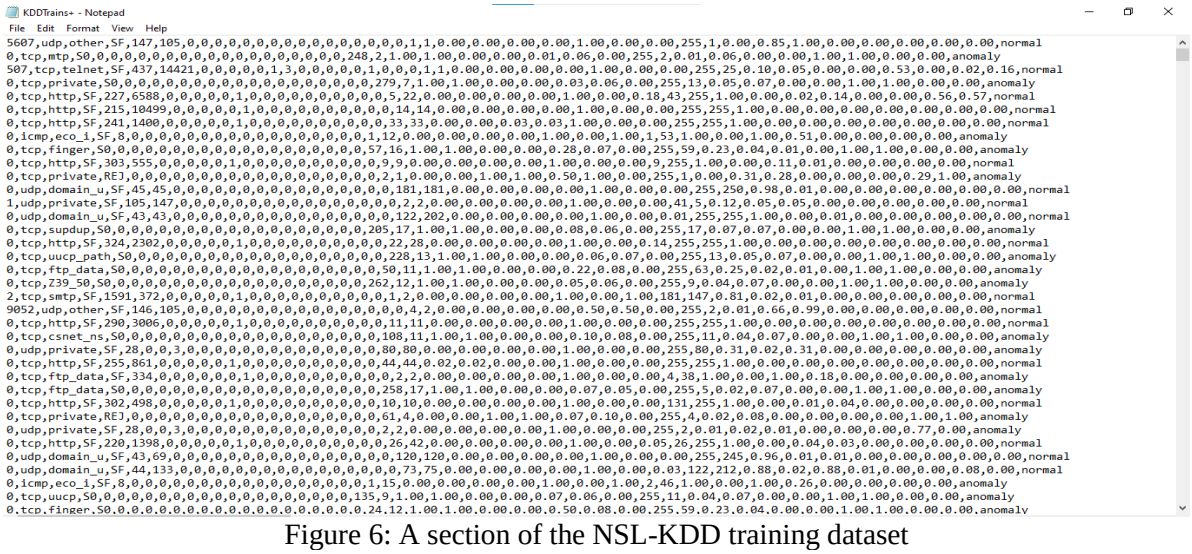
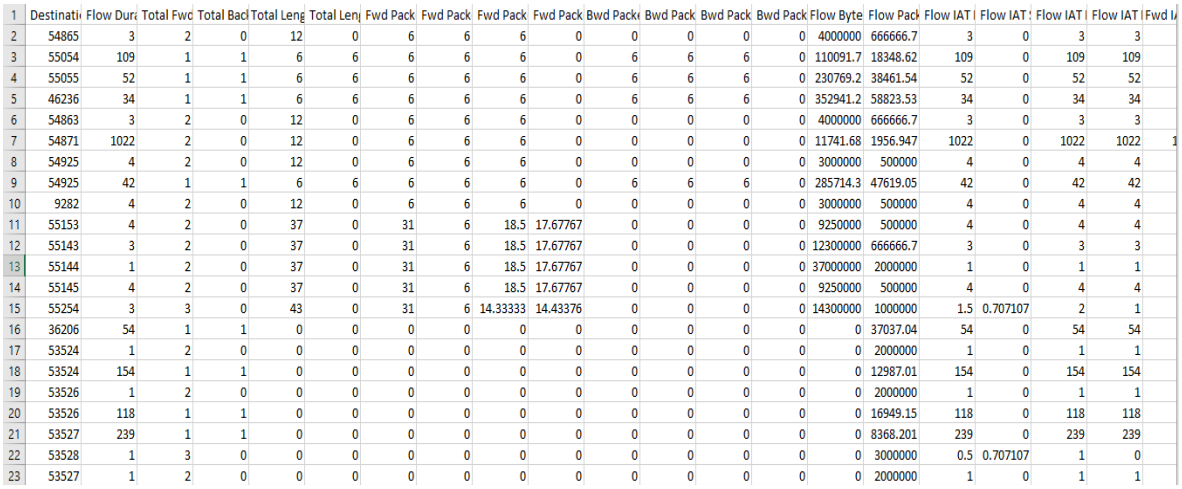


Figure 6: A section of the NSL-KDD training dataset

Figure 6 depicts a portion of the NSL-KDD training dataset in its raw and unprocessed state, prior to undergoing any cleaning or feature extraction procedures.



	Destinati	Flow Dur	Total Fwd	Total Bacl	Total Leng	Total Len	Fwd Pack	Fwd Pack	Fwd Pack	Fwd Pack	Bwd Pack	Bwd Pack	Bwd Pack	Bwd Pack	Flow Byte	Flow Pack	Flow IAT	Flow IAT	Flow IAT	Flow IAT	Fwd I
2	54865	3	2	0	12	0	6	6	6	0	0	0	0	0	4000000	666666.7	3	0	3	3	
3	55054	109	1	1	6	6	6	6	6	0	6	6	6	0	110091.7	18348.62	109	0	109	109	
4	55055	52	1	1	6	6	6	6	6	0	6	6	6	0	230769.2	38461.54	52	0	52	52	
5	46236	34	1	1	6	6	6	6	6	0	6	6	6	0	352941.2	58823.53	34	0	34	34	
6	54863	3	2	0	12	0	6	6	6	0	0	0	0	0	4000000	666666.7	3	0	3	3	
7	54871	1022	2	0	12	0	6	6	6	0	0	0	0	0	11741.68	1956.947	1022	0	1022	1022	1
8	54925	4	2	0	12	0	6	6	6	0	0	0	0	0	3000000	500000	4	0	4	4	
9	54925	42	1	1	6	6	6	6	6	0	6	6	6	0	285714.3	47619.05	42	0	42	42	
10	9282	4	2	0	12	0	6	6	6	0	0	0	0	0	3000000	500000	4	0	4	4	
11	55153	4	2	0	37	0	31	6	18.5	17.67767	0	0	0	0	9250000	500000	4	0	4	4	
12	55143	3	2	0	37	0	31	6	18.5	17.67767	0	0	0	0	12300000	666666.7	3	0	3	3	
13	55144	1	2	0	37	0	31	6	18.5	17.67767	0	0	0	0	37000000	2000000	1	0	1	1	
14	55145	4	2	0	37	0	31	6	18.5	17.67767	0	0	0	0	9250000	500000	4	0	4	4	
15	55254	3	3	0	43	0	31	6	14.33333	14.43376	0	0	0	0	14300000	1000000	1.5	0.707107	2	1	
16	36206	54	1	1	0	0	0	0	0	0	0	0	0	0	0	37037.04	54	0	54	54	
17	53524	1	2	0	0	0	0	0	0	0	0	0	0	0	0	2000000	1	0	1	1	
18	53524	154	1	1	0	0	0	0	0	0	0	0	0	0	0	12987.01	154	0	154	154	
19	53526	1	2	0	0	0	0	0	0	0	0	0	0	0	0	2000000	1	0	1	1	
20	53526	118	1	1	0	0	0	0	0	0	0	0	0	0	0	16949.15	118	0	118	118	
21	53527	239	1	1	0	0	0	0	0	0	0	0	0	0	0	8368.201	239	0	239	239	
22	53528	1	3	0	0	0	0	0	0	0	0	0	0	0	0	3000000	0.5	0.707107	1	0	
23	53527	1	2	0	0	0	0	0	0	0	0	0	0	0	0	2000000	1	0	1	1	

Figure 7: A section of the CIC-IDS-2017 training dataset

Figure 7 depicts a portion of the CIC-IDS-2017 training dataset in its raw and unprocessed state, prior to undergoing any cleaning or feature extraction procedures.

4.2 Metrics Used For Evaluation

Evaluation metrics used in this chapter includes: Precision, accuracy, true positive, true negative, false positive, false negative, F1-score and recall.

- True Positive (TP): It occurs when the model correctly predicts the positive class.
- True Negative (TN): Occurs when the model correctly predicts the negative class.
- False Positive (FP): Occurs when the model incorrectly predicts the positive class.
- False Negative (FN): Occurs when the model incorrectly predict the negative class.

The outcomes of the 10 evaluation metrics for the MLP and RNN deep learning algorithms using the NSL-KDD dataset are summarized in Table 3. From the table, it is observed that the performance of MLP outweighs that of RNN for the NSL-KDD dataset.

Table 3: Summary of results of deep learning algorithms using NSL-KDD dataset

Performance Metrics	**Multilayer Perceptron (MLP) (%)**	**Recurrent Neural Network (RNN) (%)**
Accuracy	**99.4390**	98.0208
Precision	**99.5347**	98.0449
Recall	**99.4054**	98.2213
F1-score	**99.4700**	98.1330
Error Rate	**0.5610**	1.9793
FPR	**0.5231**	2.2050
FNR	**0.5946**	1.7788
AUC	**99.4883**	99.2833
MCC	**98.9751**	98.5767
Kappa	**98.9750**	98.5766

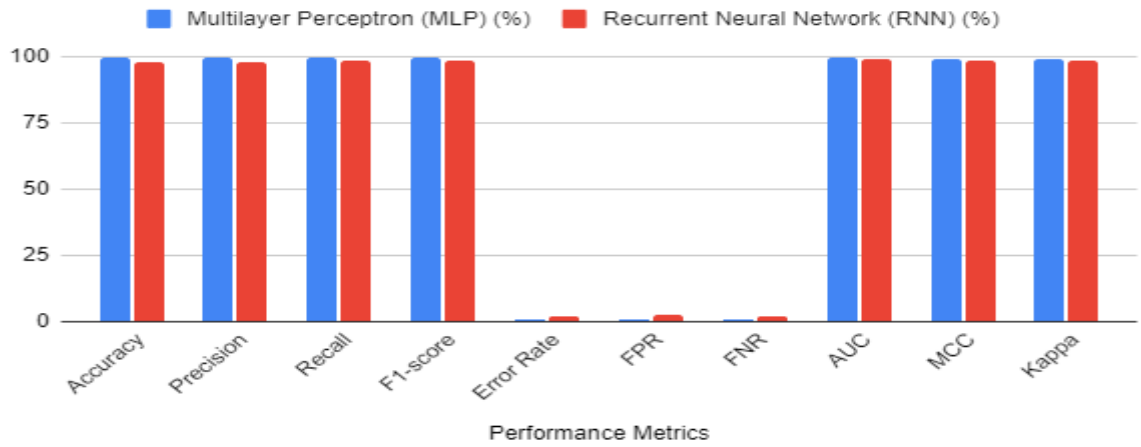


Figure 8: Graphical representation of MLP and RNN on NSL-KDD Dataset

Figure 8 shows the graphical representation of Table 3. It shows the different evaluation metrics for Multiplayer perceptron and Recurrent Neural network for NSL-KDD dataset. MLP has an accuracy of 99.43.

The outcomes of the 10 evaluation metrics for the MLP and RNN deep learning algorithms using the CIC-IDS-2017 dataset are summarized in Table 4. From the table, it is observed that the performance of MLP outweighs that of RNN for the CIC-IDS-2017 dataset.

Figure 9 shows the graphical representation of table 4. It shows the different evaluation metrics for Multiplayer perceptron and Recurrent Neural network for CIC-IDS-2017 dataset.

Table 4: Summary of results of deep learning algorithms using CIC-IDS-2017 dataset

Performance Metrics	**Multilayer Perceptron (MLP) (%)**	**Recurrent Neural Network (RNN) (%)**
Accuracy	**99.9779**	99.0896
Precision	**99.9845**	99.6977
Recall	**99.9767**	98.7016
F1-score	**99.9806**	99.1971
Error Rate	**0.0222**	0.9104
FPR	**0.0206**	0.3965
FNR	**0.0233**	1.2984
AUC	**99.9780**	98.7637
MCC	**99.9548**	97.8121
Kappa	**99.9548**	97.7935

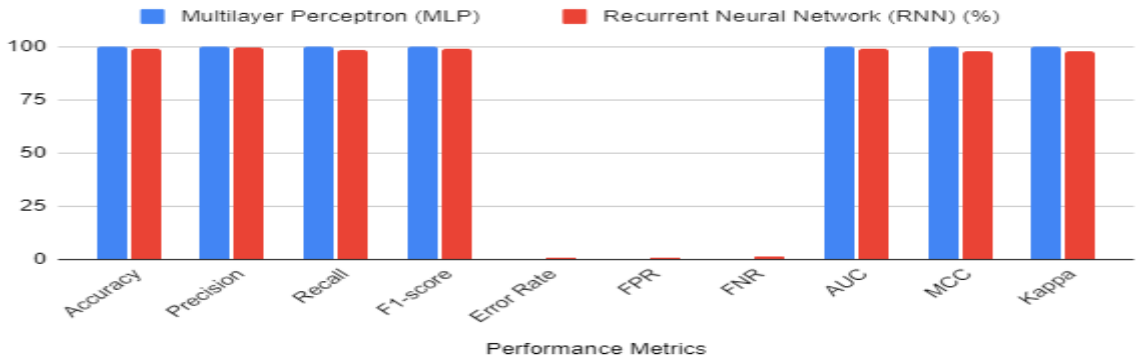


Figure 9: Graphical representation of MLP and RNN on CIC-IDS-2017 Dataset

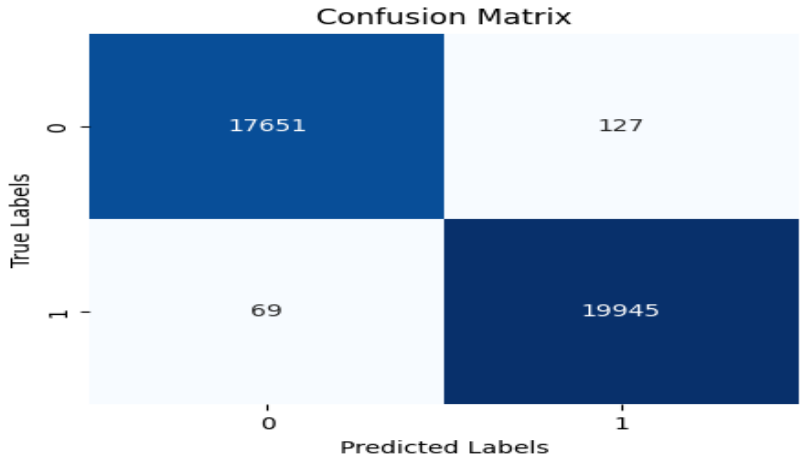


Figure 10: Confusion matrix for MLP using NSL-KDD dataset

Figure 10 provides the confusion matrix for MLP model in terms of the True positive, True Negative, False positive and False Negative using the NSL-KDD dataset.

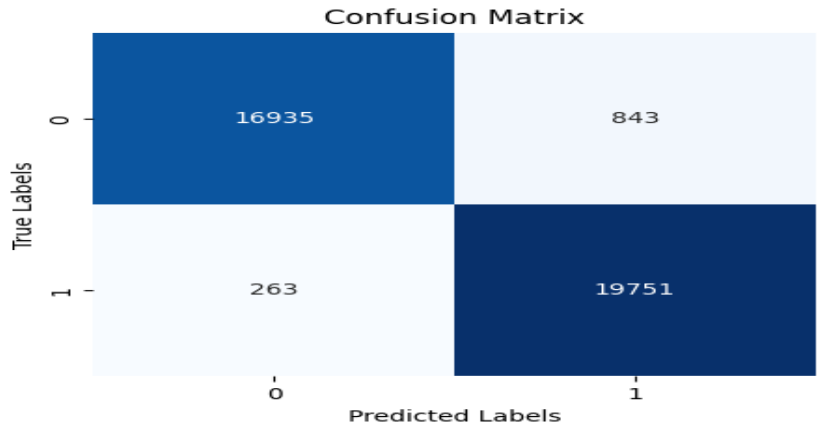


Figure 11: Confusion matrix for RNN using NSL-KDD dataset

Figure 11 provides the confusion matrix for RNN model in terms of the True positive, True Negative, False positive and False Negative using the NSL-KDD dataset.

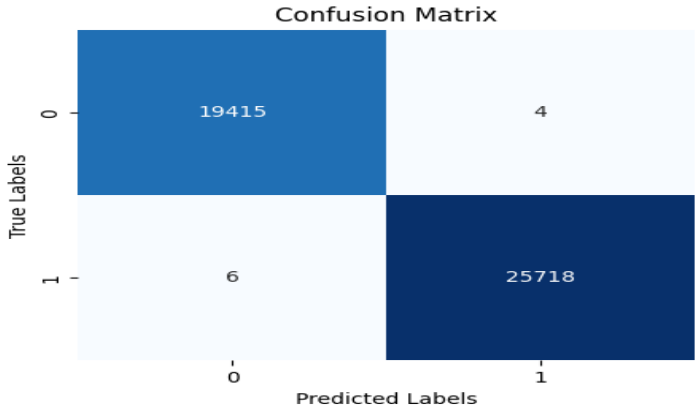


Figure 12: Confusion matrix for MLP using CIC-IDS-2017 dataset

Figure 12 provides the confusion matrix for MLP model in terms of the True positive, True Negative, False positive and False Negative using the CIC-IDS-2017 dataset.

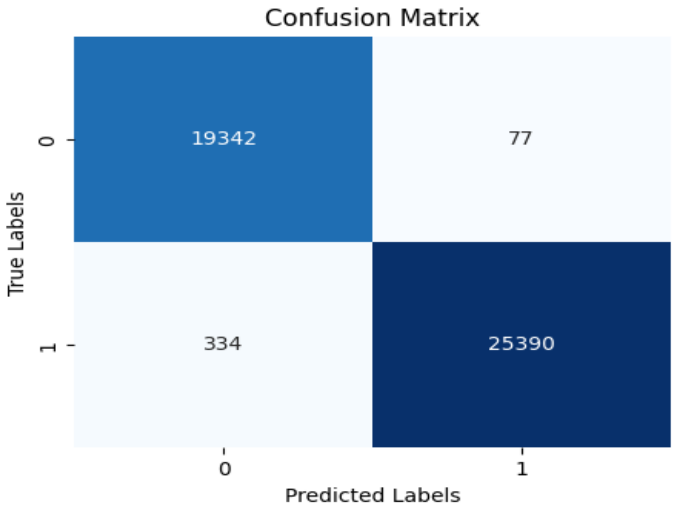


Figure 13: Confusion matrix for RNN using CIC-IDS-2017 dataset

Figure 13 provides the confusion matrix for RNN model in terms of the True positive, True Negative, False positive and False Negative using CIC-IDS dataset.

5. CONCLUSION

In this research study, the primary objective was to comprehensively assess the performance and effectiveness of Multilayer Perceptron (MLP) and Recurrent Neural Network (RNN) models for the purpose of cyber-attack detection. To accomplish this, two prominent datasets, namely NSL-KDD and CIC-IDS-2017, were carefully selected and employed in a series of experiments.

The experiments were specifically designed to compare the capabilities of MLP and RNN in identifying and classifying cyber-attacks accurately. The models were trained and evaluated using these datasets, and their respective performances were thoroughly analyzed and scrutinized. The analysis encompassed various metrics, such as accuracy, precision, recall, and F1 score, which are widely used in evaluating classification models.

The insightful findings and observations derived from the analysis were then presented and discussed in detail in Chapter 4 of the study. This chapter provides an in-depth exploration of the results obtained from the experiments.

By systematically examining the performance of these models on the given datasets, the study facilitates a comprehensive understanding of their capabilities and comparative effectiveness. It sheds light on their potential suitability for real-world deployment and aids in decision-making regarding the selection of the most appropriate model for cyber-attack detection applications.

Overall, the rigorous evaluation of MLP and RNN models on the NSL-KDD and CIC-IDS-2017 datasets, along with the extensive analysis presented in Chapter 4, allows for the formulation of valuable conclusions. These conclusions not only provide insights into the specific performance of the models but also contribute to the broader knowledge and understanding of deep learning approaches in the field of cyber-attack detection.

In summary, by analyzing the obtained results, we successfully utilized two deep learning algorithms, namely Multilayer Perceptron (MLP) and Recurrent Neural Network (RNN), for the purpose of cyberattack detection. Our objectives, which involved the accurate identification of real-time cyberattacks capable of causing significant disruptions across global networks, were achieved. Additionally, we conducted a comprehensive comparative

assessment of the performance of these selected algorithms in detecting multiple types of cyberattacks.

References

[1] Al-Haija, Q. A. (2022, January 13). Top-Down Machine Learning-Based Architecture for Cyberattacks Identification and Classification in IoT Communication Networks. Retrieved from frontiers: https://www.frontiersin.org/articles/10.3389/fdata.2021.782902/full

[2] Al-Haija, Q. A., & Zein-Sabatto, S. (2020, December 15). An Efficient Deep-Learning-Based Detection and Classification System for Cyber-Attacks in IoT Communication Networks. Retrieved from www.mdpi.com: https://www.mdpi.com/2079-9292/9/12/2152

[3] Aljanabi, M., Ismail, M. A., & Ali, A. H. (2021). Intrusion Detection Systems, Issues, Challenges, and Needs. International Journal of Computational Intelligence Systems, 560 - 571.

[4] Anwer, M., Farooq, M. U., Khan, S. M., & Waseemullah . (2021). Attack Detection in IoT using Machine Learning. In Anwer, Engineering, Technology & Applied Science Research (pp. 7273-7278). Pakistan: ETASR.

[5] Bhardwaj, A., Chandok, S. S., Bagnawar, A., Mishra, S., & Uplaonkar, D. (2022). Detection of Cyber Attacks: XSS, SQLI, Phishing Attacks and Detecting Intrusion Using Machine Learning Algorithms. India: IEEE.

[6] Bilen, A., & Özer, A. B. (2021, April 9). Cyber-attack method and perpetrator prediction using machine learning algorithms. Retrieved from peerj.com: https://peerj.com/articles/cs-475/

[7] Brownlee, J. (2019, June 17). A Gentle Introduction to Generative Adversarial Networks (GANs). Retrieved from machinelearningmastery.com: https://machinelearningmastery.com/what-are-generative-adversarial-networks-gans/

[8] Brownlee, J. (2023, January 6). An Introduction to Recurrent Neural Networks and the Math That Powers Them. Retrieved from Machine Learning Mastery: https://machinelearningmastery.com/an-introduction-to-recurrent-neural-networks-and-the-math-that-powers-them/

[9] Chatterjee, M., & Namin, A.-S. (2019). Detecting Phishing Websites through Deep Reinforcement Learning. Texas.

[10] Chisholm, K. (2020). Machine Learning for Cyberattack Detection . University of Dayton: ecommons.

[11] Choubey, V. (2020, July 23). Understanding Recurrent Neural Network (RNN) and Long Short Term Memory(LSTM). Retrieved from Medium.com: https://medium.com/analytics-vidhya/undestanding-recurrent-neural-network-rnn-and-long-short-term-memory-lstm-30bc1221e80d

[12] Data Science. (2020, October 30). Equation of a Multi-Layer Perceptron Network. Retrieved from stackexchange: https://datascience.stackexchange.com/questions/84016/equation-of-a-multi-layer-perceptron-network

[13] Diro, A. A., & Chilamkurti, N. (2018, February 17). Distributed attack detection scheme using deep learning approach for Internet of Things. Retrieved from ScienceDirect: https://www.sciencedirect.com/science/article/abs/pii/S0167739X17308488

[14] Huma, Z. E., Latif, S., Ahmad, J., Idrees, Z., Ibrar, A., Zou, Z., . . . Baothman, F. (2021, April 08). A Hybrid Deep Random Neural Network for Cyberattack Detection in the Industrial Internet of Things. IEEE Xplore, 55595 - 55605.

[15] International Telecommunication Union (ITU). (2021). Measuring digital development - Facts and figures 2021. Switzerland: ITU.

[16] Javatpoint. (2021, January 1). what-are-the-advantages-of-the-internet. Retrieved from javatpoint.com: https://www.javatpoint.com/what-are-the-advantages-of-the-internet

[17] Javatpoint. (2022, August 10). Machine learning Life cycle. Retrieved from javatpoint: https://www.javatpoint.com/machine-learning-life-cycle

[18] Kelley, K. (2022, December 8). What is Cybersecurity and Why It is Important? Retrieved from www.simplilearn.com: https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-cyber-security

[19] Kim, C., & Park, J. (2019, October 15). Designing online network intrusion detection using deep auto-encoder Q-learning. Retrieved from ScienceDirect: https://www.sciencedirect.com/science/article/abs/pii/S0045790618334104

[20] KnowledgeHut. (2023, January 25). Importance of cybersecurity. Retrieved from https://www.knowledgehut.com/: https://www.knowledgehut.com/blog/security/importance-of-cyber-security

[21] Liu, Z., & Xin, Y. (2022, January 15th). Hierarchical Long Short-Term Memory Network for Cyberattack Detection. Retrieved from ieeexplore.ieee.org: https://ieeexplore.ieee.org/abstract/document/9050476

[22] N-able. (2021, March 15). Intrusion Detection System (IDS): Signature vs. Anomaly-Based. Retrieved from www.n-able.com: https://www.n-able.com/blog/intrusion-detection-system

[23] Nedeljkovic, D., & Jakovljevic, Z. (2020, September 15). Cyber-attack detection method based on RNN. Retrieved from ResearchGate: https://www.researchgate.net/publication/346493259_Cyber-attack_detection_method_based_on_RNN

[24] Oladeji, D. (2022). CSC 504 - Security Management. Lagos: Unilag.

[25] Oliveira, N., Praça, I., Maia, E., & Sousa, O. (2021, February 13). Intelligent Cyber Attack Detection and Classification for Network-Based Intrusion Detection Systems. Retrieved from mdpi: https://www.mdpi.com/2076-3417/11/4/1674

[26] Palenzuela, F., Shaffer, M., Ennis, M., Gorski, J., McGrew, D., Yowler, D., . . . Taha, T. (2016, July 29). Multilayer perceptron algorithms for cyberattack detection. Retrieved from IEEE Xplore: https://ieeexplore.ieee.org/abstract/document/7856806

[27] Pratt, M. K. (2022, August 15). Techtarget. Retrieved from www.techtarget.com: https://www.techtarget.com/searchsecurity/definition/cyber-attack

[28] S.Abirami, & Chitra, P. (2020). The Digital Twin Paradigm for Smarter Systems and Environments: The Industry Use Cases. In ScienceDirect, Chapter Fourteen - Energy-efficient edge based real-time healthcare support system (pp. 339-368). India: Elsevier.

[29] Saha, I., Sarma, D., Chakma, R. J., Alam, M. N., Sultana, A., & Hossain, S. (2020, August 22). Phishing Attacks Detection using Deep Learning Approach. Retrieved from IEEE Xplore: https://ieeexplore.ieee.org/abstract/document/9214132

[30] Sanjeevi, M. (2019, January 14). Ch:14 Generative Adversarial Networks (GAN's) with Math. Retrieved from Medium: https://medium.com/deep-math-machine-learning-ai/ch-14-general-adversarial-networks-gans-with-math-1318faf46b43#:~:text=A%20general%20adversarial%20network(GAN,of%20fake%20results%20from%20inputs.

[31] ScienceDirect. (2017). Chapter e6 - Embedded security. In J.Rosenberg, Rugged Embedded Systems (pp. e1-e74). United States: Elsevier.

[32] Soleymanzadeh, R., & Kashef, R. (2022, January 16). The Future Roadmap for Cyber-attack Detection. Retrieved from IEEE Xplore: https://ieeexplore.ieee.org/abstract/document/9845266

[33] UNB. (2022, January 15). Intrusion Detection Evaluation Dataset (CIC-IDS2017). Retrieved from UBN: https://www.unb.ca/cic/datasets/ids-2017.html

[34] Ustebay, S., Turgut, Z., & Aydin, M. (2019). Cyber Attack Detection by Using Neural Network Approaches: Shallow Neural Network, Deep Neural Network and AutoEncoder. ResearchGate, 144-155.

[35] VELIMIROVIC, A. (2021, September 2). What Is an Intrusion Detection System? Retrieved from phoenixnap.com: https://phoenixnap.com/blog/intrusion-detection-system

[36] Vinayakumar, Alazab, M., Soman, K., Poornachandran, P., Al-Nemrat, A., & Venkatraman, S. (2019). Deep Learning Approach for Intelligent Intrusion Detection System. IEEE, 41525-41550.

[37] ZAIB, M. H. (2019, January 15). NSL-KDD. Retrieved from Kaggle: https://www.kaggle.com/datasets/hassan06/nslkdd

[38] Zhou, Y., Han, M., Liu, L., He, J., & Wang, Y. (2018, April 20). Deep learning approach for cyberattack detection. Retrieved from www.researchgate.net: https://www.researchgate.net/publication/326563074_Deep_learning_approach_for_cyberattack_detection

[39] Azeez, N.A.; Salaudeen, B.B.; Misra, S.; Damasevicius, R.; Maskeliunas, R. Identifying phishing attacks in communication networks using URL consistency features. Int. J. Electron. Secur. Digit. Forensics 2020, 12, 200–213.

[40] Azeez, N.A.; Odufuwa, O.E.; Misra, S.; Oluranti, J.; Damaševičius, R. Windows PE Malware Detection Using Ensemble Learning. Informatics 2021, 8, 10. HYPERLINK "https://doi.org/10.3390/informatics8010010" https://doi.org/10.3390/informatics8010010

[41] Azeez, N.A.; Salaudeen, B.B.; Misra, S.; Damasevicius, R.; Maskeliunas, R. Identifying phishing attacks in communication networks using URL consistency features. Int. J. Electron. Secur. Digit. Forensics 2020, 12, 200–213.

[42] Azeez, N.A, Vyver, C.V "Towards a Dependable Access Framework for E-Health", 2017 International Conference on Computational Science and Computational Intelligence (CSCI), pp.1695-1701, 2017.

[43] Azeez, N.A; Vyver, C.V "Dynamic Patient-Regulated Access Control Framework for Electronic Health Information", 2017 International Conference on Computational Science and Computational Intelligence (CSCI), pp.1684-1690, 2017.