Network Intrusion Detection by using a Sequential Deep Neural Network with an Extra Tree Classifier

Muhammad Farhan[1], Sheikh Muhammad Saqib[1], Muhammad Ijaz Khan[1], Mudasir Mahmood[1], Syed Muhammad Ali Shah[1],Saadat Ullah[1], Muhammad Fahim[2]

muhammadfarhan01@gmail.com ; saqibsheikh414@gmail.com ; ijaz171@gmail.com

mudasir@gu.edu.pk ; alishah@gu.edu.pk ; ksaadat125@gmail.com ; muhammad.fahim1@wipro.com

[1]Institute of Computing and Information Technology, Gomal University, Pakistan

[2]Department of Cloud and Infrastructure Service (CIS), Wipro Arabia, Al-Khobar, Saudi Arabia

Abstract

Network intrusion is one of the main threats to organizational networks and systems. Its timely detection is a profound challenge for the security of networks and systems. The situation is even more challenging for small and medium enterprises (SMEs) in developing countries where limited resources and investment in deploying foreign security controls and the development of indigenous security solutions are big hurdles. A robust, yet cost-effective network intrusion detection system is required to secure traditional Internet of Things (IoT) networks to confront such escalating security challenges in SMEs. The aim of an Intrusion Detection System (IDS) is to provide approaches against many fast-growing network attacks (e.g., Fuzzers, Ransomware attacks, Backdoor, etc.), as it blocks the harmful activities occurring in the network system. In this work, an efficient Deep-learning approach was used to detect the accuracy and reduce the processing time of an algorithm on the UNSW-NB15 dataset. This study uses a comprehensive Sequential Deep Neural Network (DNN) from deep learning to identify different types of network attacks for multi-class. Moreover, the Extra Tree classifier, a feature selection technique, has been used to extract highly relevant features from the UNSW-NB15 data. The results show that with the sequential DNN approach, the accuracy achieved was 90% for multi-class network attacks. The detailed experimental testing, such as classification report and Confusion Matrices, confirmed that the DNN model outperformed existing studies. The outcome of the research is significant and contributes to the performance efficiency of intrusion detection systems and the developmentof secure systems and applications.

Introduction

Data and network security problems are growing in today's developed and interconnected world. The main reasons for this problem are the expansion of network traffic and technological advancements, which may have significantly contributed to this unique type of attack. The attack level subsequently

grows [1][2]. Multiple Intrusion Detection Systems (IDS) have been developed and deployed due to today's numerous network security risks. These systems are intended to identify these attacks quickly. The IDS is a monitoring tool that searches for abnormal behavior and notifies users when it detects anything. Based on these notifications, a security operations center analyst examines the issue and takes the necessary steps to minimize the threat. However, network security is an issue for both IDS and firewalls; an IDS monitors the network for intrusions from the outside and the inside, while a firewall is designed to prevent intrusions from occurring by checking for them only on the outside. Since firewalls impose access restrictions between networks, effectively preventing outside attacks, they may be unable to identify attacks from within the network. Due to the complexity and impact of security attacks on computer networks, security experts now use deep learning technologies to protect businesses' data and reputations.

Deep learning is very scalable because it can efficiently analyze vast amounts of data to perform a variety of computations in terms of both time and cost. Several layers of Deep Neural Networks enable models to perform more difficult computing problems, i.e., perform more complex operations simultaneously and learn complex features more quickly. The proposed work focuses on using a sequential Deep Neural Network with an extra tree classifier to detect intrusion from the given dataset.

Aims of the Study

This research aims to investigate the different machine and deep learning methods to construct a model based on an intrusion detection system capable of automatically identifying various types of network attacks. It focuses on detecting potential threats, evaluating the model's efficiency, and categorizing abnormal and normal attacks. The study is designed to select the best model and increase the detection rate by examining unknown attacks compared to the benchmark [3].

Objectives of the Study

The objectives of the current study are the following:

1. Predicting network intrusions using Sequential DNN with an extra tree classifier for multi-class categories.
2. Evaluating the selected model's performance compared to other benchmark works.

Research Questions

The questions addressed by this study are:

Research Question No 1. How to detect intrusions using Sequential DNN with an extra tree classifier multi-class categories?

Research Question No 2. What performance measures are used to compare the selected intrusion classification model with similar research studies?

Related Work

In the past few years, there have been a lot of analytics studies on intrusion detection systems that use deep learning. This area of study is becoming more popular because it can learn and grow. This makes it highly effective and successful in dealing with the alarming rise in unpredictable attacks.

Using the NSL-KDD 99 dataset, researchers, Thaseen and Kumar [4]analyzed in 2013 to compare and contrast several tree-based classification techniques. To conduct the studies, the following algorithms were chosen: AD Tree, C4.5, LAD Tree, NB Tree, Random Tree, Random Forest, and REP Tree. According to the findings of the experiments, the Random Tree, Random Forest, and REP Tree models attained the highest successful accuracy scores. The authors[5]–[8]use a deep learning approach on the KDD-99 dataset to create a deep learning method for finding anomalies.Moustafa et al. [9] demonstrate the complexity of the UNSW-NB15 data set. The experimental results show that UNSW-NB15 was

more complex than KDD99 and is considered a new benchmark data set for evaluating NIDS.Mahmood and Rais [10]choose four different supervised machine-learning methods to analyze the KDD99 dataset to search for anomalies. The results of the study suggest that every machine learning algorithm generates different results for the attack classes of each KDD 99 dataset. According to the researchers, the use of feature selection algorithms will lead to the generation of improved results for future work.Baig et al. [11]introduce an ensemble-based artificial neural network cascade for multi-class intrusion detection (CANID) in computer network traffic. The proposed technique was tested on the KDD CUP 1999 dataset and UNSW-NB15, a recent synthetic attack activity dataset. Experimental results suggest that our approach may efficiently detect various cyber-attacks in computer networks. Van et al.[12]developed an anomaly-based NIDS on the KDDCup99 dataset using Deep Learning. Experiments on the KDDCup99 dataset show that the work was able to accurately identify anomalies in network-based intrusion detection systems and categorize intrusions into five groups using network data sources.In their study, Koroniotis et al. [13]introduced a framework that utilizes machine learning methods to identify botnets and their traces. They applied network flow identifiers to a portion of the UNSW-NB15 dataset. ARM, ANN, NB, and DT classification methods were used. The Decision Tree method had the highest accuracy rate (93.23%) and False Positive Rate (FPR) (6.77%).Using the NSL-KDD dataset,[14]compared three machine learning algorithms. The researchers discussed the dataset's impact for their research. They used the NSL-KDD dataset, pre-processed the data, selected ML classifiers (SVM, RF, and ELM), and measured accuracy, precision, and recall.The approach that was suggested by[15]made use of a Convolutional Neural Network (CNN) as its model. This CNN consisted of multiple layers of perceptron's.Their model was trained by optimizing the hyper parameters.Olayemi et al.[1]presented a UNSW-NB15-based machine learning IDS to defend information. The number of training datasets for naive Bayes, KNNs, and decision models has been reduced by feature selection methods. The paper also discusses the pros and cons of modern machine learning and deep learning intrusion detection models.In their research, Shashnak and Blachandra[16]did an in-depth examination of numerous academic publications that were concerned with the application of machine learning (ML) to various intrusion detection strategies. KDD Data-Cup 1999, Gure KDD-cup, and NSL-KDD were the three important intrusion detection datasets that were specifically investigated by the authors.In their study on network intrusion detection, Phadke et al. [17] explore prominent machine-learning approaches as well as available datasets. The authors provide a list of algorithms and an explanation for each of them: Support vector machine, min-max k-means clustering, artificial neural networks, and back propagation neural network are some of the artificial neural network methods. They then proceed to offer a succinct analysis of the three datasets that were utilized by other researchers, namely the KDD Cup 1999 dataset, the UNSW-NB15 dataset, and the individualized dataset that was created to demonstrate their ANN. Kok et al. [18]examine new research in IDS utilizing a method called Machine Learning (ML). According to the findings of this study, soft computing approaches are receiving a significant amount of attention because so many people are using them.Taher et al.[19]classified network traffic using the NSL-KDD dataset and supervised machine learning methods like SVM, ANN, and wrapper feature selection to evaluate performance. Comparative research reveals the ANN model detects intrusions better than other models. Sstla et al. [20]implemented a deep learning method for use in the predictive models of the NIDS in order to automatically detect anomalies. The findings of the experiments demonstrate that the newly proposed deep learning model is better to the previous model in terms of performance. The purpose of the present work is to conduct a comprehensive assessment of ML methods and DL methods in the context of intrusion detection[21]. This paper provides a summary of recent work and compares the experimental results of various researchers about the detection of

network intrusions.On the NSL-KDD dataset,Rawat et al. [22]examines the performance of traditional machine learning methods, which require considerable feature engineering, in comparison to integrated unsupervised feature learning and deep neural networks.Hameed et al. [3]provides a structure for identifying different attack categories that can be performed against a network. For the purpose of attack detection, a total of five distinct methods, namely Random Forest, Decision Tree, Logistic Regression, K-Nearest Neighbors, and Artificial Neural Networks, were utilized. In this work, we make use of a dataset called UNSW-NB15 that was published by the University of New South Wales. The application of the approach for an artificial neural network yielded results indicating an accuracy of 85.1%.

Research Methodology

In this section, the Research Methodology is mentioned. An experiment is conducted to analyze the UNSW-NB15 dataset and train them using deep learning algorithms such as sequential deep neural networks to detect the attacks.

Research Model

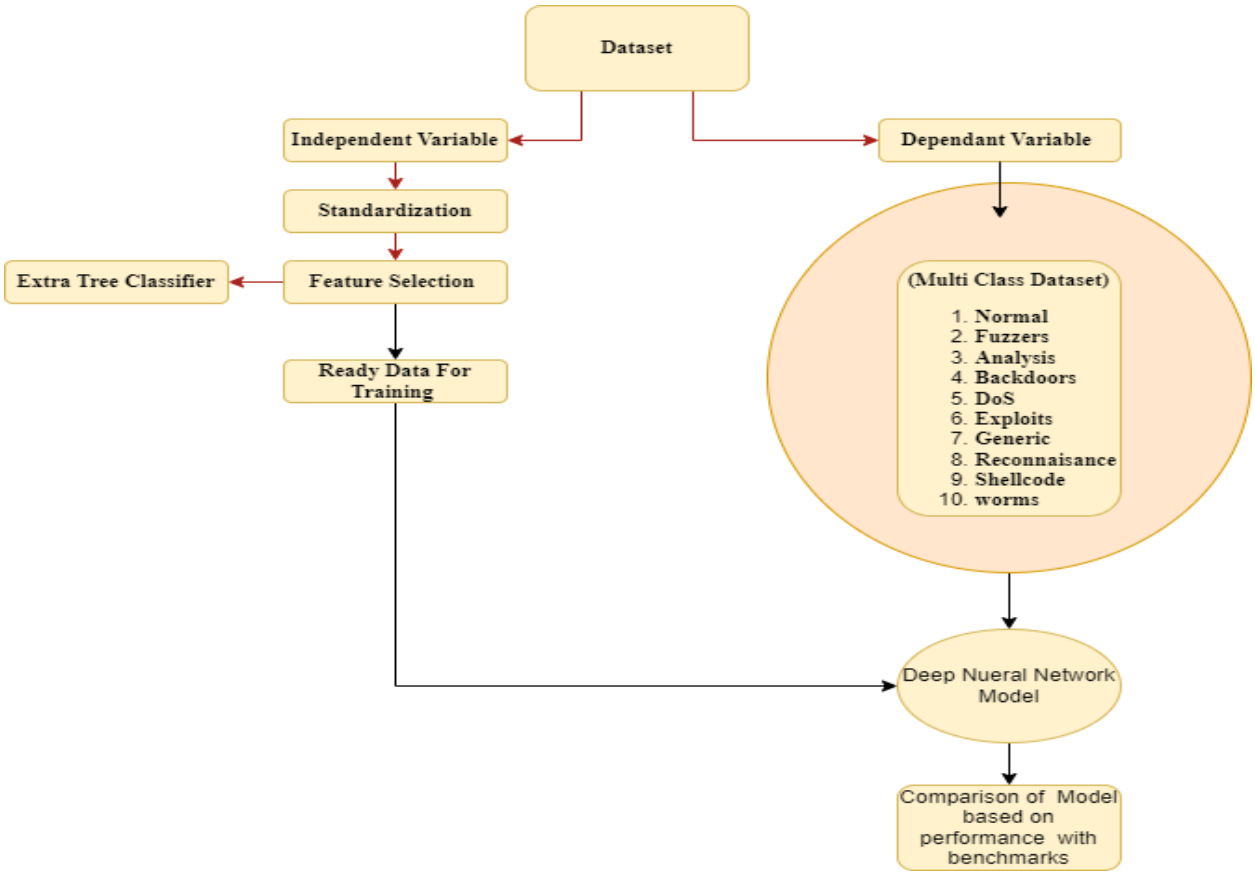

Figure 1-1: A Framework for predicting network attack categories

Sequence of Steps

To obtain the results, the research was conducted in a structured manner following a sequence of steps. Initially, the UNSW-NB15 dataset was subjected to pre-processing using StandardScaler. Subsequently, feature selection was carried out to eliminate attributes that were irrelevant or redundant. After that, classifiers were trained on the chosen attributes which were the output of the feature engineering techniques. To build a hybrid model, two classifiers, Random Forest and Sequential Deep Neural

Network Classifier, were implemented. Finally, the performance of the model was assessed using accuracy as the metric. The objective of carrying out these steps in a methodical manner was to ensure that the research was conducted systematically.

Experiment Results and Discussion

This section will summarize the findings from each study stage and describe how the various experiments worked out. The dataset considered for this research is UNSW-NB15 (***https://www.kaggle.com/datasets/mrwellsdavid/unsw-nb15***), which has 82275 records. Sequential Deep Neural Network will be used on this dataset.

RQ. 1: How to detect intrusion from a given dataset by a proposed model based on the Sequential Deep Learning Model in multi-class categories?

According to the research question, a Sequential DNN is applied to the dataset (UNSW-NB15 and considers 80000 samples for this model. The multi-classification model has ten classes. Class 0 for no attack, Class 1 for Generic attack, Class 2 for Exploits attack, Class 3 for Fuzzers attack, Class 4 for DoS attack, Class 5 for Reconnaissance attack, Class 6 for Analysis attack, Class 7 for Backdoor attack, Class 8 for Shellcode attack, and class 9 for Worms attack. The data selected for training is 70% and 30% for testing.

In**Table 1-1**, the first four and last four independent features with the actual class are presented. The actual class represents the dependent feature showing the dataset's multi-classification.

Table 1-1: Dataset Samples

id	dur	proto	service	state	....	ct_flw_http_mthd	ct_src_ltm	ct_srv_dst	is_sm_ips_ports	Attack_Cat
12049	9.00E-06	udp	dns	INT		0	36	41	0	Generic
37620	0.00424	tcp	ftp-data	FIN		0	8	3	0	Normal
3893	1.26015	tcp	ftp-data	FIN		0	2	1	0	Exploits
63481	0.91755	tcp	-	FIN		0	3	1	0	Reconnaissance
68339	0.64799	tcp	http	FIN		1	2	4	0	Normal
.....										
43669	0.71673	tcp	http	FIN		0	3	1	0	Exploits
20320	9.00E-06	udp	dns	INT		0	16	51	0	Generic
8322	2.24102	tcp	-	FIN		0	2	3	0	Reconnaissance
18942	2.00E-06	udp	dns	INT		0	21	31	0	Generic

After taking the samples, an extra tree classifier, a feature selection method, is applied to different dataset attributes, where the total number of attributes in the dataset is 43. The extra tree classifier selected only 12 different attributes with the most highly relevant scores. The scores for this relevancy are summarizedin **Table 1-2**.

Table 1-2: Selected Attributes taken from Extra Tree Classifier

Sr.No	Selected Attributes Through Extra Tree Classifier	High Relevance values selecting For Attribute
1	proto	(0.206085)
2	spkts	(0.075007)
3	sload	(0.072996)
4	attack_cat	(0.048740)
5	is_ftp_login	(0.045051)
6	ct_ftp_cmd	(0.041062)
7	dload	(0.040302)
8	dtcpb	(0.035362)
9	ct_dst_src_ltm	(0.033016)
10	trans_depth	(0.032750)
11	ct_dst_ltm	(0.031404)
12	synack	(0.026183)

Similarly, the scalar process on the selected attributes is utilized to standardize the data. Each column shows standardized outcomes for each attribute in **Table 1-3**.

Table 1-3: Standardization data after applying Extra Tree Classifier

	proto	spkts	sload	attack_cat	is_ftp_login	ct_ftp_cmd	dload	dtcpb	ct_dst_src_ltm	trans_depth	ct_dst_ltm	synack
0	0.38	0.27	0.72	-0.82	-1.05	-1.01	-0.40	-0.23	-0.12	0.05	-0.31	-0.20
1	1.62	-0.68	0.72	1.34	0.96	1.00	3.46	-0.50	-0.47	-0.45	-0.31	-0.29
2	-1.44	-0.68	0.72	-0.82	-1.05	-1.01	-0.19	-0.32	-0.35	-0.28	-0.13	-0.29
3	0.26	-0.68	0.72	1.34	0.96	1.00	0.10	0.21	-0.35	-0.45	-0.48	0.25
4	0.11	-0.68	0.72	-0.82	-1.05	-1.01	5.62	-0.59	-0.47	-0.45	-0.57	-0.64
.....												
79996	0.94	-0.68	0.72	-0.82	-1.05	-1.01	3.60	-0.50	-0.47	-0.45	-0.57	-0.47
79997	-0.59	-0.68	-1.48	-0.57	0.96	1.00	-0.40	-0.50	-0.47	-0.45	-0.57	-0.11
79998	-1.21	0.27	0.72	-0.82	-1.05	-1.01	-0.40	2.98	4.46	3.58	3.07	3.01
79999	-0.26	-0.68	-1.48	-0.57	0.96	1.00	-0.21	0.39	0.00	-0.45	-0.22	0.07

After standardization, the multi-classification model has been trained with 70% of the training data and 30% of the testing data. The model has been trained with 100 epochs, while the batch size is 50.

Likewise, due to the space limitation of the paper, only the first and last epochs have been presented here, where there are 100 epochs to fit the model. **Table 1-4**represents the first five and last five epochs, respectively.

Table 1-4: Result of Multi-classification Model

Epochs	Time	Loss	Accuracy	Val_Accuracy
1	31s 26ms	0.4546	0.8365	0.8566
2	34s 31ms	0.3630	0.8643	0.8697
3	28s 25ms	0.3388	0.8712	0.8704
4	28s 25ms	0.3219	0.8773	0.8746
5	28s 25ms	0.3093	0.8818	0.8807
.....				
96	25s 22ms	0.2040	0.9122	0.9000
97	25s 22ms	0.2025	0.9114	0.9002
98	25s 22ms	0.2044	0.9115	0.9015
99	28s 25ms	0.2056	0.9115	0.8971
100	30s 27ms	0.2020	0.9125	0.9016

A gradual increase in the Accuracy and Val_accuracy values is observed. Meanwhile, the Loss values also decreased for epochs 0 to 99. These results support the true validation of model fitting

The result of the predicted and actual values of a multi-classification model is shownin

Table.

Table1-5: Actual and Predicted Value of Multi-classification Model

Id	Actual value	Predicted value based on Array	Predicted value
7807	2	[6.9396403e-05 8.7399775e-04 3.9641237e-01 4.9909338e-01 5.7452280e-02 3.8744449e-05 7.5563671e-06 4.6052076e-02 1.6541749e-07 5.1942472e-08]	3
35945	6	[0. 0. 0. 0. 0. 0. 1. 0. 0. 0.]	6
45896	3	[6.7219608e-27 4.3993646e-12 1.2537528e-07 9.9989891e-01 1.0091578e-04 3.6740481e-08 3.1856301e-10 3.0552778e-12 8.1234325e-12 3.3541450e-20]	3
19883	5	[0. 0. 0. 0. 0. 1. 0. 0. 0. 0.]	5
10333	3	[5.8844221e-06 1.7587982e-04 1.2046760e-01 8.7922186e-01 7.0965871e-06 7.4484738e-06 1.6998569e-05 9.7268923e-05 2.6356055e-09 3.3995906e-19]	3
3714	2	[1.0883309e-06 4.7580700e-02 2.3136391e-01 7.2089636e-01 4.5372799e-05	3

		5.3781008e-05 1.5714972e-05 4.1486041e-05 1.5141048e-06 3.7993395e-10]	
27931	6	[0. 0. 0. 0. 0. 0. 1. 0. 0. 0.]	6
71361	6	[0. 0. 0. 0. 0. 0. 1. 0. 0. 0.]	6
60576	5	[0. 0. 0. 0. 0. 1. 0. 0. 0. 0.]	5
19074	5	[0. 0. 0. 0. 0. 1. 0. 0. 0. 0.]	5

In the above table, the results of the actual and predicted values are almost the same, where only a difference of two values is observed between the actual and predicted values. The model shows a good result in classifying attacks to multi-classification.

The result of the multi-classification model concerning accuracy, precision, recall, and f1-score is given in Table 1-6.

Table 1-6: Classification Report of Multi-classification Model

	Precision	**Recall**	**F1-score**	**Support**
0	0.79	0.13	0.23	199
1	0.40	0.01	0.03	168
2	0.50	0.37	0.43	1153
3	0.66	0.83	0.73	3212
4	0.81	0.82	0.81	1726
5	0.99	0.98	0.98	5469
6	1.00	1.00	1.00	10906
7	0.87	0.75	0.81	1042
8	0.77	0.40	0.53	113
9	1.00	0.38	0.55	12
Accuracy			0.90	24000
Macro Avg	0.78	0.57	0.61	24000
Weighted Avg	0.90	0.90	0.89	24000

The table displays the findings from various evaluation matrices required to verify the model's performance. The model performs well in terms of 90% accuracy in the multi-classification model. Meanwhile, the learning curve accuracy of the multi-classification model is shown in**Figure 1-2.**

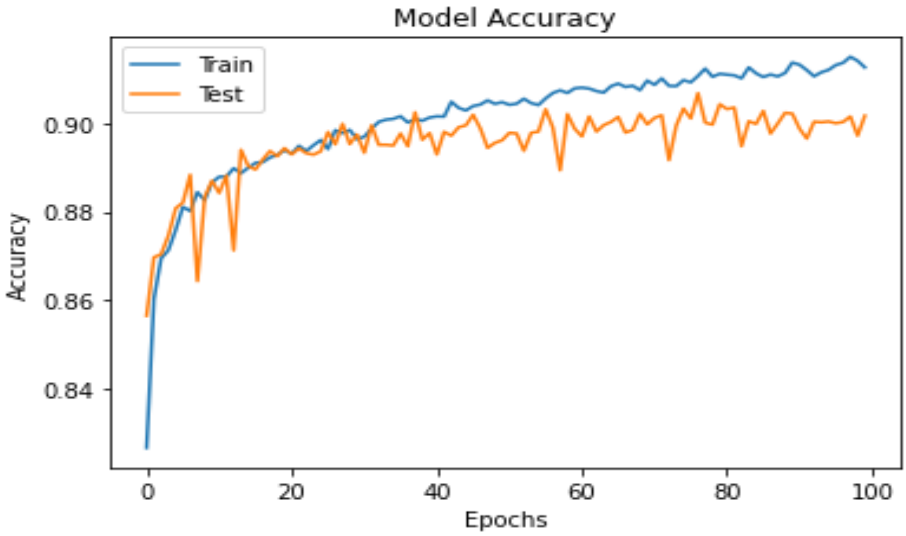

Figure 1-2: Plotting of testing and training accuracy of Multi-classification Model

The accuracy plot shows that as the number of epochs increases, training and testing accuracy is also increased. In terms of classifying attacks according to multi-classification using confusion matrices, **Figure 1-3**presents the results of a sequential deep learning model. A total of 24000 test data points were chosen to evaluate the model. The model correctly predicts that 11 corresponds to Class 0, 5 corresponds to Class 1, 573 corresponds to Class 2, 2537 corresponds to Class 3, 1295 corresponds to Class 4, 5345 corresponds to Class 5, 10893 corresponds to Class 6, 852 corresponds to Class 7. 50 corresponds to Class 8, and 2 corresponds to Class 9.

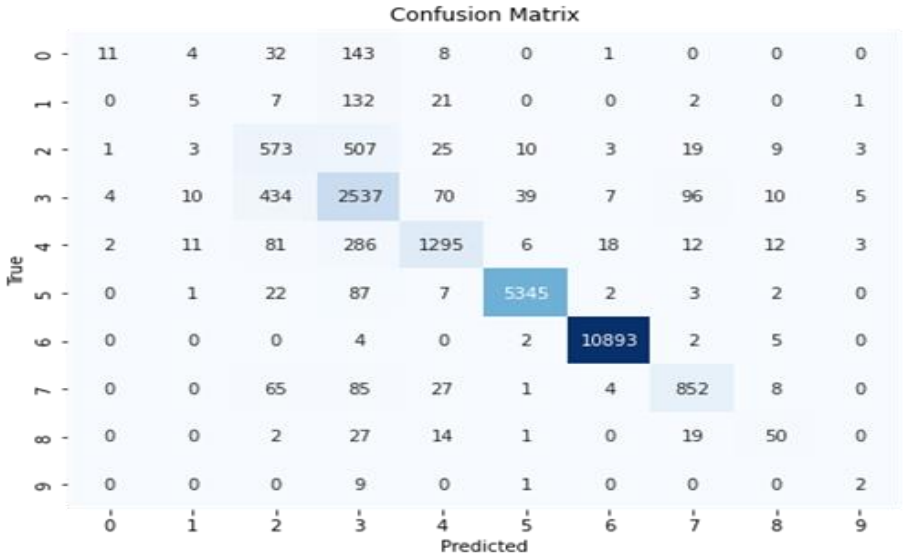

Figure 1-3: Confusion Matrix for Multi-classification Model

Finally, a ROC curve is plotted in **Figure 1-4**to enhance the understanding of the class distinction. According to the plot, thebest classifier for classifying the multi-classification to the suggested model is observed.

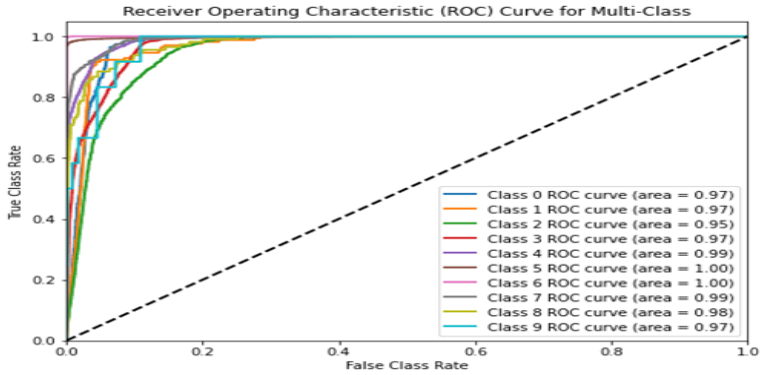

Figure 1-4: ROC Curve for Multi-classification Model

Comparison with Benchmarks

To answer the fourth research question, the proposed model's performance was compared to a benchmark study. The subsequent section provides a comprehensive overview of the comparative analysis.

Performance of Proposed Model

Among the above studies, the proposed model outperforms all of them in terms of accuracy, precision, and recall metrics. Therefore the proposed model is the best among these studies for intrusion detection. The whole comparison is shown in **Table 1-7.**

Table 1-7: Comparison of the proposed model with similar Studies

Works	Model	Multi Classification Accuracy
"The evaluation of Network Anomaly Detection Systems: Statistical analysis ofthe UNSW-NB15 data set and the comparison with the KDD99 data set" [9]	ANN	81.34%
Deep Learning Approach for Intelligent Intrusion Detection System" [23]	DNN	66%
"Performance Analysis of Intrusion Detection Systems Using a Feature Selection Method on the UNSW-NB15 Dataset" [24]	ANN	79.46
"Network intrusion detection using oversampling technique and machine learning algorithms" [3]	DNN	85.7%
Proposed Model result	DNN	90%

Conclusions

Networks play important roles in modern life, and cyber security has become a vital research area. An intrusion detection system (IDS), an important cyber security technique, monitors the state of software and hardware running in the network. Despite decades of development, existing IDSs still face challenges in improving the detection accuracy, reducing the false alarm rate, and detecting unknown

attacks. To solve the above problems, many researchers have focused on developing IDSs that capitalize on machine learning methods. Machine learning methods with high accuracy can automatically discover the essential differences between normal and abnormal data. In addition, machine learning methods have strong generalizability to detect unknown attacks. Deep learning is a branch of machine learning whose performance is remarkable and has become a research hotspot.In this study, a Deep Neural Network (Deep learning model) model has been used to find network intrusions, whereas, on the UNSW-NB15 dataset, the performance of the suggested models has been examined and compared. The proposed models use different pre-processing methods, such as standardizing the data and choosing the most important features by applying the feature selection method. The results showed that the Extra Tree Classifier's choice of feature selection method increased the accuracy of the models. Moreover, based on the test results, it was observed that the classification models performed well on the UNSW-NB15 dataset in terms of accuracy, precision, recall, and F1-score metrics. The accuracy achieved by the Sequential DNN model for multi-classification was 90% which was higher than in the previous studies. The classification reports, and confusion matrices for each class also supported the results.

References

[1] A. A. Olayemi, Alesa b, "A Machine Learning Approach for Information System Security," *Int. J. Inf. Comput. Secur.*, vol. 16, no. 12, pp. 91–101, 2018.

[2] M. I. Alghamdi, "Survey on Applications of Deep Learning and Machine Learning Techniques for Cyber Security," *Int. J. Interact. Mob. Technol.*, pp. 210–224, 2020.

[3] A. Hameed and N. Z. Bawany, "Network intrusion detection using oversampling technique and machine learning algorithms," *PeerJ Comput. Sci. 8e820*, pp. 1–19, 2022, doi: 10.7717/peerj-cs.820.

[4] S. Thaseen and C. A. Kumar, "An analysis of supervised tree based classifiers for intrusion detection system," *Proc. 2013 Int. Conf. Pattern Recognition, Informatics Mob. Eng. PRIME 2013*, pp. 294–299, 2013, doi: 10.1109/ICPRIME.2013.6496489.

[5] N. Gao, L. Gao, Q. Gao, and H. Wang, "An Intrusion Detection Model Based on Deep Belief Networks," *Proc. - 2014 2nd Int. Conf. Adv. Cloud Big Data, CBD 2014*, pp. 247–252, 2015, doi: 10.1109/CBD.2014.41.

[6] Y. Dong, R. Wang, and J. He, "Real-time network intrusion detection system based on deep learning," *Proc. IEEE Int. Conf. Softw. Eng. Serv. Sci. ICSESS*, pp. 1–4, 2019, doi: 10.1109/ICSESS47205.2019.9040718.

[7] K. Alrawashdeh and C. Purdy, "Toward an online anomaly intrusion detection system based on deep learning," *Proc. - 2016 15th IEEE Int. Conf. Mach. Learn. Appl. ICMLA 2016*, pp. 195–200, 2017, doi: 10.1109/ICMLA.2016.167.

[8] V. K. Rahul, R. Vinayakumar, K. Soman, and P. Poornachandran, "Evaluating Shallow and Deep Neural Networks for Network Intrusion Detection Systems in Cyber Security," *2018 9th Int. Conf. Comput. Commun. Netw. Technol. ICCCNT 2018*, no. November, pp. 1–6, 2018, doi: 10.1109/ICCCNT.2018.8494096.

[9] N. Moustafa and J. Slay, "The evaluation of Network Anomaly Detection Systems: Statistical

analysis of the UNSW-NB15 data set and the comparison with the KDD99 data set," *Inf. Secur. J.*, vol. 25, no. 1–3, pp. 18–31, 2016, doi: 10.1080/19393555.2015.1125974.

[10] T. Mehmood and H. B. M. Rais, "Machine Learning Allgorriitthms IIn Conttextt Off Inttrusiion Dettecttiion," *Comput. Inf. Sci. (ICCOINS), 2016 3rd Int. Conf.*, pp. 369–373, 2016.

[11] M. M. Baig, M. M. Awais, and E. S. M. El-Alfy, "A multiclass cascade of artificial neural network for network intrusion detection," *J. Intell. Fuzzy Syst.*, vol. 32, no. 4, pp. 2875–2883, 2017, doi: 10.3233/JIFS-169230.

[12] N. T. Van, T. N. Thinh, and L. T. Sach, "An anomaly-based network intrusion detection system using Deep learning," *Proc. - 2017 Int. Conf. Syst. Sci. Eng. ICSSE 2017*, pp. 210–214, 2017, doi: 10.1109/ICSSE.2017.8030867.

[13] N. Koroniotis, N. Moustafa, E. Sitnikova, and J. Slay, "towards developing network forensic mechanism for botnet activities in the IoT based on machine learning techniques," *Lect. Notes Inst. Comput. Sci. Soc. Telecommun. Eng. LNICST*, vol. 235, pp. 30–44, 2018, doi: 10.1007/978-3-319-90775-8_3.

[14] I. Ahmad, M. Basheri, M. J. Iqbal, and A. Rahim, "Performance Comparison of Support Vector Machine, Random Forest, and Extreme Learning Machine for Intrusion Detection," *IEEE Access*, vol. 6, pp. 33789–33795, 2018, doi: 10.1109/ACCESS.2018.2841987.

[15] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization," in *ICISSP 2018 - Proceedings of the 4th International Conference on Information Systems Security and Privacy*, 2018, pp. 108–116. doi: 10.5220/0006639801080116.

[16] K. Shashank and M. Balachandra, "Review on Network Intrusion Detection Techniques using Machine Learning," *2018 IEEE Distrib. Comput. VLSI, Electr. Circuits Robot. Discov. 2018 - Proc.*, pp. 104–109, 2019, doi: 10.1109/DISCOVER.2018.8673974.

[17] A. Phadke, M. Kulkarni, P. Bhawalkar, and R. Bhattad, "A review of machine learning methodologies for network intrusion detection," *Proc. 3rd Int. Conf. Comput. Methodol. Commun. ICCMC 2019*, pp. 272–275, 2019, doi: 10.1109/ICCMC.2019.8819748.

[18] M. S. SH.Kok, A.Abdullah, NZ.Jhanjhi, "Intrusion Detection System Using Machine Learning Approach," *Int. J. Eng. Res. Technol.*, vol. 12, no. 1, pp. 8–15, 2019.

[19] K. A. Taher, "Network Intrusion Detection using Supervised Machine Learning Technique with Feature Selection," *2019 Int. Conf. Robot. Signal Process. Tech.*, pp. 643–646, 2019.

[20] V. Sstla, V. K. K. Kolli, L. K. Voggu, R. Bhavanam, and S. Vallabhasoyula, "Predictive model for network intrusion detection system using deep learning," *Rev. d'Intelligence Artif.*, vol. 34, no. 3, pp. 323–330, 2020, doi: 10.18280/ria.340310.

[21] G. Kocher and G. Kumar, "Machine learning and deep learning methods for intrusion detection systems: recent developments and challenges," *Soft Comput.*, vol. 25, no. 15, pp. 9731–9763, 2021, doi: 10.1007/s00500-021-05893-0.

[22] S. Rawat, A. Srinivasan, V. Ravi, and U. Ghosh, "Intrusion detection systems using classical machine learning techniques vs integrated unsupervised feature learning and deep neural network," *Internet Technol. Lett.*, vol. 5, no. 1, pp. 1–5, 2021, doi: 10.1002/itl2.232.

[23] R. Vinayakumar, M. Alazab, S. Member, and K. P. Soman, "Deep Learning Approach for Intelligent Intrusion Detection System," *IEEE Access*, vol. 7, pp. 41525–41550, 2019, doi: 10.1109/ACCESS.2019.2895334.

[24] S. M. Kasongo and Y. Sun, "Performance Analysis of Intrusion Detection Systems Using a Feature Selection Method on the UNSW-NB15 Dataset," *J. Big Data*, vol. 7, no. 1, pp. 1–20, 2020, doi: 10.1186/s40537-020-00379-6.