# INTRUSION DETECTION USING A NEURAL NETWORK

| Guide Name | Panel Head |
|---|---|
| Dr Vigneshwaran Pandi | Dr L. Anand |

| Faculty Advisor | Project Domain |
|---|---|
| Dr Vaishnavi Moorthy | Deep Learning in Cybersecurity |

**Student(s) Details: Name**

1. Anshumaan Mishra
2.

**Passport size photo(s)**

Registration Number(s)

1. RA1811028010076
2.

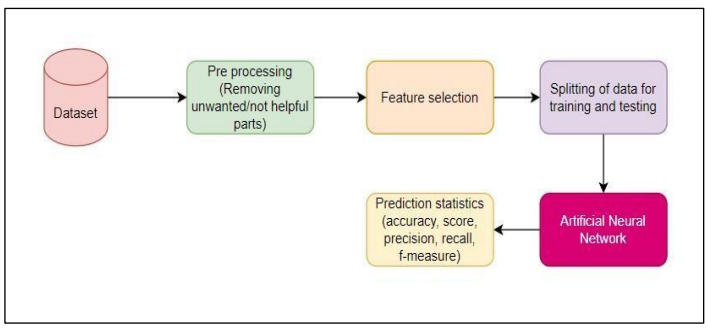
**Email ID(s)&Mobile Number(s)**

| 1: am2747@srmist.edu.in | 2: |
|---|---|
| 9619048802 | |


**Abstract**

Communication between devices in a network requires transporting data from one device to another. For this reason, data packets are present in the network carry some data from sender to receiver and vice versa. For example, the three-way TCP handshake process needs to complete in order to establish a link with the sender and receiver ports of two devices. But an attacker can leverage processes like TCP handshake to extract information from the target device. They can find out about the operating system, which service is being run on the port of the target device, number of open ports etc. To perform reconnaissance an attacker sends data packets using unique protocols, this generates malicious traffic in the network. Attackers may try their best to hide the traffic generated by them by making their traffic look benign. To find the malicious traffic inside a network a network intrusion detection system is put in place to detect abnormal traffic. In this work we have coded a neural network to identify the malicious traffic present in a network dataset. The dataset we used have multiple instances of abnormal traffic, our Neural Network seeks to learn and predict network samples. Neural networks are shown to have higher accuracy compared to most of the traditional machine learning models due to its architecture and complex computations. The deep learning algorithm we have used is a feed forward neural network with two hidden layers and an output layer. To analyse model performance, we use performance metrics like precision, recall and f-measure which are calculated using the values obtained in the confusion matrix. We use a Precision-recall curve at various thresholds to see at what threshold the model has the strongest performance.


**Architecture Diagram**



## INTRUSION DETECTION USING A NEURAL NETWORK

**Conclusion**

The broad application of neural networks is well known and has shown great progress in the history of Intrusion Detection System. The feedforward neural network properly classifies regular traffic and tests its ability to detect attacks. Neural networks have been found to recognize the known attacks used during neural network training. From the history of research in this field, we can concur that having a signature-based IDS is not useful in today's ever-growing field of cybersecurity. Due to development in zero day attacks a signature-based IDS cannot be implemented in the first place as it would repeatedly be needed to be updated. Neural Networks have been created to prefect existing machine learning algorithms, a strength that has led many researchers to use NNs a lot more than ML algorithms. We also found that neural networks can detect unknown attacks that have never used during the training phase. These results mean that neural networks are an important finding for detecting new attacks. The DNN has provided an accuracy of 89.9% which is very high.

In the future we wish to use more efficient algorithms to find more detailed attacks on the system. Our work was based on binary classification but did not tell us about the properties of specific attacks due to dataset limitations but in the future, we wish to work on a multi class classification problem which has several attack features in it. Such a classification would benefit in the discovery of weak areas in the network through the identification of the attack.

**Conference/Journal Publication Details (If Any)**

Anshumaan Mishra, Vigneshwaran Pandi. (2022). Intrusion Detection using a Feed Forward Neural Network. International Journal of Intelligent Engineering and Systems (submitted to journal)

Anshumaan Mishra, Vigneshwaran Pandi. (2022). Classifications of E-MAIL SPAM using Deep Learning Approaches. IOS press (submitted to journal)