**A Mixed Deep Learning and Statistical approach for Anomaly Detection**

Siddhant Saxena1, Vineeta Soni2

Department of Information and technology, Manipal University Jaipur, 3030071,2

**ABSTRACT**

Keywords: Anomaly detection, Network Intrusion, Statistics, Neural Networks

Anomaly detection refers to the problem of finding data patterns that do not confirm expected behavior, but it is a tedious task to prepare a model that performs quite good in a zero-day attack situation, getting the anomaly containing data required to train model is very a complex job because each attack and anomaly varies as per the situation. So here we propose a mixed statistical and deep learning approach that relies on freely available data, we capture data by tapping the network and acquire a .pcap file which can be used to extract features using the cybersectk tool then we compute probabilities of each packet w.r.t Gaussian distribution because every normal packet will lie in normal distribution and packet containing anomaly will deviate from the normal distribution.

The probability of each packet will be calculated using the equation mentioned below,

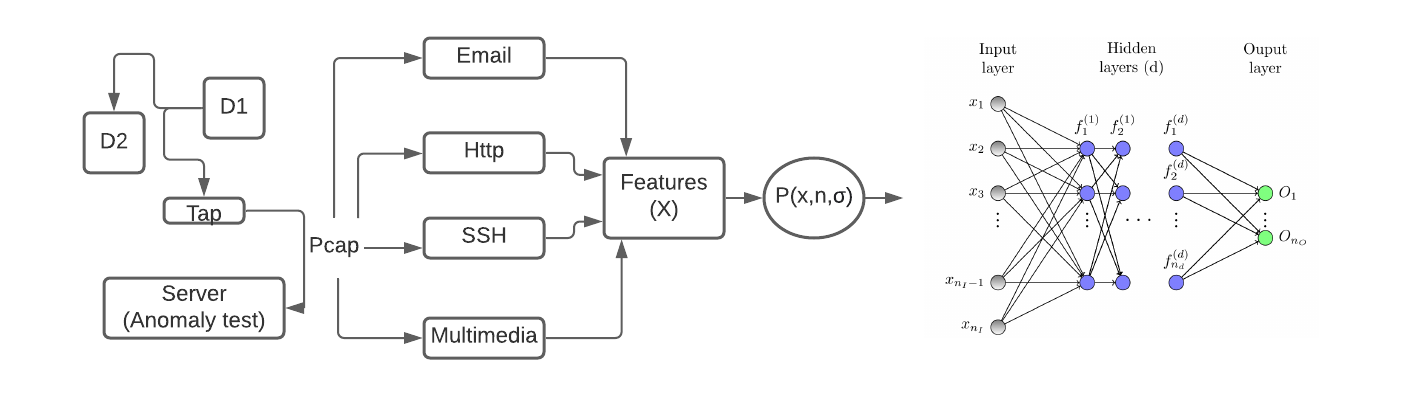
Probability if each packet will get converted to a tensor of n-dimensions and hence now all these probabilities can be used as the input layer to our deep learning model and hidden layers contain a linear function with ReLU as non-linearity,

And the output layer will  provide probabilities of normal and anomalous behavior of the packet. For validation purposes, we will use the joint probability-based approach, which assumes features are independent.

Joint Probabilities of each packet’s probability can be calculated as follows:



And we assume E by hit and trial and if P(x) < E then the packet is anomalous and if P(x) >= E then it is regular.



Flow chart for the Anomaly Detection Model