Cloud Based Network Intrusion Detection System Using Deep Learning Algorithms

Archana C, Chaitra H P, Khushi M, T. Pradhiksha Nandini

Department of Computer Science and Engineering, PES University

Problem Statement

A lot of sensitive data is held by a network of organizations. There has been a spike in the network traffic in the current times which can pose threat to the confidentiality of the data. The attacks performed these days are also very diverse. Hence the proposed model offers a scalable Network Intrusion Detection System using Deep Learning Models.

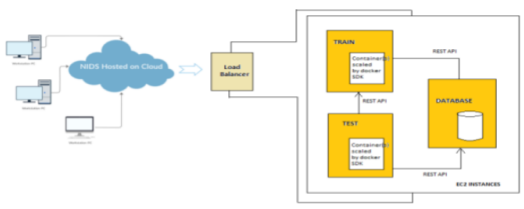
Background

Most the the papers have employed two - three stages in their architecture. The feature selection were either filter based or wrapper based or a hybrid of the two but the results weren't very accurate.

Most of the papers have implemented complex feature extraction/reduction algorithms like auto encoders, CNN or genetic algorithm to improve the efficiency of their model.

Dataset and Product Features

The dataset used is UNSW-NB15. It is a network intrusion detection dataset. The dataset has packets classified either as benign or different types of attacks. UNSW-NB15 contains approximately 2.5 million records. The dataset has 9 different categories of attack named Fuzzers, Analysis, Backdoors, Dos, Exploits, Generic, Reconnaissance, Shellcode and Worms.



The model hosted on cloud has 3 instances each running docker containers for

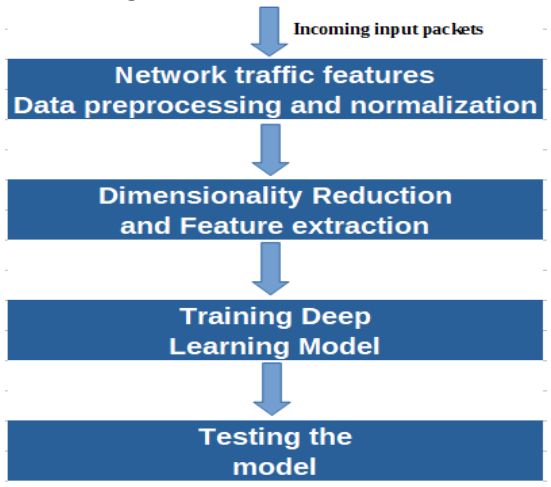
- Testing
- Training
- Storing

data. These instances have Flask Apps with REST APIs to support the functionalities. These Flask Apps can be accessed by sending requests over

Design Approach

A two stage model is used in the proposed model:

- Initial stage is to extract minimal meaningful features which best represent the data.
- Next stage is to classify the input data instance as normal or different types of attacks based on the features of the initial stage.
- Neural Networks like Deep Neural Networks and some other models are used with appropriate activation functions at each layer.
- During optimization, hyperparameter tuning like learning rate, number and depth of hidden layers are used, number of epochs can be fixed after trial and experimentation.
- In an optimization algorithm, Learning Rate is a tuning parameter which determines the step size that needs to be taken at every iteration when we are moving towards a minimum of a loss function.



Results

DEEP LEARNING ALGORITHMS	
	Accuracy
LSTM with 1 hidden layer	88.81%
LSTM with 2 hidden layers	88.75%
LSTM with 3 hidden layers	88.78%
GRU with 1 hidden layer	88.79%
GRU with 2 hidden layers	88.79%
GRU with 3 hidden layers	88.76%
CNN with 2 convolutional layers	93.11%

CNN demonstrated the highest accuracy with 2 convolutional layers.

Summary of Project Outcome

The proposed system offers a scalable solution using DL algorithms to increase the responsiveness of the NIDS during high loads, hence increasing the reliability. The experimental results shows that:

- DNN with four hidden layers achieved the best accuracy of 95.02%
- least accuracy of 88.75% was achieved by a LSTM with two layers
- highest accuracy achieved amongst the ML algorithms is 86% using Random Forest.

Conclusion and Future Work

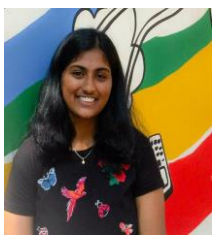
For the Multiclass and Binary Classification problems, the Feed Forward Deep Neural Networks models with full and a Feature Extraction Unit-reduced feature space achieved superior performance compared to other ML classifiers. Using batch normalization has significantly improved the accuracy of the model. CNN with 2 convolutional layers demonstrates the highest accuracy of 93.11%.

A proactive model capable of detecting possibilities of any kind of attack in the near future can be implemented.

Chuanlong Yin, Yuefei Zhu, and Xinzheng He, "A Deep Learning Approach for Intrusion Detection using Recurrent Neural Networks", 2017

R. Vinayakumar, Mamoun Alazab, K. P. Soman, Prabaharan Poornachandran, Ameer Al-nemrat, Sitalakshmi Venkatraman, "Deep Learning Approach for Intelligent Intrusion Detection System'', 2019






Guide: Dr. Sivaraman Eswaran