Common Machine Learning Algorithms in IDS

3.1. Machine Learning Models

* There are two main types of machine learning: supervised and unsupervised learning. Supervised learning relies on useful information in labeled data.
* Classification is the most common task in supervised learning . labeling data manually is expensive and time consuming.
* In contrast, unsupervised learning extracts valuable feature information from unlabeled data, making it much easier to obtain training data.
* The detection performance of unsupervised learning methods is usually inferior to those of supervised learning methods.
* The traditional machine learning models (shallow models) for IDS primarily include the artificial neural network (ANN), support vector machine (SVM), K-nearest neighbor (KNN), naïve Bayes, logistic regression (LR), decision tree, clustering, and combined and hybrid methods.
* Some of these methods have been studied for several decades, and their methodology is mature.
* They focus not only on the detection effect but also on practical problems, e.g., detection efficiency and data management.
* Deep learning models consist of diverse deep networks. Among them, deep brief networks (DBNs), deep neural networks (DNNs), convolutional neural networks (CNNs), and recurrent neural networks (RNNs) are supervised learning models.
* Deep learning models directly learn feature representations from the original data, such as images and texts, without requiring manual feature engineering.
* Thus, deep learning methods can execute in an end-to-end manner.
* For large datasets, deep learning methods have a significant advantage over shallow models.

CONCLUSION

* We can see that the detection accuracy of an attack is related to the amount of attack data when the model is trained through the experimental results.
* We acknowledge that the solution and analysis of the problem may contain some bias and KDD dataset data could not fully reflect the actual application of the network.
* With the development of network communication, attack behavior will become more and more complex.
* Therefore, collecting, processing and analyzing all aspects of users’ behavior data and applying it to the intrusion detection is important for future development.

INTRUSION DETECTION FRAMEWORK AND DATASET

A. Intrusion Detection Framework

The key of intrusion detection is to extract the characteristics of network behavior and to characterize the difference between normal behavior and network attack behavior. Then we design the classification model in feature space to detect. Network anomaly detection mainly includes two parts: the construction classification model and intrusion detection.

Intrusion detection framework is divided into two parts. The first part is the intrusion detection model training, and another part is testing. Both the training set and the test set need to be preprocessed, which is the sign feature digitization and the digital signature normalization. After the model pre-training, reverse adjustment and iteration to the final convergence, the model of deep neural network is mainly composed of fully connected layers (FC), dropout layer and the softmax layer. We can get a more accurate result than a shallow neural network by using the trained model for testing with a test set.

III.METHODOLOGY

*A. Deep Learning Based Intrusion Detection System:* The proposed model is a deep learning model containing inputlayer, multiple hidden layers and the output layer. The features are given into the input layer. There are four hidden layers in the proposed deep learning method. The first layer contains 10 neurons, the second contains 50 neurons, third layer contains 10 neurons and finally the last hidden layer contains only one neuron. The hidden layers have rectified linear unit (relu) and the output layer contains softmax activation function. The processes of the proposed deep learning based model can be split into number of different parts. The dataset used is KDD 99 Cup and the dataset requires data preprocessing in-order to transform the unlabeled and raw data into user understandable format. Further the unique features are extracted from the dataset and they will be used as the input data into the deep learning model. Different feature selection algorithms are available. The data is then split into two, one set for training and the other for validation or testing. The proposed model is trained with the data and later testing is performed in-order to validate whether the system is able to classify the data as normal and abnormal.