Abstract

Due to expansion rate of cyber attacks, there is an important requirement for intrusion detection system (IDS) in networked environments. As intrusion methods become more complicated and more stimulating to identify, this requires refine intrusion detection approach to maintain user assurance and protect network security. During the past decade, many identification approaches have been developed to perform privacy, security. The first section of this thesis analyzes the introduction and related work on intrusion detection approaches formed on machine learning and deep neural networks. The analysis detects limitations of these intrusion detection approaches that detect security issues in network surroundings. The second section of this thesis suggests a innovative Real Time Sequential deep extreme learning machine for intrusion detection that applies random forest, support vector machine classifiers and also applies CNN and RNN training models. We assess its execution on a dataset of stimulated network attacks utilized in related work, NSL-KDD and CIC-IDS2017.Firstly define the pre-processing of the dataset and feature extraction for training our RTS-DELM model and evaluate its execution based on metrics such as recall, f-measure, accuracy, precision. In the last section of thesis, we assess our model in contrast the execution with existing ML classifiers and deep extreme learning networks. Our models predict the type of intrusion by the machine learning and DELM models with 99% accuracy.Its achieving higher performance in contrast with previous models.

Keywords: Intrusion Detection System, Deep Neural Networks, Machine Learning