Abstract

Securing systems from cyber crimes has encouraged the emergence of network forensics, which is a system that can monitor, capture, secure and analyze evidence, which is transmitted through the network.

In this final task, Support Vector Machine (SVM) is used as an artificial intelligence technique for multi-label classification on network forensic data management. The engine is working by classify the intrusion on TCP packet over network traffic data.

The data analysis is done by comparing the accuracy values at various test scenarios the system. Scenarios designed to illustrate the performance of the system when applied by a variation of SVM parameters on a variety of conditions.

The results shows high accuracy can be obtained when the data is first collected. The conclusions is SVM more appropriate when used for offline data which the characteristics of the test data are made as closely as training data.

Keyword: network forensic, support vector machine, intrusion TCP packet, multi-label classification.