Abstract

The Internet of Things (IoT) system, according to literature is prone to many attacks from its interconnected devices. Most of these security treats that IoT is likely to encounter have been identified. These attacks and other security issues have called for the modeling and implementation of algorithms that can identify the current and emerging intrusion and vulnerabilities in IoT so that best security preventive methods may be deployed against them. In this study, a new algorithm, is proposed; cascading Decision Tree (DT) algorithm and Support Vector Machine (SVM) algorithm to improve classification of attacks and consequently the security systems. The proposed algorithm used Support Vector Machine for selection of features based on correlation in the features of the Network Socket Layer - Knowledge Discovery Data (NSL-KDD) data sets. And classification of intrusions was based on the DT algorithm, due to its performance over the SVM. The result of the proposed algorithm proved that the classification of attacks in the decision tree algorithm is improved in terms of prediction speed and training time. In addition, it enhanced the performance of Decision Tree in classifying misclassified classes such as “rootkit” in intrusion detection.
References


Index Terms

Computer Science
Security
Keywords