Abstract

Malware has become a major issue for computer system security today. Due to its ability to spread rapidly and negatively impact system performance, malware detection becomes crucial. One of the methods for malware detection is performing classification using Machine Learning, which learns the variable values of an application without executing it. In this study, the author evaluates the method of malware detection in the static analysis of Windows Portable Executable (PE) using Support Vector Machine (SVM) and Decision Tree. The author uses a dataset of PE files related to malware and safe applications from malware Using SVM and Decision Tree algorithms to classify the PE files as malware or not, determining the best machine learning algorithm for malware detection in PE files. This research compares the two algorithms used to determine the best algorithm for malware detection. The results show that the Decision Tree algorithm achieves an accuracy of 97.35%, while the SVM algorithm achieves a result of 95.62%.

Keywords: Malware, Detection, Support Vector Machine, Decision Tree