Abstract

Malware has emerged as a significant concern for computer system security, as it spreads rapidly and adversely affects system performance. Detecting malware has become crucial, and one of the methods utilized is Machine Learning classification, which learns the characteristics of an application without executing it. In this study, the author evaluates the efficacy of malware detection in the static analysis of Windows Portable Executable (PE) files using the Support Vector Machine (SVM) and Random Forest algorithms. The author employs a dataset containing both malware-related PE files and safe applications to train the SVM and Random Forest models to classify PE files as either malware or safe. The objective is to determine the most effective machine learning algorithm for malware detection in PE files. The research compares the performance of both algorithms to identify the superior one for malware detection. The results indicate that the Random Forest algorithm achieves an impressive accuracy of 98.53%, while the SVM algorithm performs slightly lower with an accuracy of 97.14%.

Keywords: Malware Detection, Support Vector Machine, Random Forest, Machine Learning, Windows Portable Executable