Comparison of Malware Detection Model using Supervised Machine Learning Algorithms

Syamir Mohd Shahirudin[1], Mohd Faris Mohd Fuzi[2]
[1]*syamirmdin@gmail.com*
[2]*farisfuzi@gmail.com*

ABSTRACT

Because of various security concerns and cyberattacks, cybersecurity is crucial in today's environment. In addition, malware has evolved quickly in recent years. Machine learning is utilised for malware detection with the advancement of malware analysis. The comparison of malware detection models utilising supervised machine learning techniques is the main goal of this project. The objective of this project is to develop the Windows malware detection model using supervised machine learning in Decision Tree, K-NN and Naïve Bayes, to evaluate the performance of malware detection model in term of testing and training of the features selection and to compare the accuracy detection model in all three machine learning algorithms. The Windows malware dataset has been training and testing by these three machine learning algorithms to get the percentage detection accuracy. After comparing these three result machine learning algorithms of percentage detection accuracy, the outcomes demonstrated that the best classifier for categorizing our data with 0.96% accuracy is the Decision Tree machine learning algorithm. When comparing the accuracy of a malware detection model, it is excellent if there are numerous machine learning algorithms and more malware datasets included.

Keywords: Supervised machine learning, Windows malware, Malware detection model, Percentage detection accuracy