Comparison of Detection Model Using Machine Learning on Android Malware

Muhammad Ikmal Ihsan[1], Rafiza Ruslan[2], Mohd Faris Mohd Fuzi[3]
[1]*muhammadikmal09@gmail.com*
[2]*rafiza.ruslan@uitm.edu.my*
[3]*farisfuzi@uitm.edu.my*

ABSTRACT

Mobile devices have experienced tremendous growth during the past ten years. As gadgets become more pervasive and people save more sensitive data on their mobile devices, the prevalence of mobile malware has increased. Malicious software, commonly known as malware, poses a greater risk to these mobile devices nowadays. Recently, several articles have been published regarding the proliferation of Android malware. Many new technologies, such as smartphones, have been used into Android malware development, enabling it to advance. It has been used for a long time but is now worthless due of the evolution of Android malware and the inability to detect it. This project will be using supervised machine learning techniques such as SVMs, Naive Bayes and Random Forest to build an android malware detection model. It also will test and train the selection of Android characteristics to evaluate the malware detection model's performance. Then, the project will examine the effectiveness of several machine learning detection models in identifying Android malware. This project will be divided into five distinct parts, each with a distinct purpose. Initialization, planning, development, evaluation, and documentation are all part of the process. In the end of the project, the result will discuss and will be compared for each machine learning used to get the highest accuracy to achieve the project objectives.

Keywords: Machine Learning, Mobile, Android malware, Accuracy