ABSTRACT

Technological advances, particularly in the field of internet usage, bring both positive and negative impacts. On the one hand, the internet makes it easier to obtain information and carry out various activities. However, on the other hand, internet use also carries the threat of cyberattacks, one of which is malware. Malware is a malicious program designed to enter or damage a computer system. Therefore, effective detection is needed that can differentiate malware from non-malware. One way is to apply Machine Learning to distinguish malware attacks from non-malware. This study aims to find a Machine Learning model that has optimal performance in malware detection by comparing three models: Random Forest, Support Vector Machine, and Naïve Bayes. The results showed that Random Forest had the best performance with an F1-score of 0.99. This study shows that selecting the right Machine Learning model significantly influences the accuracy of malware detection.

Keywords: Malware, Dettection, Machine Learning, Random Forest, Support Vector Machine, Naïve Bayes.