Abstract

Malware or Malicious Software is a program created to infiltrate a system so that it can stay for a certain period without going unnoticed by the system's owner. According to recent studies, malware is already increasing in an alarming phase, and some types of malware are hiding in the system using different techniques. This study detected malware on the Android operating system using a system called (syscall). Remote Access Trojan Malware Analysis on the Android operating system using Reverse Engineering Methods helps discover the technological principles of a device, object, or system by analyzing its structure, functions, and operation. This method employed dynamic analysis, namely running every malware on the Android operating system to get information on the system call (syscall) that is running. The results of the system call (syscall) information were selected using the Machine Learning selection feature using the Random Forest method. The purpose of this study is to determine the characteristics based on the system call (syscall) and the detection system's accuracy for the characteristics of Remote Access Trojan malware on the Android operating system. The average accuracy results in this study with four scenarios using the Random Forest method is 96%, and the f1-score value is 94%. This accuracy value is quite good and can be implemented in detecting remote access Trojan malware based on system call (syscall) on the Android Operating System.

Keywords : ***Malicious Software, Remote Access Trojan, Android Operating System, System Call (Syscall), Random Forest, Reverse Engineering***