ABSTRACT

Malware is software to damage and steals information on various network resources or servers that are not known by the owner, virus malware is malicious is vulnerable to system security so that malware gains access to disrupt services on the system and retrieve targeted information. The analysis process is carried out to identify whether a file is a malware or not.

The increasing development of malware can make the malware undetectable because it can avoid the malware analysis techniques it does to detect malware with malware analysis, the development of malware can avoid analysis techniques so that malware cannot be detected. Therefore, this research creates or designs an automatic malware detection system using a dynamic analysis process with cuckoo sandbox to be able to generate classified data. The analysis process is classified using a K-Nearest Neighbors algorithm which is used to classify malware files, in this method K-Nearest Neighbors prefer the closest path from its neighbors in order to get optimal accuracy results.

The process of identifying malware and goodware files on the K-Nearest Neighbors algorithm has a 95 percent accuracy of detection using dynamic characteristics, the test results using Kfold Cross-validation have an average value of 92 percent.

Keyword*: Malware, Dynamic Analysis, Classification, K-Nearest Neighbors, Cuckoo Sandbox*