Android API Malware Detection based on Permission Using Machine Learning and Deep Learning Methods

Muhammad Zhillan Amri[1], Vera Suryani[2]

[1,2,3]Fakultas Informatika, Universitas Telkom, Bandung
[1]zhillanamri@students.telkomuniversity.ac.id, [2]verasuryani@telkomuniversity.ac.id

Abstract

There are several operating systems for software in this world, but the most popular operating system on mobile devices is Android. Android is an open-source operating system that makes it easy for developers to create their own applications, including malware. Malware on Android devices can be dangerous because it can steal sensitive information, cause financial loss, and even corrupt or encrypt data. Threats can also include eavesdropping on user activity, blocking devices or being used for DDoS attacks. Different solutions analyse malware detection through network, behavior, intent, application programming interface, and permission approaches. However, no comparison has been made in the past to determine the effectiveness of different machine learning and deep learning methods. In this study, we performed malware detection through the permission approach on Android applications using the same dataset. After obtaining the dataset, we perform permission classification by converting it into binary numbers. The converted dataset is divided into two parts, namely training data and test data. Furthermore, it is processed with Support Vector Machine, Decision Tree, Artificial Neural Network, and Long Short Term Memory methods. The purpose of this research is to analyse the results of malware detection using confusion matrix and performance parameters. The results of the research conducted by the ANN deep learning method get the highest accuracy value of 99%, precision of 99%, recall of 99%, F1 score of 99%, false alarm rate of 1.3% compared to the SVM, DT, and LSTM methods.

Keywords: malware, android, permission, machine learning, deep learning, analysis, compare