Balochistan Journal of Engineering & Applied Sciences (BJEAS) – (p-ISSN: 2518-2706)
Volume 5, No. 2

Android Malware Detection Using Multi-Feature Evaluation and Machine Learning

Yasir Hussain[1], Abdul Raziq[2], Madiha Murad[1], Farhan Ahmed[3]
[1]Department of Computer Science, LUAWMS, Uthal, Pakistan
[2]Department of Computer Systems Engineering & Sciences, Balochistan UET, Khuzdar, Pakistan
[3]Department of Chemical Engineering, Mehran UET, Jamshoro, Sindh, Pakistan
Corresponding Email: rajaraziq624@gmail.com

Abstract—Malicious application poses a big threat to the privacy and integrity of the individual's life. Because of spreading rapidly in the last decade, the Android platform gains the attention of malware developers. The Android operating system allows the user to install applications downloaded from unknown sources on the web which makes it easier for malware developers to repackage legitimate applications with some kind of malware. In this paper, we proposed a model to detect malware in a more efficient way. The model contributes to the feature evaluation process that has never been used on this dataset before. After the feature extraction, feature evaluation makes the dataset more precise and boosts the performance of the model. This model is evaluated with 123,453 benign applications and 5560 malware samples. After a comparative analysis of different machine learning algorithms, the support vector machine (SVM) has the highest detection accuracy of 98.03%.

Keywords—legitimate Applications, Support Vector Machine (SVM), Application Programming Interface (API), K-Nearest Neighbors (KNN)