Machine learning approaches for malware classification in android platform: a review

ABSTRACT

The rapid growth of Android applications has led to a continuous influx of Android malware. Numerous research has been undertaken to tackle that issue. Existing research has indicated that leveraging machine learning is a highly effective and promising approach for Android malware detection. This paper presents a review of Android malware detection methodologies that rely on machine learning. We commence by providing a brief overview of the background context related to Android applications, including insights into the Android system architecture, security mechanisms, and the categorization of Android malware. Subsequently, with machine learning as the central focus, we methodically examine and condense the current state of research, encompassing crucial perspectives such as sample acquisition, data preprocessing, feature selection, machine learning models, algorithms, and the assessment of detection effectiveness. The aim of this review is to equip scholars with a holistic understanding of Android malware detection through the lens of machine learning. It is intended to serve as a foundational resource for future researchers embarking on new endeavours in this field, while also providing overarching guidance for research endeavours within the broader domain.