ABSTRACT

Android has endured to benefit popularity among cell phone users international. At the same time there has been a rise in malware focused on the platform, with greater current lines employing surprisingly state-of-the-art detection avoidance strategies. As traditional signature primarily based strategies emerge as much less strong in detecting unknown malware, options are wanted for timely 0-day discovery. Accordingly, this paper proposes a method that utilizes ensemble learning for Android malware detection. It combines benefits of hybrid analysis with the efficiency and performance of ensemble device studying to enhance Android malware detection accuracy. The machine getting to know models are built using a huge repository of malware samples and benign apps. The model designed can be able to predict the test cases of all real world applications. lists can be used to store various attributes of the APK files such as permissions, API calls, and intent filters. These lists can then be used as input to the machine learning algorithms for training and prediction. The user can able to get all the details regarding the applications in their devices. This research work proposes a novel approach for detecting Android malware using ensemble learning. The system architecture consists of various modules such as data selection, data preprocessing, data splitting, prediction module, scanning module, notification module, and user interface module. The proposed system utilizes various machine learning algorithms such as Decision Tree, Random Forest, and Androguard for ensemble learning. The testing module is designed to ensure the efficiency and effectiveness of the proposed system. The results demonstrate that the proposed approach is highly effective in detecting Android malware with a detection accuracy of up to 100%. This research work contributes to the field of Android malware detection and can be useful in providing better protection against Android malware for mobile users.