Research Article

DRIVEN BY **doi**®

Android Malware Detection Using Genetic Algorithm

B. Maheshwari and T. Archana

Corresponding Author:
archanapraneeth@gmail.com

ABSTRACT
Android is an open source operating system which is free and Google assists developers to place the Android applications on its Play Store. Anyone can create an android game and place it at the play store at no cost. Hackers are also attracted by this attribute of Android and are creating malicious applications to be installed on the play store. When one installs such malware, it will steal information on the phone and forward it to hackers or provide the scammers with complete control of the phone. The way we do it is through a ML approach to detect malware in mobile applications so that the user does not get exposed to such apps. To detect malware within an app, we must reverse engineer it to retrieve all the code in it and then examine whether it is carrying out any malevolent actions, such sending SMS messages or stealing access to contact details. We will recognize that the application is malicious if such behavior is exposed in the code. More than 100 permissions, including transact, on Service Connected, bind Service, API call signature, Service Connection, and API call signature, can be granted to a single application, and so on. We have to drag these permissions out of the code and create a features dataset. In case the app is generally authorized to do that, then we will record value 1 into the features dataset, and vice versa. These characteristics will be used to identify the dataset app as malware or good software.

Keywords: Android Malware Detection, Genetic Algorithm, Machine Learning, Feature Selection, Static and Dynamic Analysis, Evolutionary Computing, Mobile Security, Optimization Techniques.

[1] M. Tech. (Pursuing), [2]Assistant Professor,
[1,2] Department of Computer Science and Engineering
[1,2] Kakatiya University Campus, Warangal, Telangana, India.