Abstract No: SC-08 **Smart Computing**

Analysis and detection of potentially harmful Android applications using machine learning

***G. A. S. Kavneth and Shantha Jayalal**

Department of Industrial Management,
Faculty of Science, University of Kelaniya, Sri Lanka
**sathindukavneth@gmail.com*

Abstract

With the rapid advancement of technology today, smartphones have become more and more powerful and attract a huge number of users with new features provided by mobile device operating systems such as Android and iOS. Android extended its lead by capturing 86% of the total market in 2017 (Gartner, 2017) and became the most popular mobile operating system. However, this huge demand and freedom has made the hackers and cybercriminals more curious to generate malicious apps towards the Android operating system. Thus, research on effective and efficient mobile threat analysis becomes an emerging and important topic in cybersecurity research area. This paper proposes a static-dynamic hybrid malware detecting scheme for Android applications. While the static analysis could be fast, and less resource consuming technique and dynamic analysis can be used for high complexity and deep analysis. The suggested methods can automatically deliver an unknown application for both static and dynamic analysis and determine whether Android application is a malware or not. The experimental results show that the suggested scheme is effective as its detection accuracy can achieve to 93% ~ 100%. The findings have been more accurate in identifying Android malwares rather than separating those two static and dynamic behaviors. Furthermore, this research compares the machine learning algorithms for static and dynamic analysis of the Android malwares and compare the accuracy by the data used to train the machine learning models. It reveals Deep Neural Networks and SVM can be used for and higher accuracy. In addition, era of the training and testing dataset highly effect the accuracy of the results regarding Android applications.

Keywords: Android, Machine learning, Malware detection, Security

Introduction

Android operating system, which can be found on a wide range of devices, is developed by Google and powered using the Linux kernel. It is an open source operating system, which allows mobile application developers to access unlocked hardware and develop new apps as they wish.

Android application development and Android mobile market has been expanding tremendously in last few years. One of the major reason behind the success of Android OS is easy application development and distribution. Google Play Store and many other Android application markets across the globe allow developers to upload and distribute their applications almost in real time.

People tend to store / collect their life moments, photos, videos, contacts and many more private and confidential information in their mobile phones. Even nowadays, they pay for the goods and store payment information on their phones. Due to the development of IoT technologies they use smart phones to control their environment. Simply smartphones have become essential items in day-to-day life in modern