Android Mobile Malware Detection using Deep Ensemble Machine Learning

Chethana Liyanapathirana[1], Chathura Rajapakse[2]

The Android operating system is one of the most used operating systems in the world and has become a target to malware authors. Traditional malware detection methods such as signatures find it impossible to deal with detecting complex and intelligent malware which are capable of obfuscating and repackaging to avoid being detected. There is therefore an increase in the need to have more efficient and intelligent forms of malware detection. Recently deep machine learning and ensemble machine learning algorithms were used to malware detection and classification. Most of the shallow learning models such as SVM, Random Forest etc. had given less accurate results. Hence this research is focused on using deep learning and ensemble methods for better accurate results. Due to its accuracy and intelligence it has become an ideal solution to bridge the gap between traditional classifiers and the intelligent malware. Methodology used was based on opcode, syscalls and API calls in integrated using static and dynamic analysis. Currently, research is mainly being conducted using deep learning techniques to target all or a given malware family. Research addresses several issues related to android malware detection. One such is to proper identification of obfuscated and repackaged android malware packages using the implemented platform. Next research managed to solve one of the major problems faced in dynamic analysis. This is namely the issue of malware going to a silent mode once tested in the sandbox. This problem was also addressed within the research. This paper proposes a methodology which brings an ensemble solution between the shallow machine learning algorithm and deep learning algorithm to create a solution that provides a higher accuracy and performance friendly application to detect and classify malware.

Keywords: Android Malware; Deep Learning; Malware Classifications

[1] Department of Computer Systems Engineering, Sri Lanka Institute of Information Technology, Malabe, Sri Lanka, *cheth.see456@gmail.com*
[2] Department of Industrial Management, University of Kelaniya, Kelaniya, Sri Lanka