


Chapter 6

Deep Neural Network– Based Android Malware Detection (D–AMD)

Sangeetha D.

Anna University, MIT Campus, India

Umamaheswari S.

 <https://orcid.org/0000-0002-9931-9243>

Anna University, MIT Campus, India

Rakshana Gopalakrishnan

 <https://orcid.org/0000-0003-2182-9494>

Anna University, MIT Campus, India

ABSTRACT

Android is an operating system that presently has over one billion active users for their mobile devices in which a copious quantity of information is available. Mobile malware causes security incidents like monetary damages, stealing of personal information, etc., when it's deep-rooted into the target devices. Since static and dynamic analysis of Android applications to detect the presence of malware involves a large amount of data, deep neural network is used for the detection. Along with the introduction of batch normalization, the deep neural network becomes effective, and also the time taken by the training process is less. Probabilistic neural network (PNN), convolutional neural network (CNN), and recurrent neural network (RNN) are also used for performance analysis and comparison. Deep neural network with batch normalization gives the highest accuracy of 94.35%.

INTRODUCTION

Android, developed by Google, is a layered and open-source operating system that uses a Linux kernel, and is primarily designed for touch screen mobile devices (Liu & Yu, 2011; McLaughlin et al., 2017). The core applications, middleware, and an operating system form the basis of Android. As the Android operating system (OS) became increasingly desired, widely used Android devices include smartphones, tablets, and e-readers.

Despite the different hardware platforms and OSs, computer users encounter the threat of malware (Zabidi, Maarof, & Zainal, 2012). It is not possible to prevent malware from entering the system. With proper detection and monitoring, a system can be kept safe from any kind of hacking problems. Detection of malware in any application is very important to keep things safe.

A major threat of cybersecurity is mobile malware. Moreover, new security threats are pioneered by the daily emerging new mobile malware (Sen, Aydogan, & Aysan, 2018). Mobile malware causes loss or leakage of confidential information and the collapse of the system. Also, it is being a tedious task to make certain that the wireless-enabled personal digital assistants and the mobile phones are safer and possess enough security to withstand these malware attacks, as these devices are having high complexity. Mobile devices are a potential cryptocurrency mining tool, as they are manufactured with powerful graphics processors. In addition, since they are universal and easy to use, it was observed that there is an increase in trojan miner attacks manifold in 2018. According to a Kaspersky security report (Pei, J. Li, H. Li, Gao, & Wang, 2017), 884,774 new malware, three times higher than the number present in 2014, were introduced in 2015. Symantec (2016) additionally rumored that one zero-day attack per week on the average was discovered in 2015. Along with the new families of malware in 2015 (6%), there was a big increase within the volume of Android variants (40%) (2016). As a legitimate software package, malware has evolved over the years and comes with diverged functions, depending on the intent of the developer. Though the amount of recently developed families of Android mobile malware seemed to diminish in the past two years, it has been observed that there is an imperative growth in diversity in the variations of Android malware families (2016).

Owing to their high popularity, Android devices are highly targeted. As per the GDATA report (Pei et al., 2017), 750,000 new Android malware were found in the first quarter of 2017. A large range of mobile malware is expected to develop in the future (Pei et al., 2017). With the development of high quality mobile devices such as smartphones or tablets, attacks on them are increasing. Also, as Android OS allows the users to install third-party applications, it can deceive the users to download the malware from the attacker's servers. In order to address the fast increase within the range of mobile malware, several firms have delivered their own personal mobile protection options, which principally support both static and dynamic analysis. Moreover, several studies within the literature and academia also propose mobile malware detection methods.

Detecting malware in Android applications is a tedious process, since the growth of malware is exponential. Hence, some of the challenges the developers encounter are: Malware writers introduce garbage calls to confuse the analysts with faux application programming interface (API) calls; malware writers encrypt the necessary details at intervals of the malware body (e.g., XOR); malware is also packed using a documented packer. "Packing" is a technique to compress Windows executables. Malware may well be analyzed finely by unpacking them. However, the analysis on the code by unpacking the .apk file without the help of packer is tough and time-consuming, and also safe setting is required to confirm that the malware being analyzed will not infect elsewhere. Many malware Android functions are repackaged

13 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

www.igi-global.com/chapter/deep-neural-network-based-android-malware-detection-d-amd/264366

Related Content

Early Warning System Framework Proposal, Based on Big Data Environment

Goran Klepac, Robert Kopaland Leo Mrsic (2019). *International Journal of Artificial Intelligence and Machine Learning* (pp. 35-66).

www.irma-international.org/article/early-warning-system-framework-proposal-based-on-big-data-environment/233889

MHLM Majority Voting Based Hybrid Learning Model for Multi-Document Summarization

Suneetha S.and Venugopal Reddy A. (2019). *International Journal of Artificial Intelligence and Machine Learning* (pp. 67-81).

www.irma-international.org/article/mhlm-majority-voting-based-hybrid-learning-model-for-multi-document-summarization/233890

A Survey on Arabic Handwritten Script Recognition Systems

Soumia Djaghbello, Abderraouf Bouziane, Abdelouahab Attiaand Zahid Akhtar (2021). *International Journal of Artificial Intelligence and Machine Learning* (pp. 1-17).

www.irma-international.org/article/a-survey-on-arabic-handwritten-script-recognition-systems/279276

Volatility of Semiconductor Companies

Toshifumi Takada (2023). *Encyclopedia of Data Science and Machine Learning* (pp. 14-29).

www.irma-international.org/chapter/volatility-of-semiconductor-companies/317434

Early Warning System Framework Proposal, Based on Big Data Environment

Goran Klepac, Robert Kopaland Leo Mrsic (2019). *International Journal of Artificial Intelligence and Machine Learning* (pp. 35-66).

www.irma-international.org/article/early-warning-system-framework-proposal-based-on-big-data-environment/233889