Deep Learning-Based Malware Detection and Cleansing Mechanism for Server-Side Cloud Computing

Kalpa Kalhara Sampath[1], Suneth Namal Karunarathna[2]

Traditionally, malware is detected by inspecting its signature, which is a unique identifier of the software's binary. Signature based malware detection approaches are now less effective for to identifying intelligent and creative malware's that emerge today. New detection techniques inspect the behavior of the malware instead, where an algorithm is used to learn the patterns of malware activities. In machine learning we need to have handcraft features to train the algorithm. This research is focus on specifically identifying malware in cloud-based systems. For this implantation features like cloud API calls, Energy Consumption and etc. is being used. Some cases these handcraft features might fail to perform to get expected results. To overcome this problem, we proposed a deep learning-based approach. One of the major problems faced in the process of deep learning-based approach is to manage the accuracy versus the performance. Most of the shallow learning techniques records less accuracy but higher performance. But research world had realized for real time implementations the accuracy levels of shallow learning methods like SVM is not suitable with comparing to signature based methods. Hence as the authors selected the deep learning methods was proposed to improve the accuracy. Most of the research work carried out in the last few years in malware detection using deep learning had better accuracies but recorded lower performance parameters. Our approach used an experimented model based on shallow learning and deep learning which gives better accuracy values and performance values. From the deep learning models main focused was RNN/LSTM model. Hence this model is more suited for real time implementations. Initial results revealed better measurements in Precision, Recall and F-measure.

Keywords: Cloud Based Malware; Deep Learning; RNN

[1] Department of Computer Systems Engineering, Sri Lanka Institute of Information technology, Sri Lanka, *kalhara.sampath@gmail.com*
[2] Department of Computer Engineering, University of Peradeniya, Sri Lanka