Deep learning based hybrid analysis of malware detection and classification: A recent review

Syed Shuja Hussain, Mohd Faizal Ab Razak∗ and Ahmad Firdaus
Faculty of Computing, Universiti Malaysia Pahang Al-Sultan Abdullah, Malaysia
E-mail: faizalrazak@ump.edu.my
∗Corresponding Author

ABSTRACT
Globally extensive digital revolutions involved with every process related to human progress can easily create the critical issues in security aspects. This is promoted due to the important factors like financial crises and geographical connectivity in worse condition of the nations. By this fact, the authors are well motivated to present a precise literature on malware detection with deep learning approach. In this literature, the basic overview includes the nature of nature of malware detection i.e., static, dynamic, and hybrid approach. Another major component of this articles is the investigation of the backgrounds from recently published and highly cited state-of-the-arts on malware detection, prevention and prediction with deep learning frameworks. The technologies engaged in providing solutions are utilized from AI based frameworks like machine learning, deep learning, and hybrid frameworks. The main motivations to produce this article is to portrait clear pictures of the option challenging issues and corresponding solution for developing robust malware-free devices. In the lack of a robust malware-free devices, highly growing geographical and financial disputes at wide globes can be extensively provoked by malicious groups. Therefore, exceptionally high demand of the malware detection devices requires a very strong recommendation to ensure the security of a nation. In terms preventing and recovery, Zero-day threats can be handled by recent methodology used in deep learning. In the conclusion, we also explored and investigated the future patterns of malware and how deals with in upcoming years. Such review may extend towards the development of IoT based applications used many fields such as medical devices, home appliances, academic systems.

KEYWORDS
Malware detection; Distributed denial of services; Artificial intelligence; Deep learning; Static and dynamic analysis

Acknowledgment
This work was supported by Universiti Malaysia Pahang Al-Sultan Abdullah, Malaysia, under the internal grant RDU210321.