MalDroid: Secure DL-enabled intelligent malware detection framework

ABSTRACT

Nowadays, smartphones are provided with an abundance of capabilities. During the last decade, the availability of smartphone users and online mobile payment services and applications have substantially grown. Besides, the Android infotainment market is exponentially growing and thus potentially becoming a primary target for cyber adversaries and attackers. Likewise, varied Android vulnerability exploitation and targeted pervasive malware sophisticated attacks are also becoming a hot spot for both industry and academia. The authors present a secure by design efficient and intelligent Android detection framework against prevalent, sophisticated and persistent malware threats and attacks. A novel and highly proficient Cuda-enabled multi-class malware threat detection and identification Deep Learning (DL)-driven mechanism that leverages ConvLSTM2D and CNN has been proposed. The devised approach has been extensively evaluated on publicly available state-of-the-art datasets of Android applications (i.e. Android Malware Dataset (AMD), Androzoo). Standard and extended assessment metrics have been employed to thoroughly evaluate the proposed technique. Moreover, the performance of the proposed algorithm has been verified both with the constructed hybrid DL-driven algorithms and current benchmarks. Additionally, the proposed scheme is cross validated to explicitly show unbiased results.