Contribution ID: **33** Type: **not specified**

A SYSTEMATIC LITERATURE REVIEW OF MACHINE LEARNING FOR MALWARE: METHODS, ALGORITHMS, PERFORMANCE, LIMITATIONS AND FUTURE RESEARCH DIRECTION

Tuesday 28 May 2024 10:50 (10 minutes)

Malware detection is a crucial component of cybersecurity, with various techniques utilized to combat the constantly evolving landscape of malicious software. This work aims to conduct a systematic literature review (SLR) of different machine-learning models used by various authors to evaluate their effectiveness in combating malware. The objective of this work is to synthesizes the knowledge from these studies to better understand various malware detection topics and identify new research issues for possible future research directions. The systematic literature review (SLR) was conducted to review the state-of-the-art studies on Windows and Android malware detection. The results of this study indicate that machine learning algorithms have become increasingly prevalent in malware detection, which has recently gained popularity. The integration of supervised models with deep learning techniques has demonstrated a promising potential for enhancing the efficacy of malware detection and provides insights into how to improve malware detection systems.

Author: EMMANUEL, Lawrence (Federal University of Technology, Minna)

Co-authors: ISMAILA, Idris (Federal University of Technology, Minna, Nigeria); ABDULKADIR, Isah Onivehu (Federal University of Technology, Minna, Nigeria); OJENIYI, Joseph Adebayo (Federal University of Technology, Minna, Nigeria); SUBAIRU, Sikiru Olanrewaju (Federal University of Technology, Minna, Nigeria); WAZIRI, Victor Onomza (Federal University of Technology, Minna)

Presenter: EMMANUEL, Lawrence (Federal University of Technology, Minna)

Session Classification: Technical session 2

Track Classification: Technology: Information and Communication Technology