Enhanced Botnet Detection: A Systematic Literature Review of Hybrid Machine Learning Approaches

Muhammad Aiman Zainudin

College of Computing, Informatics and Mathematic, Universiti Teknologi MARA Kampus Bandaraya Melaka, Malaysia

Nor Masri Sahri

College of Computing, Informatics and Mathematic, Universiti Teknologi MARA Cawangan Melaka, Melaka, Malaysia

Mohamad Yusof Darus

College of Computing, Informatics and Mathematics, Universiti Teknologi MARA Cawangan Shah Alam, Shah Alam, Malaysia

Abstract:

Detecting a malicious activity, particularly botnet attacks, remains a major problem in assuring the security and integrity of networked systems. The suggested method is hybrid machine learning where it combines the characteristics of the Kmeans++ clustering and Decision Tree classification algorithms to improve the accuracy and efficiency of detection. The study focuses on the investigation of the nBaiot dataset, a large library of network traffic data on the Internet of Things (IoT). A systematic literature review for this study will summarises relevant studies that demonstrating the hybrid model's efficacy in identifying botnets within IoT. The result of the review is collected by implementing the searching, analysis, filtering and organising the contents of the previous study from (2018-2023) where at the end of 5 years the contents of this study is on high peak where many researchers discussed this field of study in their research. The research database that is being used are well-known platforms and publications in academia and science that is IEEE Xplore, Science Direct, Research Gate, Wiley and MDPI. This study emphasises the use of hybrid machine learning in botnet detection and provides unique insights into the intrusion detection system, identifying opportunities for further research and future studies.

Keywords:

IoT (Internet of Things), Kmeans++, Decision Tree, Hybrid Machine Learning, nBaiot.