IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Impact Factor: 7.301

Volume 3, Issue 9, May 2023

Malware Identification and Classification using Random Forest Algorithms

H Mangalam, Kiruthika K, Pooja J M, Priya T
Department of ECE
Sri Ramakrishna Engineering College, Coimbatore, India

Abstract: *The rapid expansion of malware is now the biggest danger to information security due to the current wave of technical breakthroughs. Numerous thousands of new malware programmes are created daily and propagated around the internet. Malware varieties are always changing, and these harmful software programmes can be categorized as viruses, trojan horses, worms, spyware, botnet malware, ransomware, etc. The identification and categorization of malware is a critical component for many business programmes that provide protection to an organization's data and end-to-end monitoring of the resources accessible by various users. This model can determine a files maliciousness based on its static data or other important characteristics. The idea behind the proposed methodology is to work on the dataset which consists of the signature of malware and identify the characteristics and features to detect the differently classified malwares based on the machine learning algorithms. Our aim is to effectively detect and categorize malware in order to protect the user information from the cyber threats.*

Keywords: Malware, security, detection, classification, maliciousness, cyber threats

REFERENCES

[1] Shruti Gedam, Khan, Firoz, Cornelius, Laskshmana kumar Ramasamy. "A digital DNA sequencing engine for ransomware detection using machine learning." IEEE Access 8 (2020): 119710- 119719.

[2] Al-Hashmi, Asma A., Fuad A., Ghaleb, A. Al-Marghilani. "Deep- Ensemble and Multifaceted Behavioral Malware Variant Detection Model." IEEE Access 10 (2022): 42762-42777.

[3] Xing Xiaofei, Xiang Jin, Haroon Elahi, Hai Jiang, Guojun Wang. "A Malware Detection Approach Using Autoencoder in Deep Learning." IEEE Access 10 (2022): 25696-25706.

[4] Şahın, Durmuş Özkan, Sedat Akleylek, and Erdal Kiliç. "LinRegDroid: Detectionof Android malware using multiple linear regression models-based classifiers." IEEE Access 10 (2022): 14246-14259.

[5] Sai, Anne Yeswanth, et al. "Malware Detection Using Machine Learning Techniques." Smart Data Intelligence. Springer, Singapore, 2022. 95-107.

[6] Almomani, Iman, Aala Alkhayer, and Walid El-Shafai. "An Automated Vision- Based Deep Learning Model for Efficient Detection of Android Malware Attacks." IEEE Access 10 (2022): 2700-2720.

[7] Aslan, Ömer, and Abdullah Asim Yilmaz. "A new malware classification framework based on deep learning algorithms." Ieee Access 9 (2021): 87936-87951.

[8] Mahajan, Ginika, Bhavna Saini, and Shivam Anand. "Malware classification using machine learning algorithms and tools." 2019 Second international conferenceon advanced computational and communication paradigms (ICACCP). IEEE, 2019.

[9] Ana, Madhurima, and Swathi Edem. "An Efficient Deep Learning Based Approach for Malware Classification." Machine Learning Technologies and Applications. Springer, Singapore, 2021. 193-201.

[10] Usman, Nighat, et al. "Intelligent dynamic malware detection using machine learning in IP reputation for forensics data analytics." Future Generation Computer Systems 118 (2021): 124- 141.

DOI: 10.48175/IJARSCT-10385