IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 4, May 2022
Impact Factor: 6.252

Malware Detection and Classification Framework for IOT Devices

Sayali Khirid[1], Sakshi Veer[2], Tanushika Gupta[3], Vishwajeet Waychal[4], Mrs. Asmita R. Kamble[5]
Students, Department of Computer Engineering[1]
Professor, Department of Computer Engineering[2,3,4,5]
Sinhgad Institute of Technology and Science, Pune, Maharashtra, India

Abstract: *Internet of Things (IoT) technology provides the basic infrastructure for a hyper connected society where all things are connected and exchange information through the Internet. IoT technology is fused with 5G and artificial intelligence (AI) technologies for use various fields such as the smart city and smart factory. As the demand for IoT technology increases, security threats against IoT infrastructure, applications, and devices have also increased. A variety of studies have been conducted on the detection of IoT malware to avoid the threats posed by malicious code. While existing models may accurately detect malicious IoT code identified through static analysis, detecting the new and variant IoT malware quickly being generated may become challenging. Due to the complexity of design and implementation in both hardware and software, as well as the lack of security functions and abilities, IoT devices are becoming an attractive target for cyber criminals who take advantage of weak authentication, outdated firmware's , and malwares to compromise IoT devices .This project provides the light on the system named as malware classification and detection of IOT devices, used to detect the cyber-attacks caused by malware on IOT devices by using machine learning techniques. The malware classification and detection system detect and identifies the various types of malwares using static analysis with the help of machine learning algorithm. An easy-to-use user interface for easy uploading of files and checking for virus is designed. Also, acceptance testing is performed on the application to remove vulnerabilities.*

Keywords: Internet of Things, Malware, Malware Classification, Static Analysis.

REFERENCES

[1]. Jueun Jeon 1 , Jong hyuk park 2 , (member, IEEE), and Young-Sik Jeong , ''Dynamic Analysis for IoT Malware Detection With Convolution Neural Network Model ,'' 2020.
[2]. Zhongru Ren a , Haomin Wu d , Qian Ning c ,Iftikhar Hussain e , Bingcai Chen, "End-to-end malware detection for android IoT devices using deep Learning ," 2019.
[3]. Danish Vasan, Mamoun Alazeb, Sitalakshmi Venkatraman, Junaid Akram, Zheng Qin, "MTHAEL: Cross-Architecture IoT Malware Detection Based on Neural Network Advanced Ensemble Learning," 2020.
[4]. N. Moses Babu , Qian Ningc, "Malware Detection for Multi Cloud Servers using Intermediate Monitoring Server," 2019.
[5]. Abhijit Yewale, Maninder Singh, "Malware Detection Based On Opcode Frequency," 2020.
[6]. S. Muthurajkumar, M. Vijayalakshmi, S. Ganapathy, A. Kannan, "Agent Based Intelligent Approach for the Malware Detection for Infected Cloud Data Storage Files," 2019.
[7]. Muhammad Amin, Duri Shehwar, Abrar Ullah, Teresa Guarda, Tamleek Ali Tanveer, "A deep learning system for health care IoT and smartphone malware detection," 2020
[8]. Fei Xiao , Zhaowen Lin ,Yi Sun ,Yan Ma, "Malware Detection Based on Deep Learning of Behavior Graphs," 2019
[9]. Hamed HaddadPajouh , Ali Dehghantanha , Raouf Khayami , Kim-Kwang Raymond Choo, " A deep Recurrent Neural Network based approach for Internet of Things malware threat hunting," 2018.
[10]. Quoc-Dung Ngo, Huy-Trung Nguyen, Van-Hoang Le, Doan-Hieu Nguyen, "A survey of IoT malware and detection methods based on static features," 2019.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 4, May 2022
Impact Factor: 6.252

[11]. Hamad Naeem, Farhan Ullah, Muhammad Rashid Naeem, Shehzad Khalid, Danish Vasan, Sohail Jabbar, Saqib Saeed, "Malware detection in industrial internet of things based on hybrid image visualization and deep learning model," 2020.

[12]. Hayate Takase, Ryotaro Kobayashi,Masahiko Kato,Ren Ohmura, "A prototype implementation and evaluation of the malware detection mechanism for IoT devices using the processor information," 2019.