IJARSCT

ISSN (Online) 2581-9429

Impact Factor: 6.252

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

Volume 2, Issue 3, May 2022

Developing an Efficient Feature Engineering and Machine Learning Model for Detecting IoT-Botnet Cyber Attacks

Aishwarya Tingare[1], Akshay Desainipanikar[2], Amisha Devadiga [3], Prof. Mrs. Jyoti Raghatwan[4]

Students, Department of Computer Engineering[1,2,3]

Faculty, Department of Computer Engineering[4]

RMD Sinhgad School of Engineering, Pune, Maharashtra, India

Abstract: *Computers and networks have been under threat from viruses, worms and attacks from hackers since they were first used. In 2018, the number of devices connected to the Internet exceeded the number of human beings and this increasing trend will see about 80 billion devices by 2024. Securing these devices and the data passing between them is a challenging task because the number of IBAs is also increasing sharply year by year. To address this issue, a large number of defences against network attacks have been proposed in the literature. Despite all the efforts made by researchers in the community over the last two decades, the network security problem is not completely solved. In general, defence against network attacks consists of preparation, detection and reaction phases. The core element of a good defence system is an IOT Botnet Attack (IBA) Detection System (IBA-DS), which provides proper attack detection before any reaction. An IBA-DS aims to detect IBAs before they seriously damage the network. The term IBA refers to any unauthorised attempt to access the elements of a network with the aim of making the system unreliable.*

Keywords: IOT Botnet, Attack, LSTM, Detection System

References

[1]. G. Loukas, and O. Gulay. "Likelihood ratios and recurrent random neural networks in detection of denial of service attacks." 2007.

[2]. G. Oke, G. Loukas and E. Gelenbe, "Detecting Denial of Service Attacks with Bayesian Classifiers and the Random Neural Network," 2007 IEEE International Fuzzy Systems Conference, London, 2007, pp. 1-6.

[3]. A. B. M. A. A. Islam and T. Sabrina, "Detection of various denial of service and Distributed Denial of Service attacks using RNN ensemble," 2009 12th International Conference on Computers and Information Technology, Dhaka, 2009, pp. 603-608.

[4]. Z. A. Baig and K. Salah, "Multi-Agent pattern recognition mechanism for detecting distributed denial of service attacks," in IET Information Security, vol. 4, no. 4, pp. 333-343, December 2010.

[5]. M. Kim, H. Na, K. Chae, H. Bang, and J. Na: A Combined Data Mining Approach for DDoS Attack Detection, Lecture Notes in Computer Science, Vol. 3090, pp. 943-950, 2004.

DOI: 10.48175/IJARSCT-3700