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

IJARSCT

Impact Factor: 7.301

Volume 3, Issue 11, May 2023

Detection and Prevention of DDoS Attack using Ensemble Model

Prof. R. N. Muneshwar[1], Mr. Mahale Swami[2], Mr. Muley Pranav[3], Mr. Joshi Lakshmikant[4], Mr. Sambyal Suryansh[5]

Department of Information Technology[1,2,3,4,5]
Amrutvahini College of Engineering, Maharashtra, India

Abstract*: In the current cyber world, one of the most severe cyber threats are distributed denial of service (DDoS) attacks, which make websites and other online resources unavailable to legiti- mate clients. It's a cyberattack aimed at overwhelming a server with malicious traffic, causing a website to shut down temporarily or permanently. It's typically executed using malware- infected devices called bots, and their cluster is referred to as a botnet. These bots include lap- tops, smartphones, smart TVs, wearable devices, thermometers, security cameras, in-vehicle infotainment systems, etc. So, what industries do DDoS attackers target? They commonly target the gaming, software and technology, media and entertainment, finance, and internet and telecom industries. It is different from other cyber threats that breach security parameters; how- ever, DDoS is a short-term attack that brings down the server temporarily. So we came up with a solution to decrease the impact of DDoS attack and thus proposed a model which can predict whether input given is a attack file or normal file based on the dataset (CICDDOS2019) it is trained on.To mitigate the impact of DDoS attacks, we propose a model that predicts whether an input file is an attack file or a normal file based on the CICDDOS2019 dataset it is trained on. We have developed an ensemble of machine learning classifiers, including KNN-DT, KNN-RF and DT-RF, to enhance the accuracy and robustness of the prediction model. By accurately identifying attack files, organizations can take proactive measures to protect their servers and mitigate the effects of DDoS attacks.*

Keywords: Distributed Denial of Service (DDoS), Deep Learning, CNN, KNN, Decision Tree, Random Forest etc.

REFERENCES

[1] A. Abdellatif, H. Abdellatef, J. Kanesan, C. -O. Chow, J. H. Chuah and H. M. Gheni, ”An Effective Heart Disease Detection and Severity Level Classification Model Using Machine Learning and Hyperparameter Optimization Methods,” in IEEE Access, vol. 10, pp. 79974-79985, 2022, doi: 10.1109/ACCESS.2022.3191669

[2] Juan Fernando and Gabriel Enrique Taborda Blandon,“A Deep Learning- Based Intru- sion Detection and Preventation System for Detecting and Preventing Denial-of-Service Attacks,” IEEE Access, 2022

[3] Adnan Akhunzada, Iqra Mustafa, Tanil Bharat Patel, “A Deep CNN Ensemble Framework for Efficient DDoS Attack Detection in Software Defined Network,” IEEE Access, 2020

[4] Y. Xin, L. Kong, Z. Liu, Y. Chen, Y. Li, H. Zhu, M. Gao, H. Hou, and C. Wang, “Ma- chine learning and deep learning methods for cybersecurity,” IEEE Access, vol. 6, pp. 35365–35381, 2018

[5] Ahmed Ramzy Shabaan, Mohmed Hussein, “DDoS attack detection and classification via Convolutional Neural Network (CNN),” IEEE Access, 2019

DOI: 10.48175/IJARSCT-10596