IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 2, Issue 1, May 2022
Impact Factor: 6.252

DeepDefender: High-Precision Network Threat Classification Using Adversarial-Resistant Neural Networks

Gaurav Sarraf
Independent Researcher
sarrafgsarraf@gmail.com

Abstract: *Deep learning is a recent technology that is applicable in different areas in the contemporary world. The applications that identify potential adversarial attacks and prevent them are utilized in order to offer effective solutions associated with the broad spectrum of computer security with the assistance of deep learning (DL) models. With the ever-growing adversarial deep learning, accessibility to the deep learning model can vary in the number of levels, and in this case, the attackers can conduct a series of attacks to reach the intended goal. Concurrently, the DL models and algorithms are quite susceptible to numerous cybersecurity attacks. The research details a potential approach to classifying and predicting network threats using an ANN model trained on the CICIDS 2017 dataset. To evaluate the efficacy of the stratified data-splitting artificial neural network (ANN) model, key performance indicators were recall (REC), accuracy (ACC), precision (PRE), and F1-score (F1). The results show that the model is robust and trustworthy in detecting and classifying different types of cyberattacks, with a 99.7% ACC rate, a 99.9% PRE rate, a 99.9% REC rate, and an F1 of 99.9%. These results show that deep learning systems based on ANNs have the ability to improve network security.*

Keywords: Cyber Security, Threat Classification, Intrusion Detection, Network Security, Artificial Intelligence, Artificial Neural Networks

Copyright to IJARSCT
www.ijarsct.co.in
DOI: 10.48175/IJARSCT-3600E