Augmenting IoT Intrusion Detection System Performance Using Deep Neural Network

Authors Nasir Sayed, Muhammad Shoaib, Waqas Ahmed, Sultan Noman Qasem, Abdullah M. Albarrak and Faisal Saeed

Publication Year 2022
Grant Number RG-21-07-04
DOI link https://doi.org/10.32604/cmc.2023.030831

Abstract: Due to their low power consumption and computing power, Internet of Things (IoT) devices are difficult to secure, and the rapid growth of IoT devices in the home increases the risk of cyber-attacks. One method of preventing cyberattacks is to employ an intrusion detection system (IDS), which detects incoming attacks and notifies the user, allowing for the implementation of appropriate countermeasures. Attempts have been made in the past to detect new attacks using machine learning and deep learning, but these efforts have been unsuccessful. In this paper, we classify network attacks using two Convolutional Neural Networks (CNN) models i.e., MyCNN and IoTCNN to automatically detect various kind malignant and benign intrusion in IoT network. The purpose of this research is to evaluate the use of deep learning in IoT IDS. The neural network was trained in this experiment using the NF-UNSW-NB15-v2 dataset, which contains nine distinct types of attacks. The data from the network stream was converted to Red Green and Blue (RGB) images, which were then used to train the neural network. To establish baseline models, we proposed two models with the name of MyCNN and IoTCNN. When compared the proposed MyCNN convolutional neural network for network attack classification, the IoTCNN was outperformed by the MyCNN model. Additionally, it demonstrates that both networks achieve higher accuracy in the majority of categories but the IoTCNN achieved lower than the proposed MyCNN model for network attack detection. We discovered that the MyCNN is generally more suitable to be deployed for intrusion detection in IoT devices.