Abstract

Intrusion detection in the context of the Internet of Things (IoT) has the main goal of identifying and responding to activities that could compromise system security. The focus of this research is to develop an effective intrusion detection model for IoT networks by comparing the performance of three main models, namely Convolutional Neural Network (CNN), (Long Short-Term Memory LSTM), and Recurrent Neural Network (RNN). The results show that the CNN model outperforms with the highest accuracy, reaching 99.97%. Meanwhile, LSTM and RNN also achieved high performance with accuracy of 99.76% and 99.58%, respectively. Although the difference in accuracy between models is small, CNN consistently shows slightly superior performance in classifying suspicious activity. CNN had the highest scores on all metrics, including accuracy (100%), precision (100%), recall (99.99%), F1-Score (100%), and AUC score (99.97%). LSTM and RNN models also show very good results, although slightly lower than those of CNN. Overall, these results confirm that all three models are able to provide very high levels of intrusion detection and make a significant contribution to the development of security solutions for future IoT systems.

Keywords*: intrusion detection, internet of things, convolutional neural network, long short-term memory, recurrent neural network*