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
Impact Factor: 7.67
Volume 5, Issue 7, March 2025

Performance Evaluation of Machine Learning Algorithms for IoT-Based Intrusion Detection

Siddhant Sheshrao Bharade, Sanskar Sahebrao Ghongade,
Amol Ramji Paratkar, Prof. Rajeshri P. Mane
Department of Electronics and Telecommunication,
JSPM'S RSCOE, Tathawade, Pune, India
siddhantbharade02@gmail.com, sanskarghongade0526@gmail.com
amolparatkar284@gmail.com, rpmane_entc@jspmrscoe.edu.in

Abstract: *With the rapid growth of the Internet of Things (IoT), the security of connected devices and networks has become a serious issue. IoT networks are exposed to various cyber-attacks because of their distributed nature and lack of security mechanisms. This paper introduces a machine learning-based solution for identifying IoT-specific attacks using the Multi-Layer Perceptron (MLP) classifier. The RT-IoT2022 dataset with benign and adversarial network activities was used for experimentation. This dataset combines real IoT traffic from devices such as ThingSpeak-LED, Wipro-Bulb, and MQTT-Temp and simulated attacks such as SSH brute-force, DDoS (Hping and Slowloris), and Nmap scanning. Preprocessing of the dataset was carried out to manage missing values, scale feature ranges, and filter out apt features for model training. MLP classifier, being a feedforward neural network artificial system, was implemented and trained upon the filtered dataset to segregate normal versus malicious network activity. Accuracy, precision, recall, F1-score, and confusion matrix metrics were utilized for comparison to establish how well the model performs. High detection precision showed that the proposed method indicated how the model has the potential to learn advanced network traffic patterns. The research draws attention to the significance of cognitive machine learning algorithms in enhancing IoT networks' robustness against cyber attacks. Drawing on the capacity for learning associated with neural networks, the MLP classifier offers an efficient yet efficient solution for intrusion detection in real-time. The findings of the research can facilitate the development of adaptive security mechanisms that can promptly react to adaptive threats in IoT environments.*

Keywords: IoT Security, Intrusion Detection System (IDS), Machine Learning, Multi-Layer Perceptron (MLP), RT-IoT2022 Dataset, Cyber-Attack Detection, DDoS, Brute-Force Attack, Neural Networks, Network Traffic Analysis