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 3, Issue 3, June 2023
Impact Factor: 7.301

Deep Learning-Based Fault Prediction Models for Enhanced Network Security Monitoring

Mahathi Kari
Independent Researcher
mahathikari2026@gmail.com

Abstract: *The challenge related to the security of the network operations and their reliability has gained a particular significance in the era of growing Internet of Things (IoT) ecosystems in the impact of the growing risk of cyberattacks and the system functioning collapse. The present paper describes a Deep Neural Network (DNN)-based fault prediction system that serves to complement network security monitoring by effectively detecting faults in the work of IoT network traffic. The IoT-23 dataset, a realistic and differentiated test, is used in the article. It contains both benign and malicious traffic samples. Several data preparation procedures, including cleaning, normalization, label encoding, and feature extraction, were carried out in order to optimize the model's performance. The DNN model was estimated and evaluated using common measures such as accuracy (acc), precision (pre), recall (rec), and F1-score (F1) which are calculated based on the confusion matrix. It has been experimentally verified that the proposed DNN performs better than Support Vector Machine (SVM), Naive Bayes (NB), and AdaBoost (ADA) with acc of 98.69%, 98% pre- and post-recall, and high F1. These results illustrate the power and magnitude of deep learning (DL) algorithms in fault prediction to reduce the number of false alarms, increase the detection capability, and better monitoring of the security of IoT networks.*

Keywords: Cybersecurity, Machine Learning, Network Security, Internet of Things, Fault, Machine Learning