Optimizing Lightweight Machine Learning-Based Intrusion Detection Systems for Secure IoT Networks

Abstract

The rapid growth of the Internet of Things (IoT) has increased cybersecurity challenges due to the diverse and resource-constrained nature of connected devices. Although machine learning (ML)-based intrusion detection systems (IDS) have shown promising performance, many existing approaches are computationally expensive and lack generalizability across different IoT environments. This research proposes a lightweight and optimized ML-based IDS framework that integrates feature selection, data balancing, and model optimization to improve intrusion detection while reducing computational overhead. The proposed framework will be evaluated using multiple benchmark IoT datasets, including UNSW-NB15, MQTT-IoT-IDS2020, and Bot-IoT, with cross-dataset validation to ensure robustness and practical applicability. The expected outcome is a scalable, resource-efficient, and reproducible IDS framework that enhances IoT security and supports the deployment of intelligent cybersecurity solutions in real-world environments.