MIDI 2024 Conference

Real-Time Anomaly Detection and Threat Classification in IIoT

Abstract

As the Industrial Internet of Things (IIoT) expands in scope and application, Cyber-Physical Systems (CPS) in industrial environments are increasingly vulnerable to cyber threats. This paper presents an integrated anomaly detection model by combining autoencoders with decision tree-based classification (AutoDTClass) to detect and mitigate cyberattacks in IIoT networks, a critical subset of CPS, through a data-driven approach using machine learning. The research utilises the Edge-IIoT dataset, which was selected for its comprehensive representation of industrial network attacks. The proposed model achieves high accuracy in anomaly detection, allowing the system to differentiate between cyber threats while adapting to new data patterns. Therefore it can improve anomaly detection accuracy in real-time IIoT environments, contributing to a resilient security layer for CPS amidst increasing operational complexity.