044
ENGR

Enhancing IoT Cybersecurity with AI-Enabled Zero Trust: The Integration of Reinforcement Learning for Adaptive Threat Detection and Response

Abstract

This research presents an AI-powered zero-trust framework that employs reinforcement learning (RL) instead of standard deep learning to address the increasing cybersecurity concerns in Internet of Things (IoT) networks. RL is selected for its flexible adaptability and capacity to respond in real-time, resulting in a 5% enhancement in accuracy for detecting threats and a substantial decrease in computational workload.

The system leverages the continuous updating capability of RL to adapt security measures in response to real-time feedback, so harmonizing with the continuous verification premise of the zero-trust paradigm. This methodology improves the identification of intricate and nuanced attack patterns and facilitates proactive vulnerability detection, hence enhancing both the security and privacy of IoT networks.

We showcase the efficacy of the framework in identifying and mitigating sophisticated cyber threats by utilizing simulations and real-world examples. This confirms the benefits of combining AI-powered zero trust with reinforcement learning in the field of IoT cybersecurity. This research provides comprehensive theoretical and practical knowledge, emphasizing the potential of Reinforcement Learning (RL) in improving the security of Internet of Things (IoT) networks.