Enhancing Security in Cyber-Physical Systems through AI

Pat Nelson
PhD
California Institute of Technology
1200 E California Blvd, Pasadena, CA 91125, USA

Riley White
PhD
ETH Zurich
Rämistrasse 101, 8092 Zürich, Switzerland

Cameron Thomas
PhD
National University of Singapore
21 Lower Kent Ridge Rd, Singapore 119077

Abstract. In this paper, we propose an AI-based framework to enhance the security of cyber-physical systems. By employing advanced machine learning techniques, our approach detects and mitigates potential threats in real-time, ensuring the integrity and reliability of these systems. Experimental results demonstrate the framework's effectiveness in safeguarding critical infrastructures against cyber threats.

Keywords: Cyber-Physical Systems, AI Security, Machine Learning, Threat Detection, Infrastructure Protection

Introduction

The proliferation of cyber-physical systems (CPS) in critical infrastructure sectors, such as energy and transportation, necessitates robust security measures to protect against cyber threats. This paper introduces an AI-based framework designed to enhance the security of CPS by leveraging machine learning to identify and mitigate risks in real-time. Our framework is evaluated through extensive experiments, highlighting its capability to detect potential threats and respond promptly to safeguard system integrity. The results underscore the importance of integrating AI into CPS security strategies, offering a proactive approach to managing cyber threats and ensuring system reliability.

References

1. Kumar, N., & Kataria, V. Enhanced Sentiment Classification using a Multi-layered Stacked Ensemble Architecture.
2. Рагимов, Э. Р. О. (2011). Метрология элементов безопасности программных комплексов, реализующих систему защиты информации корпоративных сетей. Вопросы защиты информации, (2), 36-41.