Chapter 3
Generative AI for Cybersecurity and Privacy in Cyber-Physical Systems

Arul Kumar Natarajan
https://orcid.org/0000-0002-9728-477X
Samarkand International University of Technology, Uzbekistan

Yash Desai
Ramrao Adik Institute of Technology, India

Pravin R. Kshirsagar
J.D. College of Engineering and Management, India

Kamal Upreti
https://orcid.org/0000-0003-0665-530X
Christ University, India

Tan Kuan Tak
Singapore Institute of Technology, Singapore

ABSTRACT

With the proliferation of Cyber-Physical Systems (CPS) across various domains, ensuring robust cybersecurity and privacy has become increasingly critical. Generative Artificial Intelligence (AI) presents innovative approaches to enhancing the security and privacy of these systems. This book chapter explores the intersection of Generative AI with cybersecurity and privacy within CPS environments. It examines how Generative AI techniques, such as Generative Adversarial Networks

DOI: 10.4018/979-8-3693-5728-6.ch003

(GANs) and Variational Autoencoders (VAEs), can be leveraged to detect and mitigate cyber threats and vulnerabilities while protecting sensitive data and user privacy. The chapter provides an overview of CPS, addressing its unique security and privacy challenges, and demonstrates the practical application of Generative AI through a case study on phishing detection using BERT-based sequence classification. The experimental results highlight the effectiveness of Generative AI in strengthening CPS security.

INTRODUCTION

Background and Motivation

Cyber-Physical Systems (CPS) are becoming increasingly integral across various sectors, including industrial automation, healthcare, transportation, and smart cities. These systems combine physical processes with digital computation and communication, creating intricate interactions between the physical world and computational algorithms. Jeffrey et al. (2023) thoroughly review anomaly detection strategies for Cyber-Physical Systems (CPS). Their examination of 296 studies identifies key challenges, including resource limitations and the absence of standardized protocols, and offers solutions to improve CPS security in the face of emerging threats. Sharma et al. (2023) present a hybrid deep learning approach combining Convolutional Neural Networks (CNNs) and Bidirectional LSTM for detecting denial of service attacks in Cyber-Physical Systems (CPS). Their model addresses the limitations of traditional intrusion detection systems by classifying network traffic flows as benign or malicious with improved accuracy, focusing on smart healthcare networks. Bashendy, Tantawy, and Erradi (2023) review intrusion response systems for Cyber-Physical Systems (CPS), focusing on their taxonomy, countermeasures, and architectures. The paper also covers recent Reinforcement Learning (RL) advancements for IRS and identifies future research directions.

The importance of CPS lies in its ability to enhance operational efficiency, improve safety, and enable advanced functionalities. However, as CPS becomes more pervasive, it faces escalating cybersecurity and privacy challenges. Threats such as unauthorized access, data breaches, and malicious attacks pose significant risks to the integrity and confidentiality of these systems. Addressing these concerns is crucial for ensuring the reliable operation of CPS and protecting sensitive data from potential threats.

Selection of Representative Feature Training Sets With Self-Organized Maps for Optimized Time Series Modeling and Prediction: Application to Forecasting Daily Drought Conditions With ARIMA and Neural Network Models

Elizabeth McCarthy, Ravinesh C. Deo, Yan Liand Tek Maraseni (2018). *Handbook of Research on Predictive Modeling and Optimization Methods in Science and Engineering (pp. 446-464).*

www.irma-international.org/chapter/selection-of-representative-feature-training-sets-with-self-organized-maps-for-optimized-time-series-modeling-and-prediction/206761