River Publishers

Security and Privacy of Cyber-Physical Systems

Emerging Trends, Technologies, and Applications

Editors:

Agbotiname Lucky Imoize, University of Lagos, Nigeria

Webert Montlouis, Johns Hopkins University, USA

Segun I. Popoola, Anglia Ruskin University, United Kingdom

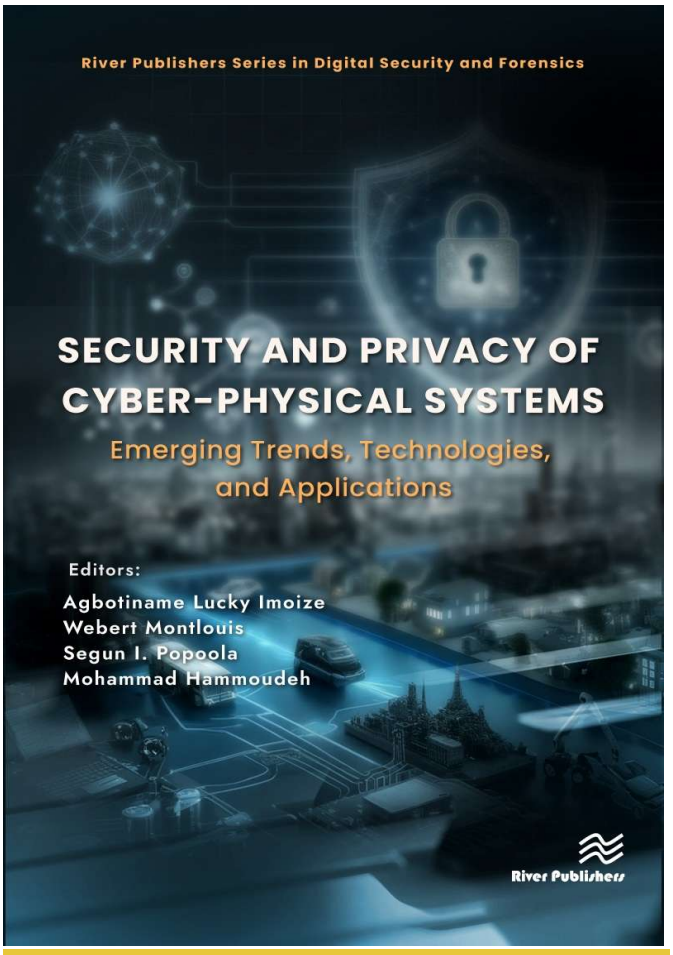
Mohammad Hammoudeh, King Fahd University of Petroleum and Minerals, Saudi Arabia.

This book examines vulnerability threats and attack detection and mitigation, including the associated legal requirements, regulatory frameworks, and policies for enabling the security and privacy of cyber-physical systems. It provides researchers, academics, and practitioners with new insights into the real-world scenarios of deploying, applying, and managing security and privacy frameworks in modern cyber-physical systems.

It addresses critical security and privacy concerns, including theoretical analysis, novel system architecture design and implementation, vulnerability discovery, analysis, mitigation, emerging application scenarios, experimental frameworks, and social and ethical dilemmas affecting all parties in cyber-physical systems. The book is an ideal reference for practitioners and researchers in cyber-physical systems, security and privacy, the Internet of Things, advanced cryptography, cyber defensive walls, industrial systems, and cyber threats. It is also a suitable textbook for graduate and senior undergraduate courses in these subjects.

TABLE OF CONTENTS

1 Overview of security and privacy in cyber-physical systems: Emerging Trends and Strategies.
2 Protection and fault diagnostics in legacy cyber-physical systems.
3 Explainable Artificial Intelligence for Intrusion Detection in Cyber-Physical Systems.
4 Addressing security and privacy issues in cyber-physical systems.
5 Physical Layer Security of 6G Vehicle Visible Light Communications for Cyber-Physical Systems.
6 Hardware security and privacy for cyber-physical systems.
7 A Secure Biometric Authentication Architecture for Blockchain-Driven Cyber-Physical Systems.
8 Secure IoT-Based Smart Wheelchair System: From Implementation to Security Enhancement Strategy.
9 Statistical Estimation of User Location Distribution via Anonymized Dummy Data Transmission.
10 Emerging security and privacy schemes for cyber-physical systems.
11 Security and Privacy Concerns and Risks in Modern Cyber-Physical Systems.
12 The Ethics of Security and Privacy of Cyber-physical Systems: Emerging Trends, Technology and Applications.
13 Intrusion Detection Techniques for Cyber-Physical Systems.
14 Cyber-Physical Systems: Strategies for Enhancing Availability, Recovery, and Auditing for Optimal Performance.
15 Legal Framework and Regulatory Policies for Cyber-Physical Systems.
16 Blockchain-based security and privacy solutions for cyber-physical systems.
17 Privacy-Utility Trade-offs in IoT Networks: A Comparative Analysis of Differential Privacy Mechanisms for Sensor Data Aggregation.
18 Enhancing Cyber-Physical Systems Through Artificial Intelligence and Machine Learning.
19 Case Studies on the Security and Privacy of Cyber-physical Systems.
20 Recent advances and the future of cyber-physical systems.



River Publishers Series in Digital Security and Forensics

ISBN: 9788743801290
e-ISBN: 9788743806738
Available From: October 2025
Price: $ 150.00

KEYWORDS:
Cyber-Physical Systems; Security and Privacy; Cyber resilience; Machine Learning; Internet of Things; Cryptography; Cyber threats; Cyber defensive walls; Threat intelligence; Industrial systems.

www.riverpublishers.com
marketing@riverpublishers.com