River Publishers

Intelligent Cybersecurity and Resilience for Critical Industries: Challenges and Applications

Editors:

Mounia Zaydi, ICL, Junia, Université catholique de Lille, LITL, France

Yassine Maleh, Sultan Moulay Slimane University, Beni Mellal, Morocco

Gabriel Chênevert, ICL, Junia, Université catholique de Lille, LITL, France

Hayat Zaydi, National Superior School of Mines (ENSMR), Rabat, Morocco

Amina El Yaagoubi, ICL, Junia, Université catholique de Lille, LITL, France

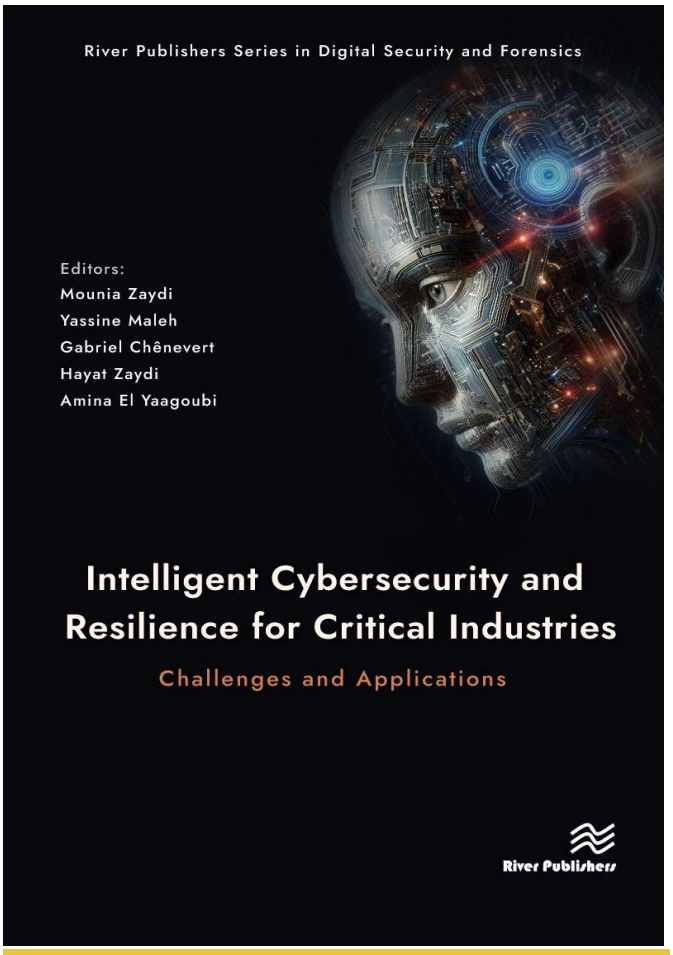
Intelligent Cybersecurity and Resilience for Critical Industries: Challenges and Applications thoroughly explores cybersecurity principles, strategies, and technologies crucial for protecting digital assets and combating evolving cyber threats in critical industries. This book provides indispensable guidance in fortifying cyber defenses for critical infrastructures. Each chapter offers invaluable insights into proactive defense measures, from AI-driven threat management in healthcare systems to practical applications of AI for cyber risk management in critical infrastructures. Unraveling the complexities of contemporary cyber threats, this book empowers readers with the knowledge and tools needed to navigate the intricate landscape of cybersecurity effectively. Through a multidisciplinary approach spanning AI, machine learning, and advanced technologies, it addresses the urgent challenges organizations encounter in securing their digital infrastructure and safeguarding sensitive data from malicious cyber-attacks.
Technical topics discussed in the book include:

- AI-driven strategies for advanced malware detection and prevention
- Hybrid deep learning techniques for precise malware classification
- Machine learning applications tailored to IoT security challenges
- Comprehensive exploration of blockchain techniques enhancing IoT security and privacy
- Practical integration of security analysis modules for proactive threat intelligence.

Designed as an essential reference, this book caters to students, researchers, cybersecurity professionals, and individuals keen on comprehending and tackling contemporary cyber defense and risk assessment challenges. It serves as a valuable resource for enhancing cybersecurity awareness, knowledge, and practical skills in critical industries.

TABLE OF CONTENTS

Part I: Intelligent Cybersecurity and Resilience: Challenges and Applications
Chapter 1 AI-Driven Threat Management in Healthcare Systems
Chapter 2 Practical Use of AI for Cyber Risk Management in Critical Infrastructures: A Review
Chapter 3 Fraud Detection in Decentralized Autonomous Organization (DAO) with Machine Learning
Chapter 4 Improving Machine Learning Performance Using Sampling Techniques for COVID-19 Imbalanced Data
Part II: Cybersecurity Challenges and Resilience in Healthcare and Industrial Domains
Chapter 5 Penetration Testing in Operations Technology and SCADA Environments
Chapter 6 Cyber-attacks in Healthcare: Analyzing Recent Trends and Preventive Measures
Chapter 7
Enhancing Cyber Resilience: A Study of Red Teaming within Operational Technology Domains
Chapter 8 Demystifying the Role of Publicly Available Up-to-date Benchmark Intrusion Datasets: A Case Study of Web Security
Part III: Advanced Technologies for Cybersecurity and Privacy
Chapter 9 Advancing Blockchain Privacy: The Role of Homomorphic Encryption
Chapter 10 Developing a Big Data Infrastructure: Integral Modules and Best Procedures for Alleviating Security and Privacy Challenges
Chapter 11 Evaluation of the Performance of Pattern Search and Genetic Algorithms for Enhancing the Lifetime of WSNs



River Publishers Series in Digital Security and Forensics

ISBN: 9788770042260
e-ISBN: 9788770042253
Available From: April 2025
Price: $ 140.00

KEYWORDS:
Intelligent cybersecurity, cyber resilience, cyber risk management, critical industries, artificial intelligence (AI), machine learning, pentesting, red teaming

www.riverpublishers.com
marketing@riverpublishers.com