

1. Record Nr.	UNINA9911035060803321
Autore	Ananthajothi K
Titolo	Securing Cyber-Physical Systems : Fundamentals, Applications and Challenges
Pubbl/distr/stampa	Newark : , : John Wiley & Sons, Incorporated, , 2025 ©2025
ISBN	1-394-28775-5 1-394-28776-3 1-394-28774-7
Edizione	[1st ed.]
Descrizione fisica	1 online resource (399 pages)
Collana	Industry 5. 0 Transformation Applications Series
Altri autori (Persone)	SangeethaaS. N DivyaD PalamurukanCa PengSheng-Lung
Disciplina	005.8
Soggetti	Computer security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Cover -- Series Page -- Title Page -- Copyright Page -- Contents -- Preface -- Chapter 1 Enhancing Safety and Security in Autonomous Connected Vehicles: Fusion of Optimal Control With Multi-Armed Bandit Learning -- 1.1 Background -- 1.1.1 Problem Statement -- 1.1.2 Motivation -- 1.2 Related Works -- 1.2.1 Contributions -- 1.2.2 Centralized CRN Scheduling -- 1.2.3 Multi-Armed Bandit (MAB) -- 1.2.4 Bandit Learning with Switching Costs -- 1.3 System Model -- 1.3.1 Resource Spectrum -- 1.3.2 CRs' Spectrum Utilization Schemes -- 1.3.3 CBS Scheduling -- 1.3.4 PUs' Activity -- 1.4 Outcomes -- 1.4.1 Scenario I: Fallen Traffic Signs -- 1.4.2 Scenario II: Traffic Signs Alert by the Road Workers -- 1.4.3 Scenario III: Back/Rotated Traffic Sign Across the Road -- 1.4.4 Scenario IV: Hacking of a Stop Sign at a Four-Way Stop Intersection -- 1.5 Conclusions and Future Enhancement -- 1.5.1 Conclusions -- 1.5.2 Future Directions -- References -- Chapter 2 Secure Data Handling in AI and Proactive Response Network: Create a Physical Layer-Proposed Cognitive Cyber-Physical Security -- 2.1 Introduction -- 2.1.1 The Role of AI in

Cybersecurity -- 2.1.2 Usage of CCPS in IoT -- 2.2 Challenges and Mechanisms -- 2.2.1 Brief Account of Challenges Faced -- 2.2.2 Innovative Mechanisms -- 2.3 Using AI to Support Cognitive Cybersecurity -- 2.3.1 Cognitive Systems -- 2.3.2 AI in IoT -- 2.4 Create a Physical Layer-Proposed CCPS -- 2.4.1 Create a Physical Layer-Proposed CCPS in Healthcare Application -- 2.4.1.1 Privacy-Aware Collaboration -- 2.4.1.2 Cycle Model of CCPS -- 2.4.1.3 Dynamic Security Knowledge Base -- 2.4.2 Method for Secure Data Handling -- 2.5 Road Map of Implementation -- 2.5.1 AI for CCPS-IoT -- 2.5.2 AI-Enabled Wireless CCPS-IoT to Provide Security -- 2.6 Conclusions and Future Enhancement -- Future Directions -- References.

Chapter 3 Intelligent Cognitive Cyber-Physical System-Based Intrusion Detection for AI-Enabled Security in Industry 4.0 -- 3.1 Introduction -- 3.1.1 Cyber-Physical Systems -- 3.1.2 Intelligent Cyber-Physical Systems (ISPS) -- 3.1.3 Cognitive Cyber-Physical Systems (CCPS) -- 3.1.4 IDS in Industry 4.0 Using iCCPS -- 3.1.5 AI in iCCPS-IDS -- 3.2 Problem Statement -- 3.3 Motivation -- 3.4 Research Gap -- 3.5 Methodology -- 3.5.1 Training Dataset -- 3.5.2 Information for Assessment and Instruction -- 3.5.3 Model -- 3.5.4 CPS Determined by Cognition Agents -- 3.5.5 Useful Implementation of the Actual Device -- 3.6 Importance and Impact of AI-Based Intrusion Detection in iCCPS in Industry 4.0 -- 3.6.1 Need -- 3.6.2 Challenges -- 3.7 Conclusions and Future Directions -- Future Directions -- References -- Chapter 4 Resilient Cognitive Cyber-Physical Systems: Conceptual Frameworks, Models, and Implementation Strategies -- 4.1 Introduction -- 4.1.1 Problem Statement -- 4.1.2 Motivation -- 4.2 Materials and Methods -- 4.3 CCPS Design Challenges -- 4.4 Cyber-Physical Systems Principles and Paradigms -- 4.4.1 CCPS Conceptual Framework -- 4.4.2 CCPS Modeling -- 4.4.3 Other Modeling Issues in CCPS -- 4.5 Conclusions and Future Enhancements -- 4.5.1 Future Enhancements -- References -- Chapter 5 Cognitive Cyber-Physical Security Challenges, Issues, and Recent Trends Over IoT -- 5.1 Introduction -- 5.1.1 From IoT to CCPS-IoT -- 5.1.2 Fundamental Cognitive Tasks -- 5.2 Motivation and Challenges -- 5.2.1 Motivation -- 5.2.2 Challenges -- 5.3 Security -- 5.3.1 Physical Layer Attacks -- 5.3.2 Physical Layer Security -- 5.3.3 Main Constituents -- 5.4 Research Gap -- 5.5 An Automatic Security Manager for CCPS Using IoT -- 5.5.1 Combatting Erroneous Estimations -- 5.5.2 Detection and Classification -- 5.6 Conclusions and Future Enhancement -- Future Enhancement -- References.

Chapter 6 Cognitive Cyber-Physical Security With IoT: A Solution to Smart Healthcare System -- 6.1 Introduction -- 6.1.1 Motivation -- 6.1.2 Need and Contribution -- 6.1.2.1 Need -- 6.1.2.2 Contribution -- 6.2 Medical CCPS with IoT -- 6.2.1 IoT Device for AI Solution -- 6.2.2 Traditional Bio-Modality Spoofing Detection -- 6.2.3 MCPS Using AI Device -- 6.3 Functional and Behavioral Perspectives -- 6.4 Modeling and Verification Methods of MCPS -- 6.4.1 MCPS Modeling Based on ICE -- 6.4.2 MCPS Modeling Based on Component -- 6.5 Artificial Intelligence for Cognitive Cybersecurity -- 6.5.1 Privacy-Aware Collaboration -- 6.5.2 Cognitive Security Cycle Model -- 6.6 Conclusions and Future Direction -- 6.6.1 Conclusions -- 6.6.2 Future Directions -- References -- Chapter 7 Cognitive Cyber-Physical Security with IoT and ML: Role of Cybersecurity, Threats, and Benefits to Modern Economies and Industries -- 7.1 Introduction -- 7.1.1 Key Contributions -- 7.1.2 Problem Statement -- 7.1.3 Motivation -- 7.2 CCPS Associated with IoT -- 7.2.1 Reasons in Favor of Cognitive Analytics -- 7.2.2 Analyses of Current Cyber Risk Data -- 7.3 Materials

and Methods -- 7.3.1 Role of Cybersecurity in CCPS with IoT and ML -- 7.3.2 ML in Cognitive Cyber-Physical Security with IoT -- 7.3.3 Threats to Modern Economies and Industries -- 7.3.4 Benefits to Modern Economies and Industries -- 7.4 Outcomes -- 7.4.1 AI-Enabled Management Technology and Approach Taxonomy -- 7.4.2 Essential Self-Adapting System Technologies -- 7.4.3 Attack Malware Classifier -- 7.5 Conclusions and Future Direction -- Future Directions -- References -- Chapter 8 A Safety Analysis Framework for Medical Cyber-Physical Systems Using Systems Theory -- 8.1 Introduction -- 8.2 Background -- 8.2.1 Cyber-Physical Systems -- 8.2.2 Quality-of-Service Issues in CPS -- 8.2.3 Medical Cyber-Physical Systems. 8.3 The Systems-Based Safety Analysis Observation for MCPS -- 8.3.1 Identification of Critical Requirements in MCPS -- 8.3.2 A Systems Theory-Based Method for Safety Analysis in Medical Cyber-Physical Systems -- 8.3.3 MCPS in Patient-Controlled Analgesia -- 8.4 Improved Wireless Medical Cyber-Physical System (IWMCPs) -- 8.4.1 Level: Data Acquisition -- 8.4.2 Layer: Data Aggregating -- 8.4.3 Level: Storing -- 8.4.4 Level: Action -- 8.4.5 IWMCPs Architectural Research -- 8.4.6 Core of Communications and Sensors -- 8.5 Hazard Analysis on PCA-MCPS -- 8.5.1 System Safety Constraint -- 8.5.2 System Safety Control Structure -- 8.5.3 Identify Unsafe Control Actions -- 8.5.4 Specifying Causes -- 8.6 Conclusions and Future Directions -- Future Directions -- References -- Chapter 9 Cognitive Cybersecurity and Reinforcement Learning: Enhancing Security in CPS-IoT Enabled Healthcare -- 9.1 Introduction -- 9.2 Methodology -- 9.2.1 Device AI Solutions -- 9.2.2 Detect the Spoofing of Bio-Modality -- 9.2.3 Detect the Spoofing of Bio-Modality Using Machine Learning -- 9.3 Challenges and Mechanisms -- 9.3.1 Challenges -- 9.3.2 Innovative Mechanisms -- 9.4 Cognitive Cyber-Physical Systems and Reinforcement Learning -- 9.4.1 Model Formulation -- 9.4.2 AI in CCPS -- 9.4.2.1 Privacy-Aware Collaboration -- 9.4.2.2 Cognitive Security Cycle Model -- 9.4.2.3 Need -- 9.4.2.4 Cross-Sectoral Techniques -- 9.4.2.5 Actuation and Data Collection -- 9.5 Conclusions and Future Directions -- 9.6 Future Directions -- References -- Chapter 10 Navigating the Digital Landscape: Understanding, Detecting, and Mitigating Cyber Threats in an Evolving Technological Era -- 10.1 The Digital Transformation: Shaping Modern Business Dynamics -- 10.2 Impact of COVID-19: Accelerating the Digital Shift -- 10.3 Online Safety Concerns: Navigating the Digital Landscape. 10.4 Interplay of Digital Technologies: Vulnerabilities and Threats -- 10.4.1 Introduction to Digital Technologies -- 10.4.2 Case Studies and Examples -- 10.5 Rise of Cyber Assaults as a Service: Automating Criminal Activities -- 10.6 Evolving Threat Landscape: Understanding Modern Cyber Attacks -- 10.7 Beyond Conventional Security Measures: The Need for Advanced Defense -- 10.8 Rise of Cyber Assaults as a Service: Automating Criminal Activities -- 10.8.1 Introduction to Cyber Assaults as a Service -- 10.8.2 Automation of Criminal Activities -- 10.8.3 Impact and Implications -- 10.9 Evolving Threat Landscape: Understanding Modern Cyber Attacks -- 10.9.1 Types of Modern Cyber Attacks -- 10.9.2 Implications for Cybersecurity Defense -- 10.10 Beyond Conventional Security Measures: The Need for Advanced Defense -- 10.10.1 Challenges with Conventional Security Measures -- 10.10.2 The Evolution of Advanced Defense -- 10.11 Uncovering Cyber Threats: Patterns, Trends, and Detection Methods -- 10.11.1 Patterns of Cyber Threats -- 10.12 Addressing Advanced Persistent Threats: Challenges and Solutions -- 10.12.1 Introduction to Advanced Persistent Threats (APTs) -- 10.12.2 Challenges Posed by APTs -- 10.12.3 Solutions for Addressing APTs -- References -- Chapter 11

Defense Strategies for Cyber-Physical Systems -- 11.1 Introduction -- 11.2 Threat Landscape in CPS -- 11.3 Advanced Defense Strategies -- 11.3.1 Anomaly Detection in CPS -- 11.3.2 Secure Communication Protocols -- 11.3.3 Machine Learning-Driven Defenses -- 11.3.4 Zero Trust Model for CPS -- 11.3.5 Resilience Techniques for CPS -- 11.3.6 Intensive Training and Awareness -- 11.3.7 Conclusion and Future Directions -- References -- Chapter 12 Cybersecurity in the Era of Artificial Intelligence: Challenges and Innovations -- 12.1 Introduction to Cybersecurity Analysis -- 12.2 Need for AI in Cybersecurity. 12.3 Current Cybersecurity Techniques.

Sommario/riassunto

Protect critical infrastructure from emerging threats with this essential guide, providing an in-depth exploration of innovative defense strategies and practical solutions for securing cyber-physical systems.
