1.

Record Nr.	UNINA9911020227803321
Autore	Naveen Palanichamy
Titolo	Digital Twins and Cybersecurity : Safeguarding the Future of Connected Systems
Pubbl/distr/stampa	Newark : , : John Wiley & Sons, Incorporated, , 2025 ©2025
ISBN	9781394272488 1394272480 9781394272501 1394272502 9781394272495 1394272499
Edizione	[1st ed.]
Descrizione fisica	1 online resource (503 pages)
Collana	Next-generation computing and communication engineering
Altri autori (Persone)	MaheswarR RagupathyU. S
Disciplina	003/.3
Soggetti	Digital twins (Computer simulation) 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 -- Acknowledgments -- Chapter 1 Introduction -- 1.1 Introduction to the Concept of Digital Twins and Cybersecurity -- 1.2 Significance of Integrating Digital Twins and Cybersecurity -- 1.2.1 Protection of Physical Assets -- 1.2.2 Mitigation of Operational Risks -- 1.2.3 Prevention of Data Breaches -- 1.2.4 Prevention of Cyber-Physical Attacks -- 1.2.5 Facilitation of Trust and Adoption -- 1.2.6 Compliance with Regulations and Standards -- 1.2.7 Future-Proofing and Resilience -- 1.2.8 An Overview of the Book's Structure and Content -- Chapter 2 Understanding Digital Twins -- 2.1 Definition of Digital Twins -- 2.2 Evolution of Digital Twins -- 2.3 Various Types of Digital Twins -- 2.3.1 Product Digital Twins -- 2.3.2 Process Digital Twins -- 2.3.3 System Digital Twins -- 2.3.4 Human Digital Twins -- 2.4 Applications in Different Industries -- 2.4.1 Manufacturing Industry -- 2.4.2 Healthcare Industry -- 2.4.3 Energy and Utilities Industry --

2.4.4 Transportation Industry -- Chapter 3 The Importance of Cybersecurity -- 3.1 Growing Threats in the Digital Landscape -- 3.1.1 Impact and Consequences -- 3.1.2 Emerging Threats -- 3.2 Significance of Cybersecurity in Protecting Digital Twins -- 3.2.1 Introduction to Digital Twins and Cybersecurity -- 3.2.2 Best Practices for Cybersecurity in Protecting Digital Twins -- 3.3 Potential Consequences of Cyberattacks on Digital Twins -- 3.3.1 Case Studies and Examples -- 3.3.2 Mitigating the Consequences -- Chapter 4 Digital Twin Architecture -- 4.1 Key Components and Infrastructure of Digital Twins -- 4.1.1 Data Collection and Sensors -- 4.1.2 Communication Networks -- 4.1.3 Data Storage and Processing -- 4.1.4 Modeling and Simulation Engines -- 4.1.5 Visualization and User Interface -- 4.1.6 Analytics and Decision Support.

4.1.7 Integration with Physical Systems -- 4.1.8 Cybersecurity Infrastructure -- 4.1.9 Scalable and Resilient Architecture -- 4.1.10 Data Governance and Standards -- 4.2 Data Flow and Communication Channels -- 4.2.1 Data Collection -- 4.2.2 Data Transmission -- 4.2.3 Data Pre-Processing -- 4.2.4 Data Storage -- 4.2.5 Data Processing and Analysis -- 4.2.6 Simulation and Optimization -- 4.2.7 Visualization and User Interfaces -- 4.2.8 Control and Actuation -- 4.2.9 Feedback and Iteration -- 4.2.10 Cybersecurity Considerations -- 4.3 Vulnerabilities and Security Considerations in the Architecture -- 4.3.1 Data Collection and Sensors -- 4.3.2 Communication Networks -- 4.3.3 Data Storage and Processing -- 4.3.4 Integration with Physical Systems -- 4.3.5 Visualization and User Interfaces -- 4.3.6 Third-Party Integrations -- 4.3.7 Insider Threats -- 4.3.8 Scalability and Resilience -- 4.3.9 Continuous Monitoring and Incident Response -- 4.3.10 Compliance and Standards -- Chapter 5 Cybersecurity Framework for Digital Twins -- 5.1 Introduction -- 5.1.1 Risk Assessment and Threat Modeling -- 5.1.2 Secure Architecture Design -- 5.1.3 Identity and Access Management -- 5.1.4 Data Security and Privacy -- 5.1.5 Secure Communication Channels -- 5.1.6 Vulnerability Management -- 5.1.7 Incident Response and Recovery -- 5.1.8 Continuous Monitoring and Threat Intelligence -- 5.1.9 Security Awareness and Training -- 5.1.10 Third-Party Risk Management -- 5.2 Key Principles and Best Practices -- 5.2.1 Defense in Depth -- 5.2.2 Least Privilege -- 5.2.3 Secure Configuration -- 5.2.4 Patch Management -- 5.2.5 Secure Development Life Cycle -- 5.2.6 Continuous Monitoring -- 5.2.7 Encryption -- 5.2.8 Access Control -- 5.2.9 Incident Response -- 5.2.10 Employee Awareness and Training -- 5.2.11 Third-Party Risk Management -- 5.2.12 Compliance.

5.3 Guidelines for Implementing Security Measures -- 5.3.1 Establish a Security Policy -- 5.3.2 Implement Access Controls -- 5.3.3 Encrypt Data -- 5.3.4 Secure Network Infrastructure -- 5.3.5 Regularly Update and Patch Systems -- 5.3.6 Implement Monitoring and Logging -- 5.3.7 Conduct Regular Security Assessments -- 5.3.8 Establish an Incident Response Plan -- 5.3.9 Train Employees on Security Best Practices -- 5.3.10 Implement Vendor Risk Management -- 5.3.11 Regularly Review and Improve Security Measures -- Chapter 6 Securing Data in Digital Twins -- 6.1 Challenges of Securing Data Within Digital Twins -- 6.1.1 Data Privacy -- 6.1.2 Data Integrity -- 6.1.3 Data Access Control -- 6.1.4 Data Integration and Interoperability -- 6.1.5 Data Storage and Retention -- 6.1.6 Data Sharing and Collaboration -- 6.1.7 Data Governance and Compliance -- 6.1.8 Data Life Cycle Management -- 6.1.9 Insider Threats -- 6.1.10 Emerging Technologies and Risks -- 6.2 Encryption Techniques and Data Protection Mechanisms -- 6.2.1 Symmetric Encryption -- 6.2.2 Asymmetric Encryption -- 6.2.3 Hash Functions -- 6.2.4 Digital Signatures -- 6.2.5

Transport Layer Security (TLS) -- 6.2.6 Virtual Private Networks (VPNs) -- 6.2.7 Data Masking -- 6.2.8 Access Control and Authentication -- 6.2.9 Data Loss Prevention (DLP) -- 6.2.10 Secure Key Management -- 6.2.11 Data Backup and Disaster Recovery -- 6.2.12 Data Retention and Destruction -- 6.3 Strategies for Ensuring Data Integrity and Confidentiality -- 6.3.1 Encryption -- 6.3.2 Access Controls -- 6.3.3 Secure Key Management -- 6.3.4 Secure Data Transmission -- 6.3.5 Data Anonymization and Pseudonymization -- 6.3.6 Data Loss Prevention (DLP) -- 6.3.7 Regular Audits and Monitoring -- 6.3.8 Data Backup and Recovery -- 6.3.9 Data Retention and Destruction Policies -- 6.3.10 Employee Training and Awareness.

6.3.11 Vendor and Third-Party Management -- Chapter 7 Authentication and Access Control -- 7.1 Importance of Robust Authentication Mechanisms -- 7.1.1 Prevent Unauthorized Access -- 7.1.2 Protect Sensitive Information -- 7.1.3 Mitigate Password-Related Risks -- 7.1.4 Multi-Factor Authentication (MFA) -- 7.1.5 Protection Against Credential Theft -- 7.1.6 Compliance with Regulatory Requirements -- 7.1.7 Safeguarding Remote Access -- 7.1.8 User Accountability and Auditing -- 7.1.9 Enhancing Trust and User Confidence -- 7.1.10 Future-Proofing Security -- 7.2 Access Control Models and Techniques -- 7.2.1 Access Control Models -- 7.2.2 Access Control Techniques -- 7.2.3 Challenges and Considerations -- 7.3 Multi-Factor Authentication and Biometrics in Digital Twins -- 7.3.1 Multi-Factor Authentication -- 7.3.2 Biometrics -- Chapter 8 Threat Detection and Incident Response -- 8.1 Importance of Proactive Threat Detection -- 8.1.1 Early Threat Identification -- 8.1.2 Mitigating Financial Losses -- 8.1.3 Protecting Sensitive Data -- 8.1.4 Maintaining Business Continuity -- 8.1.5 Enhancing Incident Response Capabilities -- 8.1.6 Meeting Regulatory and Compliance Requirements -- 8.1.7 Strengthening Cybersecurity Posture -- 8.1.8 Gaining Situational Awareness -- 8.2 Techniques for Identifying Security Breaches in Digital Twins -- 8.2.1 Intrusion Detection Systems (IDS) -- 8.2.2 Log Analysis and Security Information and Event Management (SIEM) -- 8.2.3 Behavioral Analytics -- 8.2.4 Threat Intelligence -- 8.2.5 Anomaly Detection -- 8.2.6 Penetration Testing -- 8.2.7 User and Entity Behavior Analytics -- 8.2.8 Endpoint Detection and Response -- 8.3 Guidelines for Incident Response and Recovery -- Chapter 9 Securing Communication in Digital Twins -- 9.1 Introduction -- 9.1.1 Importance of Secure Communication Protocols.

9.1.2 Commonly Used Secure Communication Protocols -- 9.1.3 Encryption Algorithms -- 9.2 The Role of Secure Gateways and Firewalls -- 9.2.1 Traffic Monitoring and Filtering -- 9.2.2 Access Control and Policy Enforcement -- 9.2.3 Network Segmentation and Isolation -- 9.2.4 Threat Prevention and Intrusion Detection/Prevention -- 9.2.5 Virtual Private Network (VPN) Support -- 9.2.6 Application-Level Gateway and Proxy Services -- 9.2.7 Logging and Auditing -- 9.3 Importance of Network Segmentation and Isolation -- 9.3.1 Limiting Lateral Movement -- 9.3.2 Enhanced Security and Access Control -- 9.3.3 Compartmentalizing Sensitive Information -- 9.3.4 Compliance and Regulatory Requirements -- 9.3.5 Containment of Security Incidents -- 9.3.6 Improved Performance and Availability -- 9.3.7 Simplified Network Management -- Chapter 10 Privacy Considerations -- 10.1 Privacy Challenges Associated with Digital Twins -- 10.1.1 Data Collection and Retention -- 10.1.2 Informed Consent and Transparency -- 10.1.3 Data Ownership and Control -- 10.1.4 Data Security and Unauthorized Access -- 10.1.5 Data Anonymization and De-Identification -- 10.1.6 Cross-Border Data Transfer -- 10.1.7 Algorithmic Transparency and Bias -- 10.2 Privacy

Regulations and Compliance Requirements -- 10.2.1 General Data Protection Regulation -- 10.2.2 California Consumer Privacy Act -- 10.2.3 Personal Information Protection and Electronic Documents Act -- 10.2.4 Health Insurance Portability and Accountability Act -- 10.2.5 Personal Data Protection Act -- 10.2.6 Australian Privacy Principles -- 10.2.7 Cross-Border Data Transfer Mechanisms -- 10.3 Recommendations for Ensuring Privacy in Digital Twin Deployments -- 10.3.1 Privacy by Design -- 10.3.2 Data Minimization and Purpose Limitation -- 10.3.3 Informed Consent -- 10.3.4 Data Security -- 10.3.5 Anonymization and De-Identification.
10.3.6 Transparency and Individual Rights.

Sommario/riassunto

This book serves as a comprehensive guide to understanding the complex relationship between digital twins and cybersecurity, providing practical strategies for safeguarding connected systems. This book explores the convergence of digital twins and cybersecurity, offering insights, strategies, and best practices for safeguarding connected systems. It examines the definition, evolution, types, and applications of digital twins across industries like manufacturing, healthcare, and transportation. Highlighting growing digital threats, it underscores the need for robust cybersecurity measures to protect the integrity and confidentiality of digital twin ecosystems. The book analyzes key components and infrastructure of digital twins, including data flow, communication channels, vulnerabilities, and security considerations. It also addresses privacy challenges and explores relevant regulations and compliance requirements. Guiding readers through implementing security measures, it presents a comprehensive cybersecurity framework, covering data protection, encryption, and strategies for ensuring data integrity and confidentiality. It also explores incident response and recovery, secure communication protocols, and the roles of gateways and firewalls. Industry-specific challenges and mitigation strategies are examined through real-world case studies, offering valuable insights and lessons learned. Emerging trends in digital twin technology are thoroughly explored, including the impact of advancements such as AI and quantum computing and their associated cybersecurity challenges and solutions. Audience This book is an essential resource for professionals in the fields of cybersecurity and industrial and infrastructure sectors, including manufacturing, healthcare, transportation, and other industries that utilize digital twins. Researchers in computer science, cybersecurity, engineering, and technology, as well as policymakers and regulatory bodies, will also find this book highly useful.