

Securing the Digital Supply Chain

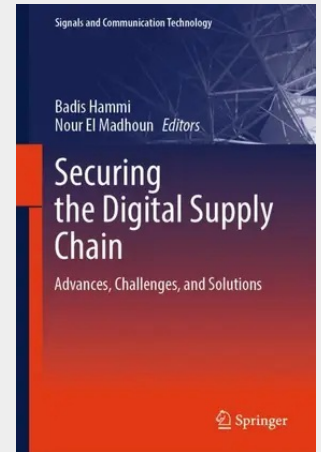
Advances, Challenges, and Solutions

This book offers a comprehensive roadmap for securing modern digital supply chains by weaving together foundational theory, organizational strategy, and advanced technologies. Beginning with a rigorous taxonomy of attack vectors and end-to-end security frameworks, it then introduces the Blueprint concept for Critical Infrastructure Protection, detailing reference architectures, reusable TOSCA-based templates, and their deployment in cloud-enabled operational technologies with integrated SBOM and DevSecOps pipelines. Building on this, the book examines the human and institutional dimensions of supply-chain security through a systematic review of European higher-education initiatives, regulatory compliance requirements, and industry-academia collaborations, and presents the SECURE framework's six strategic pillars—risk management, educational innovation, compliance integration, emerging technologies, partnerships, and workforce development—illustrated via a hypothetical case study. Finally, it showcases cutting-edge sectoral applications, from prioritizing cybersecurity measures in aerospace, agriculture, automotive, and pharmaceutical value chains using multi-criteria decision-making and Digital Twins, to leveraging AI and machine-learning models for real-time anomaly detection and predictive analytics, and deploying blockchain-based traceability solutions that employ smart contracts and QR-code verification to enhance transparency and trust. Written by leading academics and practitioners, this book bridges theory and practice to empower researchers, infrastructure operators, and policymakers with the insights and tools needed to build resilient, transparent, and secure digital supply-chain ecosystems

Chapters include :

- On the Security of Digital Supply Chain by
- Enhancing Digital Supply Chain Security Through Critical Infrastructure Protection Blueprints by
- Supply Chain Security of Critical Infrastructure Protection Software Blueprints by
- The Role of Higher Education in Addressing Cybersecurity Challenges in EU Digital Supply Chains by
- The SECURE Framework: A Strategic Response to Digital Supply Chain Cybersecurity Challenges by
- Optimal Cybersecurity Measures in Airbus's Industrial Value Chain (Aerospace) by
- Artificial Intelligence and Machine Learning for Supply Chain Security by
- Artificial Intelligence and Machine Learning by
- FARMILY: A Blockchain-Based Solution for Food Supply Chain Transparency by

This book offers a comprehensive roadmap for securing modern digital supply chains by weaving together foundational theory, organizational strategy, and advanced technologies. Beginning with a rigorous taxonomy of attack vectors and end-to-end security frameworks, it then introduces the Blueprint concept for Critical Infrastructure Protection, detailing reference architectures, reusable TOSCA-based templates, and their deployment in cloud-enabled operational technologies with integrated SBOM and DevSecOps pipelines. Building on this, the book examines the human and institutional dimensions of supply-chain security through a systematic review of European higher-education initiatives, regulatory compliance requirements, and industry-academia collaborations, and presents the SECURE framework's six strategic pillars—risk management, educational innovation, compliance integration, emerging technologies, partnerships, and workforce development—illustrated via a hypothetical case study. Finally, it showcases cutting-edge sectoral applications, from prioritizing cybersecurity measures in aerospace, agriculture, automotive, and pharmaceutical value chains using multi-criteria decision-making and Digital Twins, to leveraging AI and machine-learning models for real-time anomaly detection and predictive analytics, and deploying



181,89 €

169,99 € (zzgl. MwSt.)

Lieferfrist: bis zu 10 Tage

Artikelnummer: 9783032111180

Medium: Buch

ISBN: 978-3-032-11118-0

Verlag: Birkhäuser

Erscheinungstermin: 31.01.2026

Sprache(n): Englisch

Auflage: Erscheinungsjahr 2026

Serie: Signals and Communication Technology

Produktform: Gebunden

Gewicht: 533 g

Seiten: 228

Format (B x H): 160 x 241 mm

