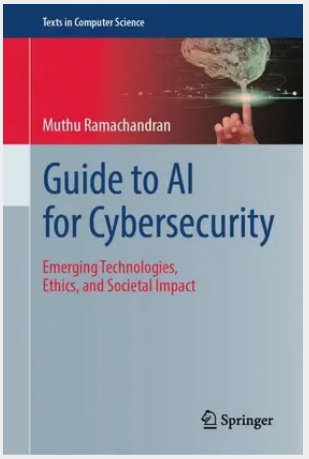
Ramachandran

Guide to AI for Cybersecurity

Emerging Technologies, Ethics, and Societal Impact



85,59 €
79,99 € (zzgl. MwSt.)

vorbestellbar, Erscheinungstermin ca. Juli 2026

Artikelnummer: 9783032258731
Medium: Buch
ISBN: 978-3-032-25873-1
Verlag: Springer Nature Switzerland AG
Erscheinungstermin: 23.07.2026
Sprache(n): Englisch
Auflage: Erscheinungsjahr 2026
Serie: Texts in Computer Science
Produktform: Gebunden
Seiten: 669
Format (B x H): 155 x 235 mm

With ransomware attacks predicted every two seconds by 2031 and 91% of successful cyberattacks beginning with social engineering, organizations face existential threats that demand AI-powered defenses integrating both technical sophistication and human behavioral insights.

This comprehensive textbook bridges cutting-edge AI research with practical cybersecurity implementation. Readers progress from specialized applications including quantum-resistant architectures and AI-blockchain integration, through ethical governance and accountability frameworks, to advanced defense techniques and societal applications addressing threats from cyberbullying to AI-powered disinformation. The text uniquely integrates cognitive psychology with AI techniques, providing frameworks for human-AI collaborative defense that strengthen rather than replace human capabilities.

Topics and features:

• Introduces post-quantum cryptography and quantum-resistant AI security frameworks for the coming cryptographic transition

• Includes complete instructor resources with slides, exercises, and assessments

• Covers Model Context Protocol (MCP) security and LLM security for emerging AI agent architectures

• Presents neurosymbolic AI approaches combining neural networks with symbolic reasoning for enhanced threat detection

• Addresses global governance strategies with regulatory compliance guidance for GDPR, AI Act, and CCPA

• Features psychological resilience-building and behavioral analytics

This essential volume provides comprehensive coverage suitable for graduate students in computer science, cybersecurity, AI, or software engineering programs. Security professionals, software architects, academic instructors, and technology leaders responsible for AI governance will find the frameworks and implementations invaluable for advancing practice in this critical field.

Muthu Ramachandran is Research Consultant at Forti5 Technologies Ltd, UK, and Visiting Professor Extraordinarius at University of South Africa.

With ransomware attacks predicted every two seconds by 2031 and 91% of successful cyberattacks beginning with social engineering, organizations face existential threats that demand AI-powered defenses integrating both technical sophistication and human behavioral insights.This comprehensive textbook bridges cutting-edge AI research with practical cybersecurity implementation. Readers progress from specialized applications including quantum-resistant architectures and AI-blockchain integration, through ethical governance and accountability frameworks, to advanced defense techniques and societal applications addressing threats from cyberbullying to AI-powered disinformation. The text uniquely integrates cognitive psychology with AI techniques, providing frameworks for human-AI collaborative defense that strengthen rather than replace human capabilities.Topics and features:• Introduces post-quantum cryptography and quantum-resistant AI security frameworks for the coming cryptographic transition• Includes complete instructor resources with slides, exercises, and assessments• Covers Model Context Protocol (MCP) security and LLM security for emerging AI agent

Kundenservice Verlag Dr. Otto Schmidt KG
Neumannstraße 10, 40235 Düsseldorf | kundenservice@otto-schmidt.de | 0221-93738-997 (Inland)