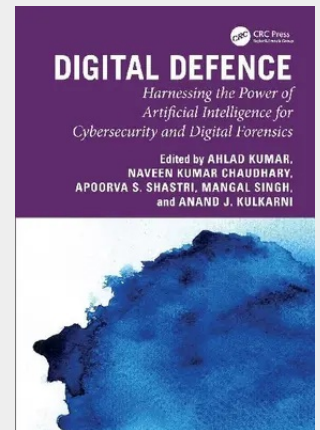


Digital Defence

Harnessing the Power of Artificial Intelligence for Cybersecurity and Digital Forensics

This book aims to provide a comprehensive overview of the applications of Artificial Intelligence (AI) in the area of Cybersecurity and Digital Forensics. The various chapters of this book are written to explore how cutting-edge technologies can be used to improve the detection, prevention, and investigation of cybercrime and help protect digital assets. Digital Defence covers an overview of deep learning and AI techniques and their relevance to cybersecurity and digital forensics, discusses common cyber threats and vulnerabilities, and how deep learning and AI can detect and prevent them. It focuses on how deep learning/artificial learning techniques can be used for intrusion detection in networks and systems, analyze and classify malware, and identify potential sources of malware attacks. This book also explores AI's role in digital forensics investigations, including data recovery, incident response and management, real-time monitoring, automated response analysis, ethical and legal considerations, and visualization. By covering these topics, this book will provide a valuable resource for researchers, students, and cybersecurity and digital forensics professionals interested in learning about the latest advances in deep learning and AI techniques and their applications.

This book aims to provide a comprehensive overview of the applications of Artificial Intelligence (AI) in the area of Cybersecurity and Digital Forensics. The various chapters of this book are written to explore how cutting-edge technologies can be used to improve the detection, prevention, and investigation of cybercrime and help protect digital assets. Digital Defence covers an overview of deep learning and AI techniques and their relevance to cybersecurity and digital forensics, discusses common cyber threats and vulnerabilities, and how deep learning and AI can detect and prevent them. It focuses on how deep learning/artificial learning techniques can be used for intrusion detection in networks and systems, analyze and classify malware, and identify potential sources of malware attacks. This book also explores AI's role in digital forensics investigations, including data recovery, incident response and management, real-time monitoring, automated response analysis, ethical and legal considerations, and visualization. By covering these topics, this book will provide a valuable resource for researchers, students, and cybersecurity and digital forensics professionals interested in learning about the latest advances in deep learning and AI techniques and their applications.



65,00 €

65,00 € (zzgl. MwSt.)

vorbestellbar, Erscheinungstermin ca.
Juli 2026

Artikelnummer: 9781032714837

Medium: Buch

ISBN: 978-1-032-71483-7

Verlag: Taylor & Francis Ltd

Erscheinungstermin: 20.07.2026

Sprache(n): Englisch

Auflage: 1. Auflage 2026

Produktform: Kartoniert

Gewicht: 453 g

Seiten: 188

Format (B x H): 178 x 254 mm

