

Big Data and Edge Intelligence for Enhanced Cyber Defense

Principles and Research

An unfortunate outcome of the growth of the Internet and mobile technologies has been the challenge of countering cybercrime. This book introduces and explains the latest trends and techniques of edge artificial intelligence (EdgeAI) intended to help cyber security experts design robust cyber defense systems (CDS), including host-based and network-based intrusion detection system and digital forensic intelligence. This book discusses the direct confluence of EdgeAI with big data, as well as demonstrating detailed reviews of recent cyber threats and their countermeasure. It provides computational intelligence techniques and automated reasoning models capable of fast training and timely data processing of cyber security big data, in addition to other basic information related to network security. In addition, it provides a brief overview of modern cyber security threats and outlines the advantages of using EdgeAI to counter these threats, as well as exploring various cyber defense mechanisms (CDM) based on detection type and approaches. Specific challenging areas pertaining to cyber defense through EdgeAI, such as improving digital forensic intelligence, proactive and adaptive defense of network infrastructure, and bio-inspired CDM, are also discussed. This book is intended as a reference for academics and students in the field of network and cybersecurity, particularly on the topics of intrusion detection systems, smart grid, EdgeAI, and bio-inspired cyber defense principles. The front-line EdgeAI techniques discussed will also be of use to cybersecurity engineers in their work enhancing cyber defense systems.

An unfortunate outcome of the growth of the Internet and mobile technologies has been the challenge of countering cybercrime. This book introduces and explains the latest trends and techniques of edge artificial intelligence (EdgeAI) intended to help cyber security experts design robust cyber defense systems (CDS), including host-based and network-based intrusion detection system and digital forensic intelligence. This book discusses the direct confluence of EdgeAI with big data, as well as demonstrating detailed reviews of recent cyber threats and their countermeasure. It provides computational intelligence techniques and automated reasoning models capable of fast training and timely data processing of cyber security big data, in addition to other basic information related to network security. In addition, it provides a brief overview of modern cyber security threats and outlines the advantages of using EdgeAI to counter these threats, as well as exploring various cyber defense mechanisms (CDM) based on detection type and approaches. Specific challenging areas pertaining to cyber defense through EdgeAI, such as improving digital forensic intelligence, proactive and adaptive defense of network infrastructure, and bio-inspired CDM, are also discussed. This book is intended as a reference for academics and students in the field of network and cybersecurity, particularly on the topics of intrusion detection systems, smart grid, EdgeAI, and bio-inspired cyber defense principles. The front-line EdgeAI techniques discussed will also be of use to cybersecurity engineers in their work enhancing cyber defense systems.



66,00 €

66,00 € (zzgl. MwSt.)

vorbestellbar, Erscheinungstermin ca. Mai 2026

Artikelnummer: 9781032104850

Medium: Buch

ISBN: 978-1-032-10485-0

Verlag: Taylor & Francis Ltd

Erscheinungstermin: 21.05.2026

Sprache(n): Englisch

Auflage: 1. Auflage 2026

Serie: Edge AI in Future Computing

Produktform: Kartoniert

Gewicht: 370 g

Seiten: 200

Format (B x H): 156 x 234 mm

