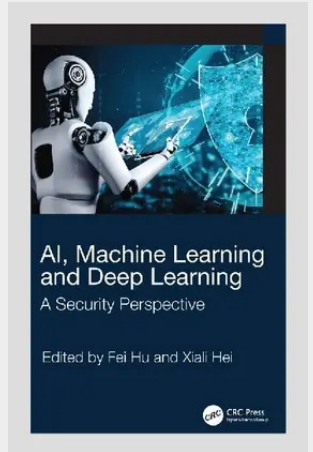


AI, Machine Learning and Deep Learning

A Security Perspective

Today, Artificial Intelligence (AI) and Machine Learning/ Deep Learning (ML/DL) have become the hottest areas in information technology. In our society, many intelligent devices rely on AI/ML/DL algorithms/tools for smart operations. Although AI/ML/DL algorithms and tools have been used in many internet applications and electronic devices, they are also vulnerable to various attacks and threats. AI parameters may be distorted by the internal attacker; the DL input samples may be polluted by adversaries; the ML model may be misled by changing the classification boundary, among many other attacks and threats. Such attacks can make AI products dangerous to use. While this discussion focuses on security issues in AI/ML/DL-based systems (i.e., securing the intelligent systems themselves), AI/ML/DL models and algorithms can actually also be used for cyber security (i.e., the use of AI to achieve security). Since AI/ML/DL security is a newly emergent field, many researchers and industry professionals cannot yet obtain a detailed, comprehensive understanding of this area. This book aims to provide a complete picture of the challenges and solutions to related security issues in various applications. It explains how different attacks can occur in advanced AI tools and the challenges of overcoming those attacks. Then, the book describes many sets of promising solutions to achieve AI security and privacy. The features of this book have seven aspects: - This is the first book to explain various practical attacks and countermeasures to AI systems - Both quantitative math models and practical security implementations are provided - It covers both "securing the AI system itself" and "using AI to achieve security" - It covers all the advanced AI attacks and threats with detailed attack models - It provides multiple solution spaces to the security and privacy issues in AI tools - The differences among ML and DL security and privacy issues are explained - Many practical security applications are covered

Today AI and Machine/Deep Learning have become the hottest areas in the information technology. This book aims to provide a complete picture on the challenges and solutions to the security issues in various applications. It explains how different attacks can occur in advanced AI tools and the challenges of overcoming those attacks.



164,60 €

164,60 € (zzgl. MwSt.)

Lieferfrist: bis zu 10 Tage

Artikelnummer: 9781032034041

Medium: Buch

ISBN: 978-1-032-03404-1

Verlag: CRC Press

Erscheinungstermin: 05.06.2023

Sprache(n): Englisch

Auflage: 1. Auflage 2023

Produktform: Gebunden

Gewicht: 846 g

Seiten: 346

Format (B x H): 183 x 260 mm

