

Generative AI Security

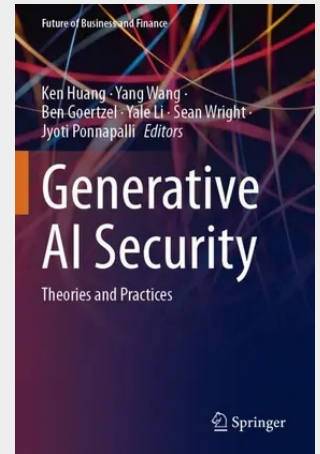
Theories and Practices

This book explores the revolutionary intersection of Generative AI (GenAI) and cybersecurity. It presents a comprehensive guide that intertwines theories and practices, aiming to equip cybersecurity professionals, CISOs, AI researchers, developers, architects and college students with an understanding of GenAI's profound impacts on cybersecurity.

The scope of the book ranges from the foundations of GenAI, including underlying principles, advanced architectures, and cutting-edge research, to specific aspects of GenAI security such as data security, model security, application-level security, and the emerging fields of LLMOps and DevSecOps. It explores AI regulations around the globe, ethical considerations, the threat landscape, and privacy preservation. Further, it assesses the transformative potential of GenAI in reshaping the cybersecurity landscape, the ethical implications of using advanced models, and the innovative strategies required to secure GenAI applications. Lastly, the book presents an in-depth analysis of the security challenges and potential solutions specific to GenAI, and a forward-looking view of how it can redefine cybersecurity practices. By addressing these topics, it provides answers to questions on how to secure GenAI applications, as well as vital support with understanding and navigating the complex and ever-evolving regulatory environments, and how to build a resilient GenAI security program.

The book offers actionable insights and hands-on resources for anyone engaged in the rapidly evolving world of GenAI and cybersecurity.

This book explores the revolutionary intersection of Generative AI (GenAI) and cybersecurity. It presents a comprehensive guide that intertwines theories and practices, aiming to equip cybersecurity professionals, CISOs, AI researchers, developers, architects and college students with an understanding of GenAI's profound impacts on cybersecurity. The scope of the book ranges from the foundations of GenAI, including underlying principles, advanced architectures, and cutting-edge research, to specific aspects of GenAI security such as data security, model security, application-level security, and the emerging fields of LLMOps and DevSecOps. It explores AI regulations around the globe, ethical considerations, the threat landscape, and privacy preservation. Further, it assesses the transformative potential of GenAI in reshaping the cybersecurity landscape, the ethical implications of using advanced models, and the innovative strategies required to secure GenAI applications. Lastly, the book presents an in-depth analysis of the security challenges and potential solutions specific to GenAI, and a forward-looking view of how it can redefine cybersecurity practices. By addressing these topics, it provides answers to questions on how to secure GenAI applications, as well as vital support with understanding and navigating the complex and ever-evolving regulatory environments, and how to build a resilient GenAI security program. The book offers actionable insights and hands-on resources for anyone engaged in the rapidly evolving world of GenAI and cybersecurity.



85,59 €
79,99 € (zzgl. MwSt.)

Lieferfrist: bis zu 10 Tage

Artikelnummer: 9783031542541
Medium: Buch
ISBN: 978-3-031-54254-1
Verlag: Springer
Erscheinungstermin: 06.04.2025
Sprache(n): Englisch
Auflage: Erscheinungsjahr 2025
Serie: Future of Business and Finance
Produktform: Kartoniert
Gewicht: 569 g
Seiten: 338
Format (B x H): 155 x 235 mm

