1. Record Nr. UNINA9910770274903321

Autore	Pan Zhixin
Titolo	Explainable AI for Cybersecurity / / by Zhixin Pan, Prabhat Mishra
Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2023
ISBN	9783031464799 3031464796
Edizione	[1st ed. 2023.]
Descrizione fisica	1 online resource (249 pages)
Collana	Intelligent Technologies and Robotics Series
Altri autori (Persone)	MishraPrabhat
Disciplina	005.8
Soggetti	Computational intelligence Electronic circuits Data protection Electronic circuit design Embedded computer systems Artificial intelligence Computational Intelligence Electronic Circuits and Systems Data and Information Security Electronics Design and Verification Embedded Systems Artificial Intelligence
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Part 1: Introduction -- Chapter 1. Cybersecurity Landscape for Computer Systems -- Chapter 2. Explainable Artificial Intelligence -- Part 2: Detection of Software Vulnerabilities -- Chapter 3. Malware Detection using Explainable AI -- Chapter 4. Spectre and Meltdown Detection using Explainable AI -- Part 3: Detection of Hardware Vulnerabilities -- Chapter 5. Hardware Trojan Detection using Reinforcement Learning -- Chapter 6. Hardware Trojan Detection using Side-Channel Analysis -- Chapter 7. Hardware Trojan Detection using Shapley Ensemble Boosting -- Part 4: Mitigation of AI Vulnerabilities -- Chapter 8. Mitigation of Adversarial Machine Learning -- Chapter 9. AI Trojan Attacks and Countermeasures -- Part 5: Acceleration of

	Explainable AI -- Chapter 10. Hardware Acceleration of Explainable AI -- Chapter 11. Explainable AI Acceleration using Tensor Processing Units -- Part 6: Conclusion -- Chapter 12. The Future of AI-Enabled Cybersecurity.
Sommario/riassunto	This book provides a comprehensive overview of security vulnerabilities and state-of-the-art countermeasures using explainable artificial intelligence (AI). Specifically, it describes how explainable AI can be effectively used for detection and mitigation of hardware vulnerabilities (e.g., hardware Trojans) as well as software attacks (e.g., malware and ransomware). It provides insights into the security threats towards machine learning models and presents effective countermeasures. It also explores hardware acceleration of explainable AI algorithms. The reader will be able to comprehend a complete picture of cybersecurity challenges and how to detect them using explainable AI. This book serves as a single source of reference for students, researchers, engineers, and practitioners for designing secure and trustworthy systems. Introduces a wide variety of software and hardware vulnerabilities; Describes solutions for detecting security attacks using explainable AI; Presents a fast and robust framework using hardware acceleration and mitigation of adversarial attacks.