1.	Record Nr.	UNINA9910869176503321
	Titolo	Artificial Intelligence for Security : Enhancing Protection in a Changing World / / edited by Tuomo Sipola, Janne Alatalo, Monika Wolfmayr, Tero Kokkonen
	Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2024
	ISBN	9783031574528
	Edizione	[1st ed. 2024.]
	Descrizione fisica	1 online resource (373 pages)
	Disciplina	006.3
	Soggetti	Data protection - Law and legislation Artificial intelligence Computer networks - Security measures Privacy Artificial Intelligence Mobile and Network Security
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Nota di contenuto	Part I Methodological Fundamentals of Artificial Intelligence -- Chapter. 1.Safeguarding the Future of Artificial Intelligence: An AI Blueprint -- Chapter.2.Cybersecurity and the AI Silver Bullet.-Chapter.3.Artificial Intelligence and Differential Privacy – Review of Protection Estimate Models -- Chapter.4.To Know What You Do Not Know: Challenges for Explainable AI for Security and Threat Intelligence -- Chapter.5. Securing the Future: The Role of Knowledge Discovery Frameworks -- Chapter.6.Who Guards the Guardians? On Robustness of Deep Neural Networks.-Part II Artificial Intelligence for Critical Infrastructure Protection -- Chapter.7.Opportunities and Challenges of Using Artificial Intelligence in Securing Cyber-Physical System -- Chapter.8.Artificial Intelligence Working to Secure Small Enterprises -- Chapter.9.On the Cyber Security of Logistics in the Age of Artificial Intelligence.-Chapter. 10.Fuzzy Machine Learning for Smart Grid Instability Detection -- Chapter.11.On Protection of the Next-Generation Mobile Networks against Adversarial Examples -- Chapter.12.Designing and Implementing an Interactive Cloud Platform for Teaching Machine

Sommario/riassunto

This book discusses the use of artificial intelligence (AI) for security purposes. It is divided into three parts: methodological fundamentals of AI, use of AI for critical infrastructure protection and anomaly detection. The first section describes the latest knowledge for creating safe AIs and using them to enhance protection. This book also presents various domains and examples of AI-driven security. The chapters describe potential methods, demonstrate use cases and discuss the challenges of the evolving field. This includes topics such as defensive use of AI to detect threats. It discusses the offensive use of AI to better understand the future threat landscape, the use of AI for automation in critical infrastructure and overall challenges of AI usage for critical tasks. As new threats emerge, the use of AI technologies to protect the world one lives in is topical. New technologies in this space have advanced rapidly, and subsequently, their use in enhancing protection is an evident development. To this effect, this book brings together a group of international researchers and professionals who present their views on how to create security through AI. This book targets postgraduate students, researchers and professionals who want to understand the use of AI for security. Understanding latest advancements in this field will also be useful to those who want to comprehend modern cybersecurity in detail and who want to follow research and latest trends. .