1.	Record Nr.	UNINA9910838286303321
	Autore	Korytkowski Marcin
	Titolo	Advanced Techniques of Artificial Intelligence in IT Security Systems / / by Marcin Korytkowski
	Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2024
	ISBN	9783031538544
		3031538544
	Edizione	[1st ed. 2024.]
	Descrizione fisica	1 online resource (94 pages)
	Collana	Studies in Big Data, , 2197-6511 ; ; 146
	Disciplina	620.00285
	Soggetti	Engineering - Data processing
		Computational intelligence
		Data protection
		Artificial intelligence
		Big data
		Data Engineering
		Computational Intelligence
		Data and Information Security
		Artificial Intelligence
		Big Data
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Nota di contenuto	Artificial neural networks -- Initialization of weights values in neural networks -- Convolution neural networks -- Application of artificial intelligence methods in profiling of computer network users -- Profiling users using the random forest algorithm -- Convolutional networks in user profiling -- User profiling using recurrent-convolutional networks -- Detection of network traffic anomalies using OC-NN.
	Sommario/riassunto	The book explores how modern technologies, including artificial intelligence and neural networks, are being used to enhance cybersecurity. In today's world, the development of the Internet is nothing short of transformative, affecting every aspect of our lives. Ensuring the safety of its users is a paramount concern, and it requires

a diverse set of disciplines to address. Researchers from various fields, including IT, mathematics, psychology, and medicine, are collectively working to tackle this interdisciplinary challenge. The significance of this issue has been magnified by the COVID-19 pandemic, which forced many aspects of our lives into the digital realm, from online payments to remote work and education. This shift brought new security challenges, with data privacy and system integrity taking center stage. It delves into the intricacies of Big Data by having to analyze an immense volume of network traffic data that can only be effectively analyzed with specialized tools. Real-time threat detection is critical, and the book sheds light on cutting-edge approaches to achieving this goal. The content of the book covers a broad spectrum of topics related to IT system security, from user and system profiling to preventing data leaks and defending against phishing attacks. Additionally, innovative concepts such as "glial networks" are introduced, offering new ways to interpret knowledge stored in convolutional networks. These solutions are not limited to security alone; they have applications across various domains. The book highlights the advantages of these cutting-edge approaches over existing methods, demonstrating their relevance to large corporations, public institutions, schools, small businesses, and households. In a world where security threats are constantly evolving, this book is a valuable resource for understanding the dynamic landscape of network security and the role of artificial intelligence in safeguarding our digital ecosystems.