

Contents

Preface	vii
About the Editors	ix
Contributors	xi

PART I Secure AI/ML Systems: Attack Models

1 Machine Learning Attack Models	3
<i>Jing Lin, Long Dang, Mohamed Rahouti, and Kaiqi Xiong</i>	
2 Adversarial Machine Learning: A New Threat Paradigm for Next-generation Wireless Communications	35
<i>Yalin E. Sagduyu, Yi Shi, Tugba Erpek, William Headley, Bryse Flowers, George Stantchev, Zhuo Lu, and Brian Jalaian</i>	
3 Threat of Adversarial Attacks to Deep Learning: A Survey	53
<i>Linsheng He and Fei Hu</i>	
4 Attack Models for Collaborative Deep Learning	65
<i>Jiamiao Zhao, Fei Hu, and Xiali Hei</i>	
5 Attacks on Deep Reinforcement Learning Systems: A Tutorial	79
<i>Joseph Layton and Fei Hu</i>	
6 Trust and Security of Deep Reinforcement Learning	83
<i>Yen-Hung Chen, Mu-Tien Huang, and Yuh-Jong Hu</i>	
7 IoT Threat Modeling Using Bayesian Networks	105
<i>Diego Heredia</i>	

PART II Secure AI/ML Systems: Defenses

8 Survey of Machine Learning Defense Strategies	121
<i>Joseph Layton, Fei Hu, and Xiali Hei</i>	
9 Defenses Against Deep Learning Attacks	131
<i>Linsheng He and Fei Hu</i>	
10 Defensive Schemes for Cyber Security of Deep Reinforcement Learning	139
<i>Jiamiao Zhao, Fei Hu, and Xiali Hei</i>	

11	Adversarial Attacks on Machine Learning Models in Cyber-Physical Systems	151
	<i>Mahbub Rahman and Fei Hu</i>	
12	Federated Learning and Blockchain: An Opportunity for Artificial Intelligence with Data Regulation	157
	<i>Darine Ameyed, Fehmi Jaafar, Riadh ben Chaabene, and Mohamed Cheriet</i>	
 PART III Using AI/ML Algorithms for Cyber Security		
13	Using Machine Learning for Cyber Security: Overview	169
	<i>D. Roshni Thanka, G. Jaspher W. Kathrine, and E. Bijolin Edwin</i>	
14	Performance of Machine Learning and Big Data Analytics Paradigms in Cyber Security	191
	<i>Gabriel Kabanda</i>	
15	Using ML and DL Algorithms for Intrusion Detection in the Industrial Internet of Things	243
	<i>Nicole do Vale Dalarmelina, Pallavi Arora, Baljeet Kaur, Rodolfo Ipolito Meneguette, and Marcio Andrey Teixeira</i>	
 PART IV Applications		
16	On Detecting Interest Flooding Attacks in Named Data Networking (NDN)-based IoT Searches	259
	<i>Hengshuo Liang, Lauren Burgess, Weixian Liao, Qianlong Wang, and Wei Yu</i>	
17	Attack on Fraud Detection Systems in Online Banking Using Generative Adversarial Networks	277
	<i>Jerzy Surma and Krzysztof Jagiello</i>	
18	Artificial Intelligence-assisted Security Analysis of Smart Healthcare Systems	287
	<i>Nur Imtiazul Haque and Mohammad Ashiqur Rahman</i>	
19	A User-centric Focus for Detecting Phishing Emails	313
	<i>Regina Eckhardt and Sikha Bagui</i>	