

Contents

Preface	vii
About the Editors	ix
Contributors	xi

PART I Secure AI/ML Systems: Attack Models

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

PART II Secure AI/ML Systems: Defenses

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

11 Adversarial Attacks on Machine Learning Models in Cyber-Physical Systems <i>Mahbub Rahman and Fei Hu</i>	151
12 Federated Learning and Blockchain: An Opportunity for Artificial Intelligence with Data Regulation <i>Darine Ameyed, Fehmi Jaafar, Riadh ben Chaabene, and Mohamed Cheriet</i>	157

PART III Using AI/ML Algorithms for Cyber Security

13 Using Machine Learning for Cyber Security: Overview <i>D. Roshni Thanka, G. Jasper W. Kathrine, and E. Bijolin Edwin</i>	169
14 Performance of Machine Learning and Big Data Analytics Paradigms in Cyber Security <i>Gabriel Kabanda</i>	191
15 Using ML and DL Algorithms for Intrusion Detection in the Industrial Internet of Things <i>Nicole do Vale Dalarmelina, Pallavi Arora, Baljeet Kaur, Rodolfo Ipolito Meneguette, and Marcio Andrey Teixeira</i>	243

PART IV Applications

16 On Detecting Interest Flooding Attacks in Named Data Networking (NDN)-based IoT Searches <i>Hengshuo Liang, Lauren Burgess, Weixian Liao, Qianlong Wang, and Wei Yu</i>	259
17 Attack on Fraud Detection Systems in Online Banking Using Generative Adversarial Networks <i>Jerzy Surma and Krzysztof Jagiełło</i>	277
18 Artificial Intelligence-assisted Security Analysis of Smart Healthcare Systems <i>Nur Imtiazul Haque and Mohammad Ashiqur Rahman</i>	287
19 A User-centric Focus for Detecting Phishing Emails <i>Regina Eckhardt and Sikha Bagui</i>	313