Studies in Computational Intelligence 1025

Mohiuddin Ahmed ·
Sheikh Rabiul Islam ·
Adnan Anwar · Nour Moustafa ·
Al-Sakib Khan Pathan *Editors*

Explainable Artificial Intelligence for Cyber Security

Next Generation Artificial Intelligence

Springer

Studies in Computational Intelligence

Volume 1025

Series Editor

Janusz Kacprzyk, Polish Academy of Sciences, Warsaw, Poland

The series "Studies in Computational Intelligence" (SCI) publishes new developments and advances in the various areas of computational intelligence—quickly and with a high quality. The intent is to cover the theory, applications, and design methods of computational intelligence, as embedded in the fields of engineering, computer science, physics and life sciences, as well as the methodologies behind them. The series contains monographs, lecture notes and edited volumes in computational intelligence spanning the areas of neural networks, connectionist systems, genetic algorithms, evolutionary computation, artificial intelligence, cellular automata, self-organizing systems, soft computing, fuzzy systems, and hybrid intelligent systems. Of particular value to both the contributors and the readership are the short publication timeframe and the world-wide distribution, which enable both wide and rapid dissemination of research output.

Indexed by SCOPUS, DBLP, WTI Frankfurt eG, zbMATH, SCImago.

All books published in the series are submitted for consideration in Web of Science.

More information about this series at https://link.springer.com/bookseries/7092

Mohiuddin Ahmed · Sheikh Rabiul Islam ·
Adnan Anwar · Nour Moustafa ·
Al-Sakib Khan Pathan
Editors

Explainable Artificial Intelligence for Cyber Security

Next Generation Artificial Intelligence

Springer

Editors

Mohiuddin Ahmed
School of Science
Edith Cowan University
Joondalup, WA, Australia

Sheikh Rabiul Islam
Department of Computing Sciences
University of Hartford
West Hartford, CT, USA

Adnan Anwar
School of IT
Deakin University
Melbourne, VIC, Australia

Nour Moustafa
School of Engineering and IT
UNSW Canberra
Campbell, ACT, Australia

Al-Sakib Khan Pathan
Department of Computer Science
and Engineering
United International University (UIU)
Dhaka, Bangladesh

ISSN 1860-949X ISSN 1860-9503 (electronic)
Studies in Computational Intelligence
ISBN 978-3-030-96629-4 ISBN 978-3-030-96630-0 (eBook)
https://doi.org/10.1007/978-3-030-96630-0

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Dedicated to

My Loving Son: Zaif Rayan

—Mohiuddin Ahmed

My studious daughter: Farisha Islam

—Sheikh Rabiul Islam

My devoted family

—Adnan Anwar

My family

—Nour Moustafa

My family

—Al-Sakib Khan Pathan

Preface

Cyber security is a very complex and diverse discipline. Numerous technological problems need to be solved to make the world safer. It is evident that there is no sign of a decrease in cyber-crime; instead, it is the opposite in nature due to the unprecedented technological advancement and our reliance on it. The cyber security community has been leveraging artificial intelligence (AI) technology to solve several complex computing problems, e.g., intrusion detection systems to identify malicious network activities. In the past two decades, there have been hundreds of algorithms developed capitalizing on the effectiveness of artificial intelligence. Therefore, we have observed the transition from classical artificial intelligence to deep learning, federated learning, reinforcement learning, etc. These techniques have been critical in providing solutions for cyber security problems. However, most recent variants of artificial intelligence-based methods are being treated as *black-box ones*. There is a lack of explanation that humans can easily understand the solution(s) offered. For example, a particular neural network that is perfect for identifying phishing attacks (i.e., the deception using email) is still obscure due to its complex internal working mechanism. Hence, it is important to explore various avenues of explainable artificial intelligence (XAI), an emerging area of artificial intelligence, to provide a human-friendly decision for cyber security from a broader perspective.

In this context, this book addresses the challenges associated with the explainable artificial intelligence for cyber security by providing a bigger picture of the core concepts, intelligent techniques, practices, and open research directions in this area. Additionally, the book will serve as a single source of reference for acquiring knowledge on the technology, process, and people involved in the next-generation artificial intelligence and cyber security.

Chapters

Chapter 1: The Past, Present, and Prospective Future of XAI: A Comprehensive Review
Chapter 2: An Overview of Explainable Artificial Intelligence for Cyber Security
Chapter 3: Artificial Intelligence: Practical and Ethical Challenges
Chapter 4: Domain Knowledge-Aided Explainable Artificial Intelligence
Chapter 5: Machine Learning Based IDS for Cyberattack Classification
Chapter 6: Artificial Intelligence for Cyber Security: Performance Analysis of Network Intrusion Detection
Chapter 7: Leveraging Artificial Intelligence Capabilities for Real-Time Monitoring of Cybersecurity Threats
Chapter 8: Network Forensics in the Era of Artificial Intelligence
Chapter 9: Obfuscation-Based Mechanisms in Location-Based Privacy Protection
Chapter 10: Intelligent Radio Frequency Fingerprinting to Identify Malicious Tags in the Internet of Things
Chapter 11: Explainable Artificial Intelligence for Smart City Application: A Secure and Trusted Platform
Chapter 12: Explainable Artificial Intelligence in Sustainable Smart Healthcare

The book reflects the intersection of artificial intelligence and cyber security. Unlike other books on similar topics, the book focuses on the ‘explainability’ of cyber security applications. Chapter 1 showcases a holistic view of explainable artificial intelligence, Chapter 2 dives into cyber security using artificial intelligence. Chapter 3 highlights ethical issues associated with artificial intelligence. Chapter 4 focuses on domain-knowledge aided explainability. Chapters 5–7 focus on network intrusion detection in depth. Chapter 8 includes insights on network forensics. Chapter 9 discusses privacy preservation and Chap. 10 highlights malicious tags identification for the Internet of Things (IoT). Chapters 11 and 12 showcase different applications of explainable artificial intelligence on smart cities and healthcare systems.

Joondalup, Australia Mohiuddin Ahmed
West Hartford, USA Sheikh Rabiul Islam
Melbourne, Australia Adnan Anwar
Campbell, Australia Nour Moustafa
Dhaka, Bangladesh Al-Sakib Khan Pathan

Acknowledgments

It is another incredible book editing experience and our sincere gratitude to the publisher for facilitating the process. This book editing journey enhanced our patience, communication, and tenacity. We are thankful to all the contributors, reviewers, and publishing team. Last but not least, our thanks to our family members whose support and encouragement contributed significantly to completing this book.

Mohiuddin Ahmed
Sheikh Rabiul Islam
Adnan Anwar
Nour Moustafa
Al-Sakib Khan Pathan

Contents