

Iqbal H. Sarker

AI-Driven Cybersecurity and Threat Intelligence

Cyber Automation, Intelligent
Decision-Making and Explainability



Springer

AI-Driven Cybersecurity and Threat Intelligence


Iqbal H. Sarker

AI-Driven Cybersecurity and Threat Intelligence

Cyber Automation, Intelligent
Decision-Making and Explainability



Springer

Iqbal H. Sarker 
Edith Cowan University
Perth, WA, Australia

ISBN 978-3-031-54496-5 ISBN 978-3-031-54497-2 (eBook)
<https://doi.org/10.1007/978-3-031-54497-2>

© The Editor(s) (if applicable) and The Author(s), under exclusive license to Springer Nature Switzerland AG 2024

This work is subject to copyright. All rights are solely and exclusively licensed by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors, and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

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

Paper in this product is recyclable.

This book is dedicated to all of my family members and well-wishers, especially my beloved parents, who've always trusted me and also have encouraged me to achieve whatever I desired. I would also like to dedicate this book to my loving wife and charming son S.M. Irfan Hasan!
Iqbal H. Sarker, PhD
(Author)

Preface

As technology advances, artificial intelligence (AI) and cybersecurity have become increasingly important. This book explores the dynamics of how AI technology intersects with cybersecurity challenges and threat intelligence as they evolve. Integrating AI into cybersecurity not only offers enhanced defense mechanisms but also presents a paradigm shift in how we conceptualize, detect, and mitigate cyber threats. An in-depth exploration of AI-driven solutions, including machine learning algorithms, data science modeling, generative AI modeling, threat intelligence frameworks, and explainable AI (XAI) models, underpins the future of cybersecurity in this comprehensive exploration. As a roadmap or comprehensive guide to leveraging AI/XAI to defend digital ecosystems against evolving cyber threats, this book provides insights, modeling, real-world applications, research issues, and potential directions to cybersecurity researchers, practitioners, and enthusiasts alike. Throughout this journey, we will discover innovation, challenges, and opportunities, providing a holistic perspective on the transformative role of AI in securing the digital world.

We can divide this book into three main parts:

- The first part of the book consists of the introduction to AI-driven cybersecurity and threat intelligence highlighting AI variants with their potentiality. We also discuss basic cybersecurity knowledge including common terminologies used in the area, attack framework, and security life cycle to provide the required background knowledge and themes for this book.
- In the next part of this book, we explore diverse AI/XAI methods and relevant emerging technologies in the context of cybersecurity, by presenting learning technologies such as machine learning and deep learning algorithms and relevant others. After that, we conduct a comprehensive empirical analysis of various security models toward anomaly and attack detection based on machine learning techniques. We also explore the potentiality of generative AI in the context of cybersecurity as well as data science modeling toward advanced analytics, knowledge, and rule discovery for explainable AI modeling in the context of cybersecurity.

- In the final part of the book, we explore various real-world application areas such as Internet of Things (IoT) and smart city applications, industrial control systems and operational technology (ICS/OT) security, and critical infrastructures within the context of AI and cybersecurity. Eventually, we provide a comprehensive summary of AI variants, explainable and responsible AI, highlighting next-generation cybersecurity.

Overall, the use of AI can transform the way we detect, respond, and defend against threats by enabling proactive threat detection, rapid response, and adaptive defense mechanisms. AI-driven cybersecurity systems excel at analyzing vast datasets rapidly, identifying patterns that indicate malicious activities, detecting threats in real time, as well as predictive analytics for proactive solution. Automation streamlines routine tasks, allowing cybersecurity professionals to focus on strategic aspects of defense. Moreover, AI enhances the ability to detect anomalies, predict potential threats, and respond swiftly, preventing risks from escalated. As cyber threats become increasingly diverse and relentless, incorporating AI/XAI into cybersecurity is not just a choice, but a necessity for improving resilience and staying ahead of ever-changing threats. Overall, this book can be used as a useful resource for academics and industry professionals working in various areas, such as CyberAI, Explainable and Responsible AI, Automation and Intelligent Systems, Adaptive and Robust Security Systems, Cybersecurity Data Science and Data-Driven Decision Making, Machine and Deep Learning, Generative AI, Behavioral and Advanced Analytics, as well as various real-world cybersecurity applications in the area of IoT, ICS/OT, Critical Infrastructures, Digital Twin and Smart City Applications, Cyber-Physical Systems and Security, and relevant others.

We are glad to introduce this book to upper-level undergraduate and postgraduate students, as well as academic and industry researchers in the relevant domains mentioned above. We would like to express our gratitude to everyone who supported and helped us complete this book. Finally, we would like to express our gratitude to Springer Nature for publishing this book. Your insightful feedback on this book would be greatly appreciated.

Enjoy the book!

Perth, WA, Australia

Iqbal H. Sarker

Acknowledgments

This book would have never been finished without the help of many, to whom I would like to express my sincere thanks. All praise be to the Almighty Allah for providing me the strengths and blessings to complete this book.

I would like to express my sincere gratitude to my advisors, teachers, and family members for their exceptional support throughout my career.

Finally, I thank everybody who was involved to the successful publication of this book with an apology for not mentioning by name.

Contents

Part I Preliminaries

1	Introduction to AI-Driven Cybersecurity and Threat Intelligence ...	3
1.1	Introduction.....	3
1.2	Cybersecurity and Threat Intelligence	5
1.2.1	What Is Cybersecurity?	5
1.2.2	What Is Threat Intelligence?.....	7
1.3	Understanding Artificial Intelligence (AI) in Cybersecurity	8
1.3.1	Potentiality of AI	9
1.3.2	Categories of AI.....	10
1.3.3	Relationship with Prominent Technologies	12
1.4	AI Trust, Explainability, and Key Factors	13
1.4.1	Traditional AI in Cybersecurity	14
1.4.2	Explainable AI (XAI) in Cybersecurity	14
1.4.3	Recommendation: AI vs XAI.....	15
1.5	An Overview of This Book	16
1.6	Conclusion	18
	References.....	19
2	Cybersecurity Background Knowledge: Terminologies, Attack Frameworks, and Security Life Cycle	21
2.1	Introduction	21
2.2	Understanding Key Terminologies	23
2.2.1	Cybersecurity	23
2.2.2	Emerging Technologies	26
2.3	Cyber Kill Chain	28
2.3.1	Reconnaissance.....	29
2.3.2	Weaponization.....	29
2.3.3	Delivery.....	29
2.3.4	Exploitation.....	30
2.3.5	Installation	30
2.3.6	Command and Control	30

- 2.3.7 Actions on Objectives 31
- 2.4 MITRE ATT&CK 31
 - 2.4.1 MITRE ATT&CK Matrices..... 32
 - 2.4.2 MITRE ATT&CK Tactics 32
- 2.5 Cybersecurity Life Cycle 34
 - 2.5.1 Govern 35
 - 2.5.2 Identify..... 35
 - 2.5.3 Protect 35
 - 2.5.4 Detect 36
 - 2.5.5 Respond..... 36
 - 2.5.6 Recover 36
- 2.6 Discussion and Lessons Learned 37
- 2.7 Conclusion 38
- References..... 38

Part II AI/XAI Methods and Emerging Technologies

- 3 Learning Technologies: Toward Machine Learning and Deep Learning for Cybersecurity** 43
 - 3.1 Introduction..... 43
 - 3.2 Various Types of Learning Technologies..... 44
 - 3.2.1 Supervised Learning 45
 - 3.2.2 Unsupervised Learning 46
 - 3.2.3 Semi-supervised Learning 46
 - 3.2.4 Reinforcement Learning 47
 - 3.2.5 Transfer Learning 47
 - 3.2.6 Self-Supervised Learning 47
 - 3.2.7 Active Learning 48
 - 3.2.8 Deep Learning 48
 - 3.2.9 Ensemble Learning..... 49
 - 3.2.10 Federated Learning..... 49
 - 3.3 Learning Tasks and Algorithms in Cybersecurity 49
 - 3.3.1 Classification and Regression Analysis 50
 - 3.3.2 Clustering Analysis 51
 - 3.3.3 Rule-Based Modeling Analysis..... 51
 - 3.3.4 Adversarial Learning Analysis 52
 - 3.3.5 Deep Learning Analysis 54
 - 3.4 Real-World Application Areas..... 56
 - 3.5 Discussion and Lessons Learned 57
 - 3.6 Conclusion 58
 - References..... 58
- 4 Detecting Anomalies and Multi-attacks Through Cyber Learning: An Experimental Analysis** 61
 - 4.1 Introduction..... 61
 - 4.2 Exploring Security Dataset 63

- 4.2.1 Security Data Preprocessing 64
- 4.2.2 Feature Ranking and Selection 65
- 4.2.3 Machine Learning Algorithms 66
- 4.3 Experimental Analysis and Discussion 68
 - 4.3.1 Impact of Security Features and Ranking 68
 - 4.3.2 Effectiveness Analysis for Detecting Cyber-anomalies 69
 - 4.3.3 Effectiveness Analysis for Detecting Multi-attacks 72
 - 4.3.4 Effectiveness Analysis for Neural Network-Based Security Model 74
- 4.4 Conclusion 76
- References 77
- 5 Generative AI and Large Language Modeling in Cybersecurity 79**
 - 5.1 Introduction to Generative AI and LLM 79
 - 5.2 Potentiality of Generative AI-enabled Cybersecurity 81
 - 5.3 Generative AI Methods 82
 - 5.3.1 Generative Adversarial Network (GAN) 83
 - 5.3.2 Transformer-Based Methods 84
 - 5.3.3 Autoencoder-Based Method 86
 - 5.4 Generative AI Modeling 87
 - 5.4.1 Generative Language Model 87
 - 5.4.2 Generative Image Model 88
 - 5.4.3 Generative AI Implementation Phases 89
 - 5.5 Cybersecurity Large Language Modeling (CyberLLM) 92
 - 5.5.1 Fine-Tuning Approaches 92
 - 5.5.2 Our Suggested CyberLLM Framework 94
 - 5.6 Challenges and Research Direction 96
 - 5.7 Discussion and Lessons Learned 97
 - 5.8 Conclusion 98
 - References 98
- 6 Cybersecurity Data Science: Toward Advanced Analytics, Knowledge, and Rule Discovery for Explainable AI Modeling 101**
 - 6.1 Introduction 101
 - 6.2 Types of Analytics and Outcome 102
 - 6.2.1 Descriptive Analytics 103
 - 6.2.2 Diagnostic Analytics 103
 - 6.2.3 Predictive Analytics 103
 - 6.2.4 Prescriptive Analytics 104
 - 6.3 Understanding Data Science Modeling 104
 - 6.3.1 Understanding Business Problems 105
 - 6.3.2 Understanding Data 106
 - 6.3.3 Data Preprocessing and Exploration 106
 - 6.3.4 Machine Learning Modeling and Evaluation 107
 - 6.3.5 Data Product and Automation 107

- 6.4 Data Science-Based Knowledge Discovery Process..... 108
 - 6.4.1 Knowledge Discovery Process from Cyber Data 108
 - 6.4.2 Cybersecurity Data Science Modeling 109
- 6.5 Data-Driven Rule-Based Explainable Cybersecurity Modeling ... 111
 - 6.5.1 Data Collection Module: Layer 1..... 111
 - 6.5.2 Data Preparation and Augmentation Module: Layer 2..... 112
 - 6.5.3 Rule Mining Module: Layer 3 112
 - 6.5.4 Rule Management Module: Layer 4..... 112
 - 6.5.5 Explainable Outcome Module: Layer 5 113
- 6.6 Real-World Cybersecurity Applications Based on Knowledge Discovery and Data-Driven Rules 113
 - 6.6.1 Anomaly or Intrusion Detection 114
 - 6.6.2 Attack Categorization or Classification 114
 - 6.6.3 Predicting Emerging Threats and Vulnerabilities..... 114
 - 6.6.4 Diagnostic Analytics and Incident Investigation..... 115
 - 6.6.5 Effective Mitigation Strategies 115
 - 6.6.6 Incident Response 115
- 6.7 Discussion and Lessons Learned 116
- 6.8 Conclusion 117
- References..... 117

Part III Real-World Application Areas with Research Issues

- 7 AI-Enabled Cybersecurity for IoT and Smart City Applications 121**
 - 7.1 Introduction to AI for IoT and Smart Cities 121
 - 7.2 Background: IoT and Smart Cities 122
 - 7.2.1 The IoT Paradigm 122
 - 7.2.2 Application Areas of Smart Cities..... 123
 - 7.2.3 IoT Attack Surface Areas 124
 - 7.3 IoT System Architectures with Security Issues and AI Potentiality 125
 - 7.3.1 Security Issues and AI Potentiality at Perception or Sensing Layer 125
 - 7.3.2 Security Issues and AI Potentiality at Networking and Data Communications Layer..... 127
 - 7.3.3 Security Issues and AI Potentiality at Middleware or Support Layer 128
 - 7.3.4 Security Issues and AI Potentiality at Application Layer 129
 - 7.4 Potentiality of AI-Enabled Security Modeling and Real-World Use Cases..... 130
 - 7.5 Challenges and Research Directions 133
 - 7.6 Discussion and Lessons Learned 134
 - 7.7 Conclusion 135
 - References..... 135

- 8 AI for Enhancing ICS/OT Cybersecurity** 137
 - 8.1 Introduction to AI for ICS/OT Cybersecurity 137
 - 8.2 OT Components and Cybersecurity Issues 139
 - 8.3 Why AI in ICS/OT Cybersecurity 142
 - 8.4 Cyber Modeling Process in ICS/OT Environment 143
 - 8.5 Real-World ICS/OT Application Areas 145
 - 8.5.1 Smart Grid Protection 145
 - 8.5.2 Manufacturing and Factory 146
 - 8.5.3 Oil and Gas Facilities 146
 - 8.5.4 Water and Wastewater Systems 146
 - 8.5.5 Agriculture Sector 147
 - 8.5.6 Chemical Processing Plants 147
 - 8.6 Challenges and Directions on AI-Based Cybersecurity
in ICS/OT Environment 147
 - 8.7 Discussion and Lessons Learned 150
 - 8.8 Conclusion 151
 - References 151
- 9 AI for Critical Infrastructure Protection and Resilience** 153
 - 9.1 Introduction to Critical Infrastructure 153
 - 9.2 Critical Infrastructure Sectors and Impact on Society and
Economy 155
 - 9.3 Potentiality of AI-Based Cybersecurity in Critical
Infrastructure 157
 - 9.4 Cyber Modeling Process in Critical Infrastructure 158
 - 9.5 Real-World Cybersecurity Use Cases 160
 - 9.5.1 Potential Attacks and AI-Based Cybersecurity
Solutions 160
 - 9.5.2 Example of Domain-Specific Attacks with
Cybersecurity 162
 - 9.6 Challenges on AI-Based Cybersecurity in Critical
Infrastructure 169
 - 9.7 Discussion and Lessons Learned 170
 - 9.8 Conclusion 171
 - References 171
- 10 CyberAI: A Comprehensive Summary of AI Variants,
Explainable and Responsible AI for Cybersecurity** 173
 - 10.1 Introduction 173
 - 10.2 AI Variants in Cybersecurity: A Summary 175
 - 10.2.1 Analytical AI in Cybersecurity 175
 - 10.2.2 Functional AI in Cybersecurity 175
 - 10.2.3 Interactive AI in Cybersecurity 176
 - 10.2.4 Textual AI in Cybersecurity 176
 - 10.2.5 Visual AI in Cybersecurity 177
 - 10.2.6 Generative AI in Cybersecurity 177

- 10.2.7 Discriminative AI in Cybersecurity 177
- 10.2.8 Hybrid AI in Cybersecurity 178
- 10.3 AI Transparency and Accountability 178
 - 10.3.1 Explainable AI (XAI) in Cybersecurity 179
 - 10.3.2 Responsible AI in Cybersecurity 182
 - 10.3.3 Human-AI Teaming in Cybersecurity 182
 - 10.3.4 Recommendation for AI Systems: Inclusive and Responsible AI 183
- 10.4 Key AI Technologies in Cybersecurity: A Summary 184
 - 10.4.1 Machine Learning 184
 - 10.4.2 Deep Learning 185
 - 10.4.3 Data Science Modeling and Advanced Analytics 185
 - 10.4.4 Knowledge Discovery and Rule Mining 186
 - 10.4.5 Semantics and Knowledge Representation 186
 - 10.4.6 Large Language Modeling 186
 - 10.4.7 Multimodal Intelligence Modeling 187
- 10.5 Real-World Application Areas 187
 - 10.5.1 AI in Cyber-Physical Systems Security 188
 - 10.5.2 AI in Critical Infrastructure Security 189
 - 10.5.3 AI in Digital Twin Security 190
 - 10.5.4 AI in Smart Cities and IoT Security 190
 - 10.5.5 AI in Metaverse Security 191
- 10.6 Potential Usages and Research Scope 192
 - 10.6.1 Potential Usages Scope of AI 192
 - 10.6.2 Understanding and Mitigating Data Poisoning Risks ... 194
 - 10.6.3 Effectively Handling Dynamic and Evolving Threat Landscape 194
 - 10.6.4 Advancing Data Analytics 195
 - 10.6.5 Advancing Knowledge Discovery and Refining Rule Mining 195
 - 10.6.6 Advancing Large Language Model (LLM) 195
 - 10.6.7 Advancing Model Transparency and Explainability 196
 - 10.6.8 Ensuring Data Freshness and Recency in AI Security Solutions 196
 - 10.6.9 Ensuring Inclusivity and Fairness in AI Security Solutions 197
 - 10.6.10 Research Scopes in Pre-modeling, In-modeling, and Post-modeling Phases: A Broad Picture 197
- 10.7 Discussion and Lessons Learned 199
- 10.8 Conclusion 200
- References 200

About the Author

Dr. Iqbal H. Sarker (ORCID ID: <https://orcid.org/0000-0003-1740-5517>) received his PhD in Computer Science from Swinburne University of Technology, Melbourne, Australia, in 2018. Now he is working as a research fellow at Cybersecurity Cooperative Research Centre (CRC) in association with the Centre for Securing Digital Futures, Edith Cowan University, Australia, through academia-industry collaboration including CSIRO's Data61. Before that, he also worked as a faculty member of the Department of Computer Science and Engineering of Chittagong University of Engineering and Technology. His professional and research interests include cybersecurity, AI/XAI-based modeling, machine learning, data science and behavioral analytics, data-driven decision-making, automation and intelligent systems, digital twin, IoT and smart city applications, critical infrastructure security, and resilience. He has published 100+ journal and conference papers in various reputed venues published by Elsevier, Springer Nature, IEEE, ACM, Oxford University Press, etc. Moreover, Dr. Sarker is a LEAD author of the book "Context-Aware Machine Learning and Mobile Data Analytics", Springer Nature (2021) and "AI-driven Cybersecurity and Threat Intelligence", Springer Nature (2024). He has also been listed in the world's TOP 2% of most-cited scientists in both categories (Career-long achievement and Single-year), published by Elsevier and Stanford University, USA. In addition to research work and publications, Dr. Sarker is also involved in a number of research engagement and leadership roles such as journal editorial, international conference program committee (PC), student supervision, visiting scholar, national and international. He is a member of ACM, IEEE, and Australian Information Security Association (AISA).

Part I

Preliminaries

This first part of the book consists of the introduction to AI-driven cybersecurity and threat intelligence highlighting AI variants with their potentiality (Chap. 1) and basic cybersecurity knowledge including common terminologies used in the area, attack framework, and security life cycle (Chap. 2) to provide the required background knowledge and themes for this book.

Chapter 1

Introduction to AI-Driven Cybersecurity and Threat Intelligence



Abstract With the convergence of artificial intelligence (AI) and cybersecurity, a new paradigm has emerged in how we defend against evolving digital threats. This book explores the dynamic landscape of AI-driven cybersecurity and threat intelligence, emphasizing how the computing and analytical power and decision-making capabilities of AI technologies are revolutionizing the detection, prevention, and response to cyberattacks. AI and machine learning algorithms can analyze vast datasets quickly, identify patterns, and predict potential threats, enabling organizations to strengthen their digital infrastructure proactively. In this book, we have bestowed a comprehensive study on this topic that explores not only the potentiality of cyber threat intelligence but also how different AI methods such as machine learning modeling, deep learning modeling, data science process, generative AI modeling, natural language processing with large language modeling, etc. can be employed to provide intelligent cybersecurity services. We have also discussed various essential real-world application areas such as Internet of Things and smart cities, industrial control systems and operational technology environments, critical infrastructures, cyber-physical systems, digital twins, and relevant others where AI-driven cybersecurity and threat intelligence could be useful for effective and automated solutions. Throughout this book, we have also highlighted relevant research issues and challenges as well as their potential solution directions within the context of AI-based cybersecurity and threat intelligence.

Keywords Cybersecurity · Threat intelligence · AI · Explainable AI · Machine learning · Data science · Intelligent decision-making · Next-generation cyber applications

1.1 Introduction

Technology advancement in today's interconnected and digital environment has created both amazing opportunities and cybersecurity challenges. The threat landscape continues to become more complicated and sophisticated as organizations, governments, and individuals rely on technology more than ever before. Traditional

cybersecurity techniques are no longer sufficient in this high-stakes game of cat and mouse as criminals constantly come up with creative ways to breach defenses. Thus, artificial intelligence (AI)-driven cybersecurity and threat intelligence, a cutting-edge solution that leverages the computing and analytical power of different AI techniques, has emerged as a revolutionary force, transforming the way traditional cybersecurity and threat intelligence are dealt with.

The foundation of AI-driven cybersecurity lies in its capability to learn from historical data, known as machine learning [1], and continuously refine its understanding of normal and malicious behavior across networks, systems, and applications. AI has shown its potential in the field of cybersecurity because of its capability to process enormous volumes of data, identify trends, and adapt its responses. Traditional security methods, while still effective in some cases, often fall behind the constantly evolving strategies used by cybercriminals. AI-driven cybersecurity fills this gap by providing an adaptable and proactive defense approach. Additionally, threat intelligence powered by AI expands cybersecurity's capabilities beyond preventative measures. AI systems can discover new threats, and vulnerabilities, and even anticipate future attack vectors by analyzing data from a variety of sources, including dark web forums, social media, and other online platforms. This predictive capability enables organizations to proactively strengthen their defenses, fix vulnerabilities before they become a problem, and adopt robust strategies to mitigate potential risks.

AI-driven cybersecurity promises a paradigm shift in how we protect digital assets and information. It combines sophisticated machine learning algorithms, deep learning, advanced data analytics, natural language processing, and automation to build a dynamic and adaptive defense system [2]. AI-driven systems can learn and adapt in real time, staying one step ahead of cyber threats, unlike conventional cybersecurity techniques that mainly rely on predetermined rules and signatures. AI systems can detect anomalies and potential threats in real time using machine learning algorithms and deep neural networks, allowing security teams to react quickly and efficiently. AI provides security professionals with the capabilities they need to stay one step ahead of cyber adversaries, from detecting sophisticated malware to identifying unauthorized access attempts. The power of machine learning, deep learning, natural language processing, and other AI approaches [2] are employed in AI-driven cybersecurity and threat intelligence to not only detect and mitigate attacks but also anticipate and prevent them before they can cause damage.

In this exploration of AI-driven cybersecurity and threat intelligence, we will delve into the cutting-edge applications and technologies that are reshaping the way we protect our digital environments. We will investigate how AI boosts threat detection, automates incident response, and provides valuable insights into new threats that assist organizations in gaining a strategic advantage over cyber adversaries. Understanding the role of AI in protecting against cyber threats and utilizing its potential to increase our digital resilience is crucial as we traverse the continually changing cybersecurity landscape. We will further look at the ethical issues and challenges posed by AI-driven security solutions, as well as the ongoing

efforts to achieve a balance between innovation and responsible use. This journey into the world of AI-driven cybersecurity and threat intelligence is intended to shed light on the revolutionary promise of AI and its profound impact on how best to secure the digital realm.

Overall, AI-driven solutions offer a promising path forward, enabling us to defend against a wide range of constantly evolving and more advanced cyber threats. This book aims to present diverse methods for AI-driven cybersecurity and threat intelligence including machine learning and data science modeling along with real-world applications. Thus, this introduction gives readers an exclusive glimpse of the revolutionary possibilities in this emerging area of study. We will also explore a wide range of real-world applications of AI, the difficulties it poses, and the ethical issues that surround its widespread adoption as we delve deeper into this field.

1.2 Cybersecurity and Threat Intelligence

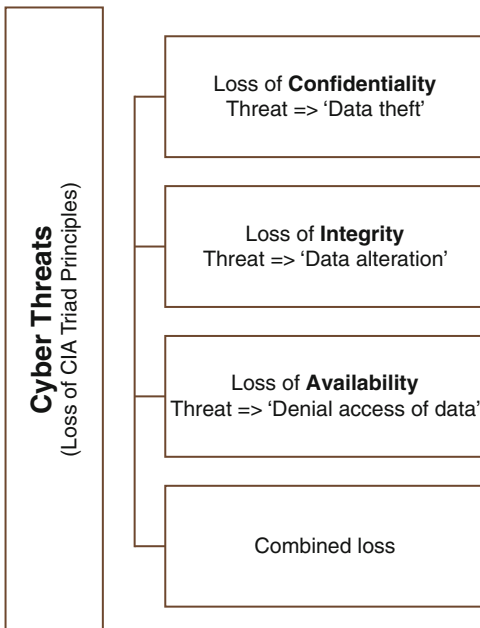
This section defines cybersecurity and threat intelligence from a variety of perspectives, including how they are related.

1.2.1 *What Is Cybersecurity?*

During the recent half-century, our modern and digital civilization has been more interconnected with information and communication technologies (ICT). The prevalence of data breaches and attacks is growing due to the majority of the smart computers and systems we use daily are powered by global Internet access. Therefore, ICT security, defined as the detection and defense of ICT systems against various types of advanced cyberattacks or threats, has been a top priority for our security professionals or policymakers in recent years [2, 3]. Enterprises use ICT security to ensure the confidentiality, integrity, and availability known as the CIA triad of their data and systems by implementing safeguards, policies, and processes. Simply said, cybersecurity is the process of protecting things that are vulnerable due to the use of ICT. Cybersecurity is a term that has a variety of different meanings and is widely used nowadays; several key terms such as “information security,” “data security,” “network security,” and “Internet or IoT security” [4] are frequently interchanged, confusing readers and professionals in the field. Among these, the term “cybersecurity” has higher global popularity than others and is growing day by day [5].

Cybersecurity has been characterized in a variety of ways by various researchers. For example, cybersecurity refers to the various activities or policies that are implemented to protect ICT systems from threats or attacks [6]. Craigen et al. [7] defined “cybersecurity as a set of tools, practices, and guidelines that can be used to protect computer networks, software programs, and data from attack, damage,

Fig. 1.1 An illustration of cyber threats with the loss of CIA (confidentiality, integrity, and availability) triad principles used to drive information security policy within an enterprise, adopted from Sarker et al. [2]



or unauthorized access.” According to Aftergood et al. [8], “cybersecurity is a set of technologies and processes designed to protect computers, networks, programs and data from attacks and unauthorized access, alteration, or destruction.” Thus, cybersecurity is concerned with identifying various cyberattacks or threats as well as the related defense tactics to prevent them and, ultimately, secure the systems, which is associated with confidentiality, integrity, and availability. The CIA triad exploring confidentiality, integrity, and availability as mentioned is the core principle used to drive information security policy within an enterprise, where the individual losses of these principles or their combinations are considered a threat. Such cyber threats are also known as “data theft,” “data alteration,” and “denial access of data,” respectively, as shown in Fig. 1.1. Therefore, based on the CIA triad for the security policy stated above, we can conclude that “confidentiality” protects data, objects, and resources from unauthorized access and misuse; “integrity” protects data from unauthorized changes; and “availability” ensures accessibility to the systems and the resources to authorized users or the appropriate entity. Overall, cybersecurity can be defined as the practice of protecting computer systems, networks, and digital information from unauthorized access, attacks, damage, or theft. It involves implementing a combination of technologies, processes, and practices to safeguard against cyber threats and ensure data confidentiality, integrity, and availability, as defined above.