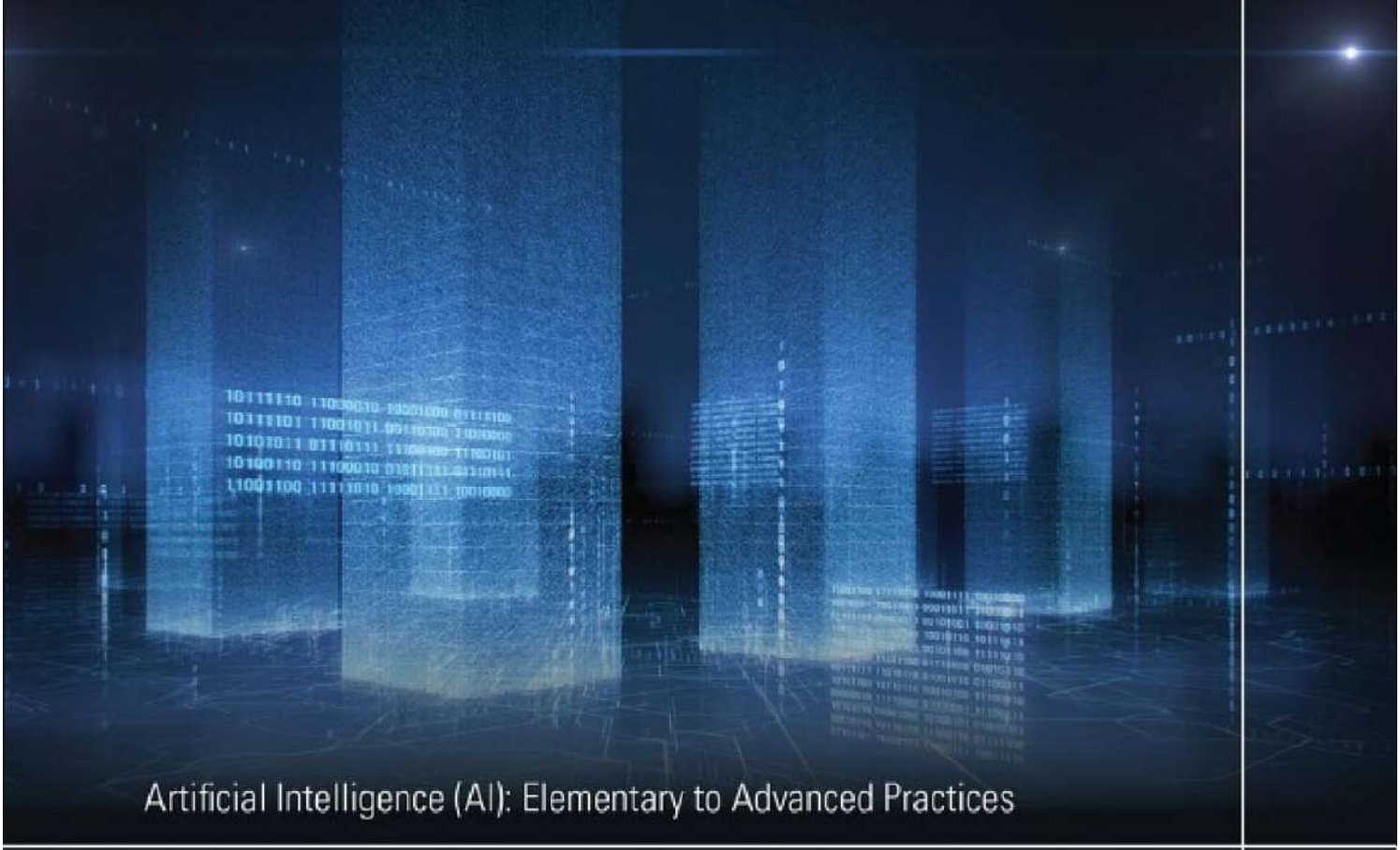

Artificial Intelligence (AI): Elementary to Advanced Practices

CYBERSECURITY

Ambient Technologies, IoT, and Industry 4.0 Implications

Edited by

Gautam Kumar
Om Prakash Singh
Hemraj Saini

CRC Press
Taylor & Francis Group

First edition published 2021
by CRC Press
6000 Broken Sound Parkway NW, Suite 300, Boca Raton, FL 33487-2742

and by CRC Press
2 Park Square, Milton Park, Abingdon, Oxon, OX14 4RN

CRC Press is an imprint of Taylor & Francis Group, LLC

Library of Congress Cataloging-in-Publication Data
Names: Kumar, Gautam, 1990- editor. | Singh, Om Prakash, editor. | Saini,Hemraj, 1977- editor.
Title: Cybersecurity : ambient technologies, IoT, and industry 4.0implications / edited by Gautam Kumar, Om Prakash Singh, Hemraj Saini.
Other titles: Cybersecurity (CRC Press)
Description: First edition. | Boca Raton : CRC Press, 2022. | Series:Artificial intelligence (AI) : elementary to advanced practices |Includes bibliographical references and index.
Identifiers: LCCN 2021019345 (print) | LCCN 2021019346 (ebook) | ISBN9780367702168 (hbk) | ISBN 9780367702175 (pbk) | ISBN 9781003145042 (ebk)
Subjects: LCSH: Internet of things--Security measures. | Industry4.0--Security measures.
Classification: LCC TK5105.8857 .C96 2022 (print) | LCC TK5105.8857(ebook) | DDC 005.8--dc23
LC record available at https://lccn.loc.gov/2021019345
LCebook record available at https://lccn.loc.gov/2021019346

ISBN: 978-0-367-70216-8 (hbk)
ISBN: 978-0-367-70217-5 (pbk)
ISBN: 978-1-003-14504-2 (ebk)

DOI: 10.1201/9781003145042

Typeset in Times
by SPi Technologies India Pvt Ltd (Straive)

Contents

Preface

Humankind has ventured into the time of the Industrial Revolution 4.0. Industry 4.0 could be a standard term to portray the fourth-generation Industrial Revolution that we are encountering these days. With each passing day, innovations such as cloud computing, the IoT, and mechanical technology are disturbing the conventional manufacturing process. With computerization, the IoT, and data analytics making production methods more and more intelligent, smart, and productive, the Industrial Revolution 4.0 has been evidently apparent. To all intents and purposes, this transitional move to digitization and robotization is known as "Industry 4.0."

However, this stage of the industrial revolution has introduced challenges, especially in terms of cybersecurity threats. Around the world, cybersecurity specialists have been concerned around the suggestions of Industry 4.0. In an age where everything is hyper-connected, industries have recently become more defenseless than ever. In other words, digitally connected industries are more vulnerable to assailants who are looking to abuse assets and information. As a result, the need for compelling cybersecurity measures inside an IIoT-enabled generation environment is posing a genuine threat to new-age industrial revolution systems and methods.

Nowadays, smart manufacturing plants and supply chains are consistently associated by means of an Industrial Internet of Things (IIoT) that makes use of IP addresses to associate and communicate inside and outside the production line. These internet-connected gadgets are always vulnerable to unauthorized access without legitimate cybersecurity measures.

Therefore, we attempt to provide a significant effort to identify and combat these risks, in the form of present book, *Cybersecurity: Ambient Technologies, IoT & Industry 4.0 Implications*. The book contains 12 chapters.

Chapter 1 covers the general security services and modeling aspects associated with any system. It also looks at the latest research done on such services and security models. The chapter explores the risks associated with a system and how, for a specific use-case of virtual reality implementation, we help the reader to see what risks can be mapped out and tackled. This chapter acts as a baseline for an individual to understand security services, the risks associated with a system, and the security models available, which can be used while designing a system.

Chapter 2 discuses the IDS approach, and methodology and different types of computer and network attacks. The latest trends, issues, and future research issues regarding intrusion detection systems are also presented. The chapter addresses the emerging research issues in designing reliable and accurate ID systems.

Chapter 3 defines the ethics and techno-ethics concepts, along with the main challenges and issues for ethics in technology. The chapter explains the main applications of cybersecurity, considering two main types: secure web applications and secure mobile applications. Finally, it explores the ethics for cybersecurity applications. This includes user privacy, freedom of speech, intellectual property rights, legal protections, and responsibility for crimes.

Chapter 4 presents the dependency on the technology that defines cloud computing and the IoT. Consumers face challenges from the risk of security flaws surrounding data

privacy, loss, theft of intellectual property, insecure APIs, etc. These can become huge risks for any organization, as described in the chapter.

Chapter 5 discusses the software's Internet of Things, hardware, telecommunication network, and related technology issues required for these projects. Smart mobility applications and data are integral parts of the system, and therefore, problems related to data and their privacy may arise. The chapter deals with the security concerns of the public, legal issues, etc. Finally, the chapter discusses various levels of regulatory requirement and their roles.

Chapter 6 discusses various models of digital forensics, underlying principles, the concept of cryptography, and its impact on the domain of digital forensics. The chapter also addresses the impact of related technologies on human life, as Industry 4.0 has had a tremendous impact on these areas, enabling them, as well as enforcing the acceptance of such smart technologies in various aspects of our lives.

Chapter 7 proposes a mathematical model for malware attacks through the IoT, considering proper vaccination. The existence and uniqueness of the model have been proven. The infection-free and endemic equilibrium points have been found successfully. This model explains how the basic reproduction number determines the local and global stability of the system in IoT devices. It adapts the vaccination-based IoT devices in the network for protecting against malware attacks. The numerical simulations are critically analyzed and performed to validate the developed model.

Chapter 8 endeavors to build up a mechanized framework on rice plant disease detection using the IoT, which recognizes the presence of infection in the leaves and soil. There are various factors that determine pH, temperature, moisture, DHT 11, and TCS 3200 to detect the current position of the soil and plant. Those sensor values are sent, using an Ethernet shield, to be stored on an IoT server. Here, we have created a framework to detect the current condition of the plants' environment. We then analyze the current situation of the environment by comparing it with the healthy plant's actual values and show it on our constructed platform.

Chapter 9 focuses on the security issues of e-health care systems and provides the methodology to assure security. Various security protocols have been proposed, including an energy-efficient routing protocol, a secure protocol for user authentication and key agreement, a node-to-node authentication protocol, eliminating the man-in-middle attack, a lightweight anonymous authentication protocol for network security, and a trust key management protocol for biomedical smart devices. Finally, the chapter also discusses security protocols for biomedical smart devices.

Chapter 10 discusses different access control mechanisms associated with the health care system. In today's world, data has become the most important thing. Therefore, data privacy and security are crucial. In any information system, the satisfactory security of data, as well as access control by the owner of the data, are the primary requisites. Health care information systems have very crucial data on the patient. Therefore, the chapter concentrates on electronic health record information systems, which require the development of a strong mechanism to protect unauthorized access to the data.

Chapter 11 identifies approaches combining several classification techniques with PSO for intrusion detection. A general presentation of the PSO algorithm is provided. PSO-based techniques for intrusion detection are introduced and detailed. The most common datasets and evaluation measures are discussed. Finally, a summary discussion about PSO-based intrusion detection techniques is provided, along with possible directions and insights.

Chapter 12 introduces the various types of vulnerabilities and their mitigation techniques. The biggest challenge for an organization is to prevent the web applications or portals from unauthorized activities, because web applications are available to all users

24/7, through the internet. Therefore, violating an implicit or explicit security policy is discussed, to counter the system's hardware or software vulnerabilities.

We hope that the works published in this book will serve the communities concerned with cybersecurity, the IoT, and Industry 4.0.

Editors

Dr. Gautam Kumar is currently Associate Professor at CMR Engineering College, Hyderabad, India. He received his PhD in Computer Science and Engineering from Jaypee University of Information Technology, Himachal Pradesh, India, in 2017. He received his M.Tech from Rajasthan Technical University, in 2012, and B.E. from Rajiv Gandhi Proudyogiki Vishwavidyalaya, Madhya Pradesh, in 2005. He has more than 15 years of academic experience. His research interests are in the fields of Cryptography, Information Security, Algorithms Design and Analysis. He has published more than 45 research journal articles and conference papers in Science Citation, Scopus, and Indexed Journals. He has also served as a president of Institute's Innovation Council, Ministry of Human Resource Development (MHRD), India and acted a Convenor/SPOC to the Smart-India Hackathon.

Dr. Om Prakash Singh is a Postdoc Research Associate in Medical Device Engineering at the University of Edinburgh, Edinburgh, Scotland, UK. He received a BA in Science, an MA in Physics and Biomedical Engineering, and a PhD in Biomedical Engineering, in

2005, 2007, 2009, and 2019, respectively. He has six years of teaching experience and four years of research experience. He has also filed 1 IP and obtained 2 copyrights for his research work. He has been awarded 2 gold awards and 1 merit award for his research. His research interests include the development of handy medical devices using optical-based sensors, by deploying signal-processing algorithms, and machine learning techniques for the automatic classification of cardiopulmonary conditions. To date, he has authored and coauthored around 19 researched and reviewed manuscripts, with an accumulated impact factor of 14.573.

Dr. Hemraj Saini is Associate Professor in the Department of Computer Science and Engineering, Jaypee University of Information Technology-(H.P), India. He received a PhD in Computer Science from Utkal University, Bhubaneswar (Orissa) in 2012, an M.Tech in IT from Panjabi University, Patiala, Panjab in 2005, and a B.E. in CSE from the National Institute of Technology, H.P., in 2000. His research interests include Network Security, Information Security, Cybersecurity, the Internet of Things (IoT), Cloud Computing, Big Data, etc. He was awarded an Academic Excellence Award for Projects, a Merit cum Scholarship Award, and a National Scholarship. He has more than 20+ years of teaching and R&D experience at the national (Rajasthan, Orissa, H.P.) and international levels (Libya). He has published more than 160 research papers in journals and 45 conferences of international repute. He is in editorial member of reputed journals and conferences, with a great number of research collaborations. He has produced five PhD candidates, 4 of whom are under supervision, guided 13 M.Tech student projects, and guided 45 UG projects.

Contributors

Abhijit Chirputkar
Symbiosis Institute of Digital and Telecom Management
Symbiosis International (Deemed University)
Pune, India
director@sidtm.edu.in

Dr. Arjun Singh
Computer and Communication Engineering Department
Manipal University Jaipur, India
vitarjun@gmail.com

Binayak Dihudi
Department of Mathematics
Konark Institute of Science and Technology
Jatni, Bhubaneswar, India
bdihudi@gmail.com

Bipin Kumar Rai
IT department
ABES Institute of Technology
Ghaziabad, UP, India
bipinkrai@gmail.com

Dinesh Kumar Saini
Computer and Communication Engineering Department
Manipal University Jaipur, India
dineshkumar.saini@jaipur.manipal.edu

FarjanaYeasmin Trisha
East West University
Dhaka, Bangladesh
farjana186@gmail.com

Jabar H Yousif
Computing and Information Technology Department
Sohar University, Oman
jyusif@su.edu.om

Dr. Kamaljit Singh Saini
University Institute of ComputingChandigarh University
Punjab, India
kamaljit.cse@cumail.in

Mahmudul Hasan
Jahangirnagar University
Dhaka, Bangladesh
mahmudul2843@gmail.com

Maram Bani Younes
Information Technology, Philadelphia University
Amman, Jordan
mbaniyounes@philadelphia.edu.jo

Nameer N. El-Emam
Information Technology
Philadelphia University
Amman, Jordan
nemam@philadelphia.edu.jo

Dr. Prabhjot Kaur
IT Department
MSIT, GGSIP University
New Delhi
prabhjot.kaur@msit.in

Poonam Sharma
University Institute of Computing
Chandigarh University
Punjab, India
poonam4sharma1987@gmail.com

Praveen Gupta
Department of Computer Engineering
Poornima Institute of Engineering and Technology
Jaipur, India
praveen2gupta@gmail.com

Dr. Punit Gupta
Computer and Communication Engineering Department
Manipal University Jaipur, India
punitg07@gmail.com

Raneem Qaddoura
Information Technology
Philadelphia University
Amman, Jordan
rqaddoura@philadelphia.edu.jo

Reena Sharma
Department of Computer Engineering
Poornima College of Engineering
Jaipur, India
shreena275@gmail.com

Samaya Pillai

Symbiosis Institute of Digital and Telecom Management
Symbiosis International (Deemed University)
Pune, India
samaya.pillai@sidtm.edu.in

Sachin Kumar Sharma
Manipal University Jaipur and Cybersecurity Analyst at Dr CBS Cyber Security Services LLP
Jaipur, India
sachin_43721@yahoo.com

Suman De
Development Specialist
SAP Labs India Pvt. Ltd.,
Bangalore, India
suman.de@sap.com

Tarini Charan Panda
Department of Mathematics
Ravenshaw University
Cuttack, India
tc_panda@yahoo.com

Tanu Solanki
IT Department
Galgotia College of Engineering and Technology
Greater Noida, UP, India
tanucsengg@gmail.com

Venkatesh Iyengar
Symbiosis Institute of International Businesses
Symbiosis International (Deemed University)
Pune, India
venkatesh.iyengar@siib.ac.in

Dr. Vijay Kumar Sharma
Computer and Communication Engineering Department
Manipal University Jaipur, India
Vijaymayankmudgal2008@ gmail.com

Yerra Shankar Rao
Department of Mathematics
Gandhi Institute of Excellent Technocrats
Ghangapatana, Bhubaneswar, India
Email: sankar.math1@gmail.com