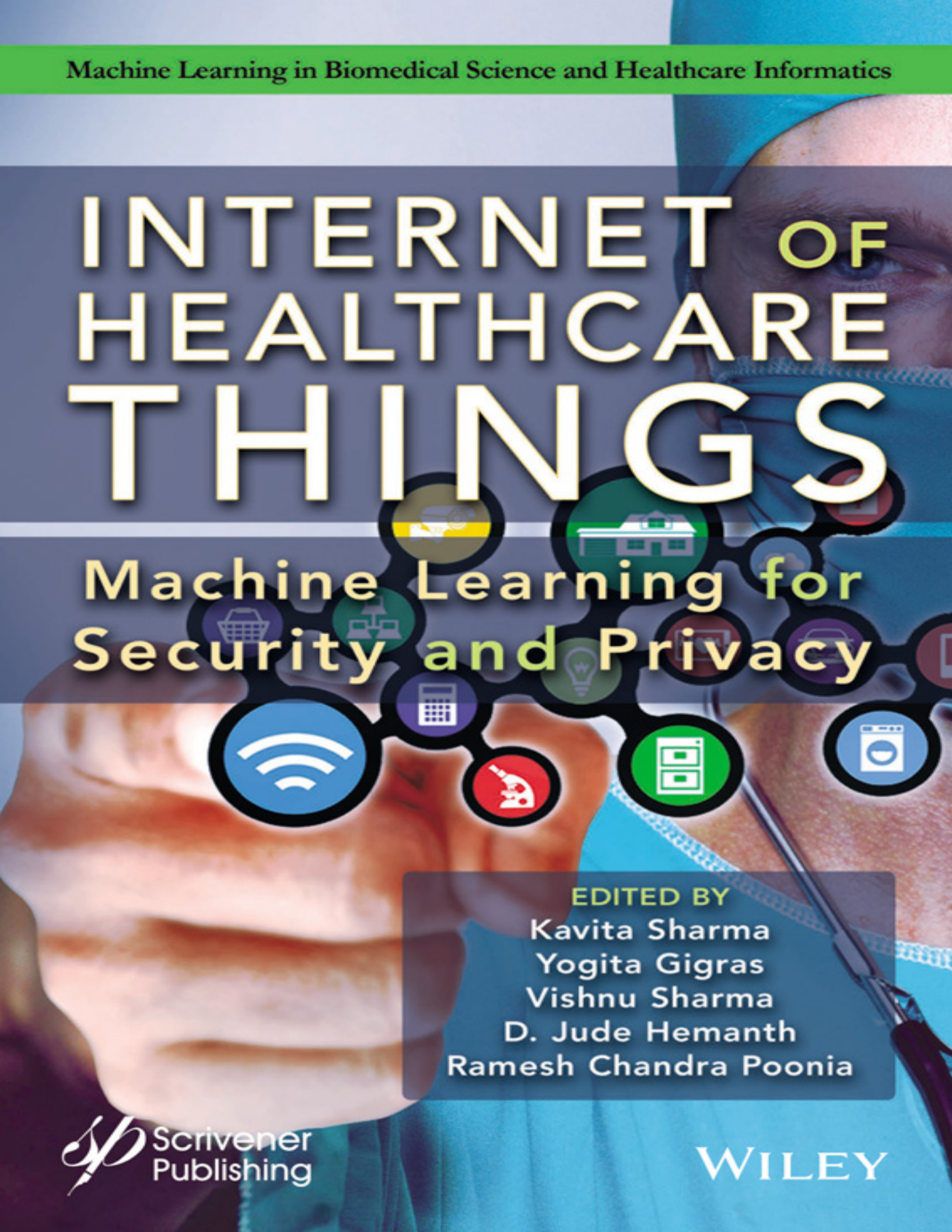
Machine Learning in Biomedical Science and Healthcare Informatics

INTERNET OF HEALTHCARE THINGS

Machine Learning for Security and Privacy



EDITED BY
Kavita Sharma
Yogita Gigras
Vishnu Sharma
D. Jude Hemanth
Ramesh Chandra Poonia

Scrivener Publishing

WILEY

Table of Contents

List of Illustrations

List of Tables

Scrivener Publishing
100 Cummings Center, Suite 541J
Beverly, MA 01915-6106
Publishers at Scrivener
Martin Scrivener (martin@scrivenerpublishing.com)
Phillip Carmical (pcarmical@scrivenerpublishing.com)

Internet of Healthcare Things

Machine Learning for Security and Privacy

Edited by

Kavita Sharma,

Yogita Gigras,

Vishnu Sharma,

D. Jude Hemanth

and

Ramesh Chandra Poonia

WILEY

This edition first published 2022 by John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, USA and Scrivener Publishing LLC, 100 Cummings Center, Suite 541J, Beverly, MA 01915, USA

For more information about Scrivener publications please visit www.scrivenerpublishing.com.

Wiley Global Headquarters

111 River Street, Hoboken, NJ 07030, USA

For details of our global editorial offices, customer services, and more information about Wiley products visit us at www.wiley.com.

Limit of Liability/Disclaimer of Warranty

While the publisher and authors have used their best efforts in preparing this work, they make no representations or warranties with respect to the accuracy or completeness of the contents of this work and specifically disclaim all warranties, including without limitation any implied warranties of merchant-ability or fitness for a particular purpose. No warranty may be created or extended by sales representatives, written sales materials, or promotional statements for this work. The fact that an organization, website, or product is referred to in this work as a citation and/or potential source of further information does not mean that the publisher and authors endorse the information or services the organization, website, or product may provide or recommendations it may make. This work is sold with the understanding that the publisher is not engaged in rendering professional services. The advice and strategies contained herein may not be suitable for your situation. You should consult with a specialist where appropriate. Neither the publisher nor authors shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages. Further, readers should be aware that websites listed in this work may have changed or disappeared between when this work was written and when it is read.

Library of Congress Cataloging-in-Publication Data

ISBN 978-1-119-79176-8

Cover image: Pixabay.Com

Cover design by Russell Richardson

Set in size of 11pt and Minion Pro by Manila Typesetting Company, Makati, Philippines

Printed in the USA

10 9 8 7 6 5 4 3 2 1

Preface

In recent years, the use of the Internet of Things (IoT) has been on the rise worldwide, bringing with it new challenges and possibilities along with new cybersecurity risks in the area of IoT-enabled healthcare. These new challenges involve smart connectivity, high security, and confidentiality, generating big data, reducing total data latency between machine-to-machine interfaces, and reducing bandwidth, complexity, and power consumption. In the healthcare sector, the IoT has made it possible for devices to monitor patient's health remotely, unleashing the capability to ensure their health and allowing physicians to deliver unmatched care. These IoT devices are more efficient for identifying disease in less time with more precision and have an absence of network segmentation, inadequate access control of legacy systems, and an increased susceptible surface area that cyber attackers exploit. Therefore, even though the IoT has significantly impacted healthcare costs and improving treatment results, IoT-enabled healthcare devices' greatest common threats are data safety and confidentiality. Since these devices communicate and obtain data in real-time, cybercriminals can break into the system and steal the Personal Health Information (PHI) of both patients and their doctors. Even so, the IoT is certainly improving the healthcare sector by redefining the scope of the devices.

Another significant threat is the combination of numerous network devices, which creates difficulties in implementing the IoT in the healthcare sector. The enormous amount of data produced by these devices can also impede the ability of doctors to identify diseases. So, this book addresses these issues and provides solutions through authentication

and authorization mechanisms, blockchain, fog computing, machine learning algorithm, etc. Machine learning-enabled IoT devices deliver the information concealed in data for fast, computerized responses and enhanced decision-making. This information might be used to plan for upcoming patterns, distinguish anomalies, and expand intelligence by audio, image and video analyses. The IoT permits devices to send information to isolate blockchain networks to generate tamper-resistant accounts of collective transactions. Blockchain empowers business associates to access and share IoT data but without the necessity of central management and control.

As the world is entering the fourth industrial revolution-otherwise known as Industry 4.0-the combination of the IoT with other technologies, such as cybersecurity, big data, cloud computing and blockchain, is fundamentally changing the healthcare industry. The development of these fields is critical in healthcare because it improves the quality and efficiency of treatments and improves the patients' health.

Objective of the Book

This book's main objective is to motivate the reader to use telemedicine facilities to monitor patients in remote areas and gather clinical data for further research. To this end, it provides an overview of the Internet of Healthcare Things (IoHT) and discusses the significant threats: the data security and data privacy of health records. Another major threat is the combination of numerous devices and protocols, precision time, data overloading, etc. In the IoHT, multiple devices are connected and communicate through specific protocols. Therefore, the application of emerging technologies to mitigate these threats and provide secure data communication over the network is

discussed. This book also discusses the integration of machine learning with the IoHT for analyzing vast amounts of data for predicting diseases more accurately. Case studies are also given to verify the concepts presented in the book.

Organization of the Book

The 12 chapters of the book are organized into three sections. The first section consists of three chapters on data security and privacy concerns in the IoHT. The second section contains five chapters describing the application of machine learning, blockchain, and fog computing in the IoHT. The third section discusses the latest case studies in the healthcare sector.

Section 1: Security and Privacy Concerns in the IoHT (Chapters 1–3)

- Chapter 1 discusses the changes and standards required for the healthcare sector, covering privacy and security concerns, requirements, existing solutions, future challenges, and privacy-preserving methods. This chapter focus to enhance the knowledge of monitoring for adverse medical events and leading to a rise in the quality of treatment for diseases.
- Chapter 2 states that the purpose of the IoHT is to enrich the users' experience by providing a responsive, discernible, seamless information service and denial of service to unauthorized proponents. In terms of security, the protection for IoT systems in the healthcare sector emanates from both physical and virtual access. Devices and equipment engaged in the IoHT will only be made accessible to authorized personnel, and this denial of physical access to strangers would in itself ensure the avoidance of cyber intrusion in a significant number of cases. The next layer of protection is at the virtual level, wherein the identity of the access seeker is authenticated by secured protocols and standard measures deployed in the system's design.
- Chapter 3 discusses security and privacy issues at every stage of healthcare data's big data life cycle. This chapter also provides an overview of different laws applicable to the protection of healthcare data in different countries, such as the Health Insurance Portability and Accountability Act (HIPAA), Data Protection Act (DPA), Personal Information Protection and Electronic Documents Act (PIPEDA), etc. The chapter focuses on finding a reasonable explanation for

data protection and security behind crucial health information in the future.

Section 2: Application of Machine Learning, Blockchain and Fog Computing in the IoHT (Chapters 4–8)

- Chapter 4 gives an overview of the Internet of Things (IoT) and its applications in several fields, and the security challenges faced while deploying it. Then the chapter focuses on its application in the healthcare field. The architectural design of IoT-enabled healthcare is illustrated along with the benefits, necessities and several challenges faced when using it. The security protocols that researchers have designed for intrusion detection in the IoHT are discussed, along with the further application of machine learning and its contribution to intrusion detection in the IoHT. Moreover, a direction is given for future research towards designing a secure IoHT framework with low latency and fast processing ability for accurate end-to-end data delivery.
- Chapter 5 presents a sentiment analysis and topic modelling-based approach for early warning of a health crisis, which can be integrated with the IoHT's framework and can be fruitful in assisting medical specialists. In this research, information related to the IoHT is collected, followed by dataset generation. Modelling is performed on the proposed IoHT dataset for predicting trends in IoHT domains. Sentiment analysis towards the IoHT's applicability is evaluated to find the overall sentiment orientation of people. In the current pandemic situation, variations in the sentiment orientation of users towards IoHT systems are evaluated, and analysis is carried out to determine the effectiveness of these systems.

- Chapter 6 focuses on telemedicine, providing medical services and clinical data and administering medicine to patients in the current pandemic. It is a cooperative for communication between specialists, drug specialists, patients, and individuals in remote regions. Telemedicine systems are progressively being used by patients, clinicians, and organizations. This chapter illustrates the few steps, which can consider in the case of emergence.
- Chapter 7 discusses blockchain networks in the healthcare sector, focusing on the multilayer IoT/blockchain grounded on architecture customized and planned to be utilized in the medical field. The role of several parties and health service providers, doctors, insurance companies, and pharmacies are integrated with this work. The decisive goal is to crack the problem of performance and scalability. This chapter addresses the convergence across different elements, such as modern architecture, device designs, process, scheme, paradigm, platform, approach, protocol, and algorithm, upon the mechanism designs of decentralized healthcare implementation. It also discusses suitable security solutions, like lightweight cryptographic procedures and protocols, which are challenged with lowering the overhead in the rankings of computations and resources. This leads to the inference that designing an effective intrusion discovery/prevention system that collaborates with dynamic data processing is required. The chapter concludes with a blockchain-based security solution is proposed that is divided into three distinct layers to distinguish and avoid attacks and authorize patient details when registered in cloud-based applications.
- Chapter 8 reviews healthcare systems and their challenges, followed by blockchain and its integration

with healthcare. Blockchain can be securely implemented in healthcare systems for sharing, storing, and creating electronic medical records and prescriptions, personalized medicine, remote monitoring, mobile health applications, and the Internet of Medical Things (IoMT), which are vital to improving the quality of patient care. Fraud detection, insurance claims, medical transactions, checking for counterfeit drugs, and tracking, along with other uses for patients, doctors, and healthcare institutes, can also be achieved by using blockchain in healthcare. This chapter ends with a discussion of the challenges faced when implementing blockchain in healthcare.

Section 3: Case Studies on Healthcare (Chapters 9–12)

- Chapter 9 addresses the dark web. The internet is an open platform for communicating across boundaries. Without the usual security checks, the anonymous part of the internet, called the dark web, is used by cybercriminals to perform illicit activities. Security research agencies are continuously designing and executing covert operations to track criminals. For instance, organ trafficking is sometimes used by patients who urgently need a quick organ transplant, but due to the scarcity and long-term storage deficiency, healthy living donors are required who are trafficked from multiple nations to avoid being tracked by security agencies. Here, the rich pay the cost of the organ to the donor. But the secure communication and exchange occur using intermediate agents who manage safe locations, operating doctors, and the patient's travel and recuperation after the operation. So, this chapter discusses the illicit trafficking market, including other criminal activities done over dark web platforms.
- Chapter 10 provides an overview of deep learning algorithms, neural networks, random forest, and decision tree classifiers for analyzing patients' data to predict heart disease. This chapter shows how the medical practitioner can detect heart disease by attaining precise troponin levels and prescribe effective medicine according to the foreseen disease. The study results presented in this chapter demonstrate that heart disease can be predicted with 90% accuracy.
- Chapter 11 describes how the Internet of Things (IoT) has transformed the routine and lifestyle of individuals

and its involvement in the arena of healthcare. It is grounded on different machine learning applications, and information is mined for real-time scrutiny of data and secluded health supervision constructed on IoT infrastructure. It helps in forecasting schemes for using machine learning methods, like MLP, Bayes net, SVM, J48, decision trees, etc., in experimental results for breast cancer. In this chapter, features selection, growing efficiency, and deep neural network classification approaches will be exploited to further boost the investigative procedure's performance for breast cancer diagnosis.

- Chapter 12 aims to enhance the reader's understanding of how the Internet of Things (IoT) is used in various medical treatment areas, such as brain cancer. To be trusted Internet of Healthcare Things (IoHT), machine learning algorithms have settled on a colossal commitment to decision-making, which has been clarified through a portion of the contextual investigations in this chapter. This chapter explains the exact therapy of brain tumors, beginning with the types to the best reasonable investigative techniques and survival rates.

We would like to thank all the authors who kindly contributed their chapters to this book. We are also grateful to the publishing and production teams at Scrivener Publishing Group for their assistance in the preparation and publication of this book.

Dr. Kavita Sharma
Department of CSE, Galgotias College of Engineering & Technology,
Greater Noida, India
Dr. Yogita Gigras
Department of CSE and IT, The NorthCap University,

Gurugram, India
Dr. Vishnu Sharma
Department of CSE, Galgotias College of Engineering & Technology,
Greater Noida, India
Dr. D. Jude Hemanth
Department of ECE, Karunya University,
Coimbatore, India
Dr. Ramesh Chandra Poonia
CHRIST (Deemed to be University),
Bangalore, Karnataka, India

Section 1
SECURITY AND PRIVACY CONCERN IN IoHT