DECENTRALIZED COLLABORATIVE LEARNING FOR DATA PRIVACY AND SECURITY

Edited By
Bipin Kumar Rai, Rupa Rani, and Chin-Shiuh Shieh

Scrivener Publishing

WILEY

Decentralized Collaborative Learning for Data Privacy and Security

Scrivener Publishing
100 Cummings Center, Suite 541J
Beverly, MA 01915-6106

Publishers at Scrivener
Martin Scrivener (martin@scrivenerpublishing.com)
Phillip Carmical (pcarmical@scrivenerpublishing.com)

Decentralized Collaborative Learning for Data Privacy and Security

Edited by

Bipin Kumar Rai

Rupa Rani

and

Chin-Shiuh Shieh

WILEY

This edition first published 2026 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.

The manufacturer's authorized representative according to the EU General Product Safety Regulation is Wiley-VCH GmbH, Boschstr. 12, 69469 Weinheim, Germany, e-mail: Product_Safety@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 merchantability 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 978-1-394-46468-5

Cover image: Generated with AI using Adobe Firefly
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

Contents

Preface

As artificial intelligence systems grow more capable, they increasingly depend on vast quantities of data to learn, adapt, and make decisions that affect real lives. Yet the very act of centralizing data for AI training introduces profound risks: breaches of privacy, erosion of trust, single points of failure, and a growing imbalance of power between those who own data and those who control the systems that process it.

This book was born from a conviction that it does not have to be this way. Over the past decade, two transformative technologies, federated learning and blockchain have matured independently to a point where their convergence offers something genuinely new: a pathway to AI systems that are simultaneously intelligent, privacy-preserving, transparent, and trustworthy. *Decentralized Collaborative Learning for Data Privacy and Security* is an attempt to chart that pathway in a rigorous, practical, and accessible manner.

The Problem We Set Out to Solve

Conventional centralized AI architectures were designed in a world where aggregating data in one place was both feasible and acceptable. Regulatory frameworks such as GDPR, HIPAA, and emerging cross-border data governance treaties now impose strict constraints on where data may reside and how it may be used. At the same time, high-profile breaches have demonstrated that centralized repositories are attractive targets, and that the consequences of failure are not merely financial but deeply human affecting patients, consumers, and communities.

Federated learning addressed part of this challenge by enabling model training across distributed nodes without requiring raw data to leave its source. Yet federated learning alone carries its own vulnerabilities: model updates can leak information, participants may act dishonestly, and the absence of a neutral coordinating authority makes accountability difficult to enforce. Blockchain technology, with its decentralized consensus mechanisms, immutable audit trails, and programmable smart contracts, offers precisely the missing layer of trust and governance that federated systems need.

This book addresses the challenge of bringing these two paradigms together in a coherent, deployable framework—one that preserves data sovereignty, ensures verifiable integrity of model contributions, and supports cross-organizational collaboration without demanding blind trust in any single party.

What this Book Covers

The book is organized as a deliberate journey from foundations to frontiers. Early chapters establish the conceptual bedrock: the principles of collaborative machine learning, the landscape of data privacy threats and protections, and the mechanics of blockchain technology. Readers who are new to any of these fields will find these chapters sufficient to build genuine fluency; readers who are already specialists will benefit from seeing their domain placed in dialogue with the others.

The middle sections move into the architecture of integrated systems—how blockchain-enhanced federated learning frameworks are designed, how consensus mechanisms are adapted for edge intelligence, and how advanced cryptographic primitives such as differential privacy, homomorphic encryption, zero-knowledge proofs, and secure multiparty computation are applied in practice. These chapters are the technical heart of the book, and they are written with the assumption that readers wish not merely to understand these techniques but to implement them.

The later chapters turn to application domains—healthcare, finance, IoT, smart cities, and education—demonstrating through concrete case studies how decentralized collaborative AI is already transforming these sectors and what obstacles remain. Dedicated attention is also given to the legal, regulatory, and ethical dimensions that any practitioner or researcher must navigate: cross-border data governance, liability in autonomous AI systems, algorithmic fairness, and the evolving regulatory environment across jurisdictions.

The book closes by looking ahead—at decentralized autonomous AI networks, the integration of the Economy of Things, and quantum-resistant privacy solutions—equipping readers not only for the present state of the field but for the directions in which it is rapidly moving.

Who this Book is For

This book is written for graduate students, academic researchers, data scientists, AI engineers, and technology professionals who want to engage seriously with the intersection of distributed AI and privacy-preserving technology. It assumes comfort with the basics of machine learning and programming, but does not presuppose deep expertise in cryptography,

distributed systems, or blockchain development—those foundations are built carefully within the text itself.

Policy professionals and ethicists working on AI governance will find the legal and ethical chapters directly relevant to their work. Practitioners in healthcare, finance, and the public sector who are evaluating decentralized AI solutions for their organizations will find the application chapters particularly actionable. And for those building the next generation of Web3-native AI systems, the later chapters on incentive mechanisms, token economics, and decentralized autonomous networks offer a rigorous grounding for that emerging space.

How to Use this Book

The chapters are sequenced to be read in order, but each is also written to stand on its own for readers who wish to focus on particular topics. Readers who are entirely new to federated learning are encouraged to begin with the foundational chapters before tackling the cryptographic sections. Those already working in blockchain development may find it productive to begin with the chapters on federated learning integration and then loop back to the privacy-preserving methods as needed. The ethical and legal chapters are recommended for all readers, regardless of their primary technical focus, because the deployment of these systems does not occur in a social vacuum.

Acknowledgements

A work of this scope is never the product of its authors alone. We are deeply grateful to the researchers, engineers, and practitioners whose published work forms the foundation of every chapter. We thank our academic colleagues and industry collaborators for their insights, critiques, and encouragement throughout the writing process. Finally, we thank our readers—students, researchers, builders, and policymakers—for bringing the curiosity and seriousness of purpose that a subject of this importance deserves. The challenge of building AI systems that are both powerful and trustworthy is one of the defining technical and ethical tasks of our time. We are glad to be thinking through it together.

The Editors
Bipin Kumar Rai
Rupa Rani
Chin-Shiuh Shieh