



# 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

© 2026 Scrivener Publishing LLC

For more information about Scrivener publications please visit [www.scrivenerpublishing.com](http://www.scrivenerpublishing.com).

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, except as permitted by law. Advice on how to obtain permission to reuse material from this title is available at <http://www.wiley.com/go/permissions>.

### **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](http://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](mailto: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

|                                                                                       |            |
|---------------------------------------------------------------------------------------|------------|
| <b>Preface</b>                                                                        | <b>xxv</b> |
| <b>1 Cross-Border Healthcare Data Sharing Using Blockchain and Federated Learning</b> | <b>1</b>   |
| <i>Bipin Kumar Rai, Chin-Shiuh Shieh and Anoop Kumar Srivastava</i>                   |            |
| 1.1 Introduction                                                                      | 2          |
| 1.2 Related Work                                                                      | 3          |
| 1.3 Role of Blockchain in Cross-Border Federated Learning in Healthcare               | 7          |
| 1.4 Major Research Trends                                                             | 9          |
| 1.5 Common Datasets and Benchmarks                                                    | 10         |
| 1.6 Prevailing Challenges and Open Research Gaps                                      | 10         |
| 1.6.1 Privacy Leakage through Model Updates                                           | 11         |
| 1.6.2 Scalability and Performance Limitations                                         | 11         |
| 1.6.3 Heterogeneity of Data, Systems, and Participants                                | 12         |
| 1.7 Promising Directions for Future Work                                              | 13         |
| 1.8 Practical Notes for Deployment                                                    | 13         |
| 1.9 Conclusion                                                                        | 14         |
| References                                                                            | 14         |
| <b>2 The Role of Artificial Intelligence in Privacy-Aware Data Collaboration</b>      | <b>17</b>  |
| <i>Kumar Dilip, Bipin Kumar Rai and Yashwant Shukla</i>                               |            |
| 2.1 Introduction                                                                      | 18         |
| 2.2 Background and Primitives                                                         | 18         |
| 2.2.1 Federated Learning—Overview and Objectives                                      | 19         |
| 2.2.2 Statistical Privacy: Differential Privacy                                       | 19         |
| 2.2.3 Secure Multi-Party Computation                                                  | 20         |
| 2.2.4 Homomorphic Encryption                                                          | 20         |
| 2.2.5 Blockchain-Based Collaborative Governance                                       | 21         |

|        |                                                                           |    |
|--------|---------------------------------------------------------------------------|----|
| 2.3    | Taxonomy of Privacy-Aware Collaborative AI                                | 22 |
| 2.3.1  | Centralized Training with Differential Privacy                            | 22 |
| 2.3.2  | Federated Learning with Secure Aggregation                                | 23 |
| 2.3.3  | Federated Learning with Differential Privacy (FL+DP)                      | 23 |
| 2.3.4  | Hybrid Federated Learning with HE/SMPC                                    | 24 |
| 2.3.5  | Peer-to-Peer (P2P) Collaboration with Blockchain Governance               | 24 |
| 2.3.6  | Encrypted Inference <i>via</i> Homomorphic Encryption                     | 25 |
| 2.4    | Mathematical Formulation: Privacy–Utility–Efficiency Trade-Off            | 25 |
| 2.4.1  | Federated Optimization with Privacy Noise                                 | 26 |
| 2.4.2  | Secure Aggregation Correctness and Adversarial Model                      | 27 |
| 2.4.3  | End-to-End Risk Function                                                  | 27 |
| 2.5    | System Design Patterns and Examples                                       | 28 |
| 2.6    | Privacy-Preserving Explainable AI                                         | 29 |
| 2.7    | Legal, Ethical, and Governance Consideration                              | 31 |
| 2.7.1  | Legal Landscape, Key Instruments and Implications                         | 31 |
| 2.7.2  | Ethical Principles and Translation to Practice                            | 31 |
| 2.7.3  | Governance Structures for Collaborative AI                                | 32 |
| 2.7.4  | Accountability, Auditability, and Assurance                               | 33 |
| 2.7.5  | Emerging Gaps and Research Needs                                          | 33 |
| 2.8    | Performance, Efficiency, and System Engineering                           | 33 |
| 2.8.1  | Key System Engineering Concerns in Collaborative AI                       | 34 |
| 2.8.2  | Performance-Efficiency Trade-Offs in Privacy-Aware AI Collaboration       | 34 |
| 2.8.3  | Engineering Best Practice Guidelines                                      | 35 |
| 2.8.4  | Emerging Research and Engineering Frontiers                               | 36 |
| 2.9    | Evaluation Metrics and Benchmarks                                         | 36 |
| 2.10   | Open Problem and Research Agenda                                          | 39 |
| 2.10.1 | Key Challenging Areas in Privacy Aware AI Collaboration                   | 39 |
| 2.10.2 | Proposed Research Agenda                                                  | 40 |
| 2.11   | Conclusion                                                                | 42 |
|        | References                                                                | 44 |
| 3      | <b>Understanding Data Privacy in the Age of Distributed AI</b>            | 47 |
|        | <i>Ayush Tripathi, Prashant Upadhyay, Pawan Kumar and Sinem Alturjman</i> |    |
| 3.1    | Introduction                                                              | 48 |

|          |                                                                                       |           |
|----------|---------------------------------------------------------------------------------------|-----------|
| 3.2      | Distributed Intelligence and the Shift toward Privacy-Preserving AI                   | 50        |
| 3.3      | The Privacy Problems in the Contemporary Distributed AI World                         | 53        |
| 3.4      | Generalized Privacy-Preserving Techniques That Support Secure Distributed AI          | 55        |
| 3.5      | Distributed Artificial Intelligence Blockchain Foundations of Trust and Transparency  | 58        |
| 3.6      | Edge and Fog Computing As the Strengths of Distributed AI                             | 60        |
| 3.7      | Regulatory Landscapes and Ethical Expectations in Distributed Artificial Intelligence | 62        |
| 3.8      | Future Scope                                                                          | 66        |
| 3.9      | Conclusion                                                                            | 67        |
|          | References                                                                            | 68        |
| <b>4</b> | <b>Blockchain Technology for Secure and Ethical AI-Driven Healthcare</b>              | <b>71</b> |
|          | <i>Jaishree Jain, Updesh Kumar Jaiswal, Shraddha Mishra and Mani Dubish</i>           |           |
| 4.1      | Introduction                                                                          | 72        |
| 4.1.1    | Background Study                                                                      | 73        |
| 4.1.2    | Importance of Research                                                                | 73        |
| 4.2      | Literature Review                                                                     | 74        |
| 4.2.1    | Criteria for Selection                                                                | 75        |
| 4.2.2    | Evaluation of Quality                                                                 | 76        |
| 4.2.3    | Selection Outcomes                                                                    | 76        |
| 4.3      | Artificial Intelligence Possible Attacks                                              | 77        |
| 4.3.1    | Vulnerabilities in AI                                                                 | 78        |
| 4.3.2    | Algorithms and Classifiers                                                            | 79        |
| 4.3.2.1  | Backdoor/Trapdoor Attack                                                              | 79        |
| 4.3.3    | Possible Solutions                                                                    | 79        |
| 4.4      | Blockchain-Based AI Healthcare Solution                                               | 80        |
| 4.4.1    | NLP-Based Medical Services                                                            | 81        |
| 4.4.2    | Healthcare Based on Computer Vision                                                   | 83        |
| 4.4.2.1  | Constructed Structure                                                                 | 84        |
| 4.4.3    | Healthcare with Acoustic AI                                                           | 87        |
| 4.5      | Blockchain-Based AI Healthcare Methods Results                                        | 87        |
| 4.5.1    | Insufficiently Stable Computational Environment                                       | 87        |
| 4.5.2    | A Lack of Interoperability and a Standardized IT System                               | 87        |

|          |                                                                                                    |           |
|----------|----------------------------------------------------------------------------------------------------|-----------|
| 4.5.3    | Blockchain Developments                                                                            | 88        |
| 4.5.3.1  | The Blockchain of Quantum                                                                          | 88        |
| 4.5.3.2  | Encryption That is Homeopathic                                                                     | 88        |
| 4.6      | Conclusion                                                                                         | 90        |
|          | References                                                                                         | 91        |
| <b>5</b> | <b>Federated Learning and Blockchain: A Collaborative Paradigm for Secure and Decentralized AI</b> | <b>95</b> |
|          | <i>Sonam Gupta and Pradeep Gupta</i>                                                               |           |
| 5.1      | Introduction                                                                                       | 96        |
| 5.2      | Fundamental Principles and Architecture                                                            | 96        |
| 5.2.1    | Core Concepts                                                                                      | 96        |
| 5.2.2    | Architectural Components                                                                           | 97        |
| 5.2.3    | Communication Protocols                                                                            | 98        |
| 5.3      | Privacy and Security Mechanisms                                                                    | 99        |
| 5.3.1    | Privacy Preservation Techniques                                                                    | 99        |
| 5.3.2    | Security Challenges and Solutions                                                                  | 99        |
| 5.3.3    | Trust and Verification                                                                             | 100       |
| 5.4      | Algorithmic Foundations                                                                            | 100       |
| 5.4.1    | Federated Averaging Algorithm                                                                      | 100       |
| 5.4.2    | Handling Non-IID Data                                                                              | 101       |
| 5.4.3    | Advanced Optimization Techniques                                                                   | 101       |
| 5.5      | Blockchain Integration in Federated Learning                                                       | 101       |
| 5.5.1    | Rationale for Integration                                                                          | 101       |
| 5.5.2    | Architectural Synergy                                                                              | 102       |
| 5.5.3    | Security and Trust Reinforcement                                                                   | 102       |
| 5.5.4    | Applications and Emerging Directions                                                               | 102       |
| 5.6      | Applications and Use Cases                                                                         | 103       |
| 5.6.1    | Healthcare Applications                                                                            | 103       |
| 5.6.2    | Financial Services                                                                                 | 103       |
| 5.6.3    | Internet of Things and Edge Computing                                                              | 104       |
| 5.7      | Technical Challenges and Solutions                                                                 | 104       |
| 5.7.1    | Communication Efficiency                                                                           | 104       |
| 5.7.2    | System Heterogeneity                                                                               | 105       |
| 5.7.3    | Scalability and Performance                                                                        | 106       |
| 5.8      | Evaluation Metrics and Benchmarks                                                                  | 106       |
| 5.8.1    | Performance Metrics                                                                                | 106       |
| 5.8.2    | Privacy Evaluation                                                                                 | 107       |
| 5.8.3    | Benchmark Datasets and Frameworks                                                                  | 107       |

|          |                                                                                               |            |
|----------|-----------------------------------------------------------------------------------------------|------------|
| 5.9      | Future Directions and Emerging Trends                                                         | 108        |
| 5.9.1    | Integration with Emerging Technologies                                                        | 108        |
| 5.9.2    | Regulatory and Ethical Considerations                                                         | 108        |
| 5.10     | Conclusion                                                                                    | 109        |
|          | References                                                                                    | 110        |
| <b>6</b> | <b>Smart Contracts-Based Autonomous Governance System for Smart City</b>                      | <b>113</b> |
|          | <i>Pawan Kumar, Rupa Rani, Jyoti Rani, Santosh Kumar Mishra and Shivpratap Singh Kushwah</i>  |            |
| 6.1      | Introduction                                                                                  | 114        |
| 6.2      | Smart City                                                                                    | 116        |
| 6.3      | Challenges in Smart City                                                                      | 117        |
| 6.3.1    | Collaborative Services                                                                        | 117        |
| 6.3.2    | Security Challenges                                                                           | 118        |
| 6.3.3    | Security Requirement                                                                          | 119        |
| 6.4      | Smart Contracts                                                                               | 119        |
| 6.4.1    | Benefits of Smart Contracts                                                                   | 120        |
| 6.4.2    | Disadvantages of Smart Contracts                                                              | 123        |
| 6.5      | Smart Contracts in Smart City                                                                 | 124        |
| 6.5.1    | Key Applications of Smart Contracts in Smart Cities                                           | 125        |
| 6.5.2    | Challenges of Implementing Smart Contracts in Smart City                                      | 126        |
| 6.5.3    | Advantages for Implementing Smart Contracts in Smart City                                     | 127        |
| 6.5.4    | Disadvantages of Implementing Smart Contracts in Smart City                                   | 128        |
|          | References                                                                                    | 130        |
| <b>7</b> | <b>Securing Legal Practice in Nigeria: Integrating AI and Blockchain for Cyber Resilience</b> | <b>133</b> |
|          | <i>Udebuani, Chidiogo Mercy and Rajesh Prasad</i>                                             |            |
| 7.1      | Introduction                                                                                  | 134        |
| 7.1.1    | Overview                                                                                      | 135        |
| 7.1.1.1  | The Threat Landscape: Why Law Firms are Targets                                               | 135        |
| 7.1.1.2  | Core Challenges Facing the Nigerian Legal Industry                                            | 136        |
| 7.1.1.3  | Case Illustrations and Recent Developments (Selected)                                         | 137        |

|         |                                                                                               |     |
|---------|-----------------------------------------------------------------------------------------------|-----|
| 7.1.1.4 | Limitations of the Study                                                                      | 137 |
| 7.1.1.5 | Methodology                                                                                   | 138 |
| 7.2     | The Role of AI and Blockchain in Enhancing Legal Practice and Cybersecurity                   | 138 |
| 7.2.1   | The Role of AI in Enhancing Legal Practice and Cybersecurity                                  | 138 |
| 7.2.2   | Blockchain Applications for Trust and Resilience                                              | 139 |
| 7.3     | Strategic Pathways for Nigeria's Legal Sector                                                 | 139 |
| 7.4     | Nigerian Legal-Regulatory and Evidentiary Context                                             | 139 |
| 7.4.1   | Regulatory and Institutional Context (Breakdown)                                              | 141 |
| 7.5     | AI for Cyber-Resilient Legal Practice                                                         | 141 |
| 7.6     | Blockchain for Integrity, Auditability, and Trust                                             | 142 |
| 7.7     | AI-Blockchain Integration: A Reference Architecture for Law Firms                             | 142 |
| 7.7.1   | Hybrid AI-Blockchain Cybersecurity Model for Nigeria's Legal Industry                         | 143 |
| 7.7.2   | Risk, Compliance, and Professional Responsibility                                             | 147 |
| 7.8     | Implementation Roadmap for Nigerian Law Firms                                                 | 147 |
| 7.8.1   | A Model AI Usage Policy for a Typical Nigerian Law Firm                                       | 147 |
| 7.9     | Conclusion and Recommendations                                                                | 150 |
| 7.9.1   | Practical Recommendations for Strengthening Safety and Technology in Nigeria's Legal Industry | 150 |
| 7.9.2   | Technological Innovations and Practical Controls for Law Firms                                | 153 |
| 7.9.2.1 | Foundational Controls (Low-to-Moderate Cost; Immediate Impact)                                | 153 |
| 7.9.2.2 | Cloud + Managed Services (Scalable; Requires Governance)                                      | 153 |
| 7.9.2.3 | Advanced Innovations (Strategic; Longer-Term Adoption)                                        | 154 |
| 7.9.2.4 | Legal-Technology Integration and Vendor Risk Management                                       | 154 |
| 7.9.3   | Ethical, Professional, and Practice Considerations                                            | 154 |
| 7.9.4   | Further Recommendations                                                                       | 155 |
| 7.10    | Conclusion                                                                                    | 156 |
|         | References                                                                                    | 157 |
|         | Appendix                                                                                      | 159 |

|          |                                                                                                     |            |
|----------|-----------------------------------------------------------------------------------------------------|------------|
| <b>8</b> | <b>Encouraging Secure Collaboration: AI's Function in Privacy-Aware Data Governance and Sharing</b> | <b>161</b> |
|          | <i>Mani Dublish, Updesh Kumar Jaiswal, Jaishree Jain and Shikha Mittal</i>                          |            |
| 8.1      | Introduction                                                                                        | 162        |
| 8.1.1    | Context and Motivation                                                                              | 162        |
| 8.1.2    | The Need for Secure Data Collaboration                                                              | 163        |
| 8.1.3    | Challenges in Data Sharing and Privacy                                                              | 163        |
| 8.1.4    | Role of AI in Privacy-Aware Governance                                                              | 164        |
| 8.2      | Background and Literature Review                                                                    | 165        |
| 8.3      | Foundations of Privacy-Aware Data Governance                                                        | 167        |
| 8.3.1    | Definition and Principles of Data Governance                                                        | 167        |
| 8.3.2    | Privacy Principles                                                                                  | 167        |
| 8.3.3    | Ethical and Legal Considerations                                                                    | 168        |
| 8.3.4    | Emerging Governance Frameworks                                                                      | 168        |
| 8.4      | AI Techniques for Privacy-Aware Data Sharing                                                        | 169        |
| 8.4.1    | Federated Learning                                                                                  | 169        |
| 8.4.2    | Differential Privacy                                                                                | 170        |
| 8.4.3    | Homomorphic Encryption and SMPC                                                                     | 171        |
| 8.4.4    | AI for Dynamic Access Control and Policy Enforcement                                                | 171        |
| 8.4.4.1  | Role-Based and Attribute-Based Controls                                                             | 171        |
| 8.4.4.2  | AI in Policy Adaptation                                                                             | 172        |
| 8.5      | Secure Data Collaboration Architectures Powered by AI                                               | 172        |
| 8.5.1    | Centralized vs. Decentralized Architectures                                                         | 172        |
| 8.5.1.1  | Centralized Architectures                                                                           | 172        |
| 8.5.1.2  | Decentralized Architectures                                                                         | 173        |
| 8.5.2    | Role of Mist, Fog, and Edge Computing                                                               | 173        |
| 8.5.2.1  | Edge Computing                                                                                      | 173        |
| 8.5.2.2  | Fog Computing                                                                                       | 174        |
| 8.5.2.3  | Mist Computing                                                                                      | 174        |
| 8.5.3    | Interoperability Across Systems                                                                     | 174        |
| 8.5.4    | AI-Enabled Data Brokers and Middleware                                                              | 175        |
| 8.5.4.1  | Features of AI-Powered Middleware                                                                   | 175        |
| 8.6      | Cross-Sector Use Cases                                                                              | 175        |
| 8.6.1    | Healthcare Sector                                                                                   | 175        |
| 8.6.1.1  | Secure Patient Data Exchange                                                                        | 175        |
| 8.6.1.2  | AI in Clinical Decision Support                                                                     | 177        |

|          |                                                                                             |            |
|----------|---------------------------------------------------------------------------------------------|------------|
| 8.6.2    | Finance Sector                                                                              | 177        |
| 8.6.2.1  | Federated Fraud Detection                                                                   | 177        |
| 8.6.2.2  | AI for Risk Assessment                                                                      | 177        |
| 8.6.3    | Smart Cities                                                                                | 178        |
| 8.6.3.1  | Multi-Agency Data Sharing                                                                   | 178        |
| 8.6.3.2  | Privacy in Urban Surveillance                                                               | 178        |
| 8.6.4    | Education and Research Sector                                                               | 178        |
| 8.6.4.1  | Collaborative Analytics in EdTech                                                           | 178        |
| 8.7      | Risks, Challenges, and Limitations                                                          | 179        |
| 8.7.1    | Model Vulnerabilities and Adversarial Threats                                               | 179        |
| 8.7.2    | Data Bias and Fairness in AI Systems                                                        | 180        |
| 8.7.3    | Legal and Ethical Dilemmas                                                                  | 180        |
| 8.7.4    | Scalability and Real-Time Limitations                                                       | 181        |
| 8.8      | Compliance and Regulatory Alignment                                                         | 181        |
| 8.8.1    | AI in GDPR, HIPAA, and CCPA Compliance                                                      | 181        |
| 8.8.1.1  | General Data Protection Regulation                                                          | 181        |
| 8.8.1.2  | Health Insurance Portability<br>and Accountability Act                                      | 182        |
| 8.8.2    | AI for Audit Trails and Reporting                                                           | 182        |
| 8.8.3    | Automating Privacy Impact Assessments                                                       | 183        |
| 8.9      | Future Trends and Research Directions                                                       | 183        |
| 8.9.1    | Blockchain Integration for Trust and Auditability                                           | 184        |
| 8.9.1.1  | Key Benefits for AI-Enabled Data Sharing                                                    | 184        |
| 8.9.2    | Explainable AI in Governance                                                                | 185        |
| 8.9.2.1  | Current and Future Directions                                                               | 185        |
| 8.9.3    | Zero-Trust Architectures                                                                    | 185        |
| 8.9.4    | AI and Privacy Metrics                                                                      | 186        |
| 8.10     | Conclusion                                                                                  | 186        |
|          | References                                                                                  | 187        |
| <b>9</b> | <b>Criminal Identification System Using Face Detection<br/>with Artificial Intelligence</b> | <b>193</b> |
|          | <i>Sunil Gupta, Tejas Singhal, Aman Kumar, Bipin Kumar Rai<br/>and Kamal Saluja</i>         |            |
| 9.1      | Introduction                                                                                | 194        |
| 9.2      | Related Work                                                                                | 196        |
| 9.3      | Objectives and Scope                                                                        | 197        |
| 9.3.1    | Scope of the Research Work                                                                  | 197        |
| 9.3.2    | Usages of AI in Crime Detection                                                             | 198        |
| 9.4      | Methodology                                                                                 | 199        |
| 9.5      | Results and Discussion                                                                      | 201        |

|           |                                                                                 |            |
|-----------|---------------------------------------------------------------------------------|------------|
| 9.5.1     | Pose Detection Output                                                           | 201        |
| 9.5.2     | Punch or Stab Detection                                                         | 201        |
| 9.5.3     | Kick Detection                                                                  | 201        |
| 9.5.4     | Punch Detected in Full Scale Code                                               | 201        |
| 9.5.5     | Kick Detected in Full Scale Code                                                | 203        |
| 9.5.6     | Fall Detected in Full Scale Code                                                | 203        |
| 9.5.7     | Crime Detected Successfully                                                     | 205        |
| 9.5.8     | Methods for Detection Analysis                                                  | 206        |
| 9.6       | Conclusion                                                                      | 207        |
|           | References                                                                      | 208        |
| <b>10</b> | <b>Zero-Knowledge Proofs for Model Integrity and Privacy</b>                    | <b>211</b> |
|           | <i>A. Kishore Kumar, T. Nivethitha, P.K. Poonguzhali and D. Saranyanandhini</i> |            |
| 10.1      | Introduction                                                                    | 212        |
| 10.1.1    | Motivation for Privacy and Integrity in Decentralized Learning                  | 213        |
| 10.1.2    | Role of Cryptography in Trustworthy AI                                          | 214        |
| 10.1.3    | Overview of Zero-Knowledge Proofs (ZKPs) and Their Relevance                    | 216        |
| 10.1.4    | Fundamentals of Zero-Knowledge Proofs                                           | 217        |
| 10.1.5    | Core Properties of ZKPs                                                         | 218        |
| 10.1.6    | Relevance of ZKPs                                                               | 219        |
| 10.2      | Decentralized Collaborative Learning: Security and Privacy Challenges           | 219        |
| 10.2.1    | Threats to Model Integrity in Federated and Distributed Learning                | 220        |
| 10.2.2    | Data Leakage and Model Inversion Attacks                                        | 223        |
| 10.2.2.1  | Data Leakage                                                                    | 224        |
| 10.2.2.2  | Model Inversion Attacks                                                         | 224        |
| 10.2.2.3  | Conclusions and Reductions                                                      | 225        |
| 10.3      | Introduction of ZKPs to Frameworks of Collaborative Learning                    | 226        |
| 10.3.1    | ZKP-Based Validation of Local Model Updates                                     | 227        |
| 10.3.2    | Verifiable Aggregation in Federated Learning                                    | 228        |
| 10.3.3    | Protocols for Proof of Training Compliance without Revealing Data               | 229        |
| 10.4      | ZKPs for Model Provenance and Integrity Verification                            | 230        |
| 10.4.1    | Ensuring Tamper-Proof Model Histories                                           | 231        |
| 10.4.2    | Transparent and Trustworthy Contributions in Collaborative Model Training       | 233        |

|           |                                                                                                             |            |
|-----------|-------------------------------------------------------------------------------------------------------------|------------|
| 10.4.3    | Use of Commitment Schemes and Cryptographic Hashes                                                          | 234        |
| 10.4.3.1  | Commitment Schemes                                                                                          | 234        |
| 10.4.3.2  | Cryptographic Hashes                                                                                        | 235        |
| 10.4.3.3  | Combined Use                                                                                                | 235        |
| 10.5      | Protection and Implementation Frameworks and Tools                                                          | 236        |
| 10.5.1    | ZKP Libraries and Platforms (e.g., ZoKrates, SnarkJS, Halo2)                                                | 237        |
| 10.5.1.1  | ZoKrates                                                                                                    | 237        |
| 10.5.1.2  | SnarkJS                                                                                                     | 238        |
| 10.5.1.3  | Halo2                                                                                                       | 238        |
| 10.5.2    | Integration with Federated Learning Systems (e.g., TensorFlow Federated, Pysyft)                            | 239        |
| 10.5.2.1  | TensorFlow Federated                                                                                        | 240        |
| 10.5.2.2  | PySyft                                                                                                      | 240        |
| 10.5.2.3  | Benefits of Integration                                                                                     | 240        |
| 10.5.2.4  | Considerations of Practical Implementation                                                                  | 241        |
| 10.6      | Use Cases and Case Studies                                                                                  | 241        |
| 10.6.1    | Inter-Hospital Healthcare Data Sharing                                                                      | 241        |
| 10.6.2    | Privacy-Constrained Financial Fraud Detection                                                               | 243        |
| 10.7      | Conclusion and Future Directions                                                                            | 245        |
|           | References                                                                                                  | 248        |
| <b>11</b> | <b>Edge and Fog Computing for Distributed Intelligence</b>                                                  | <b>251</b> |
|           | <i>Vadym Slyusar</i>                                                                                        |            |
| 11.1      | Introduction                                                                                                | 252        |
| 11.2      | Differences Between Fog Computing and the Distribution of a Multi-Agent System Across Multiple Edge Devices | 254        |
| 11.3      | Combined Architecture Integrating Fog Computing and Multi-Agent Distribution at the Edge                    | 256        |
| 11.4      | Cognitive Decentralized Systems                                                                             | 257        |
| 11.5      | Concept of Loitering Models                                                                                 | 260        |
| 11.6      | Migration Protocol with Decision-Making Metrics                                                             | 263        |
| 11.7      | Splitting of Models                                                                                         | 267        |
| 11.8      | Swarms of Loitering Models                                                                                  | 272        |
| 11.9      | Architecture with Distributed Embedding                                                                     | 275        |
| 11.10     | The Concept of the Embedding Swarm                                                                          | 278        |
| 11.11     | Hardware Aspects of the Edge Level                                                                          | 280        |
| 11.12     | Conclusion                                                                                                  | 282        |
|           | References                                                                                                  | 283        |

|                                                                                                                                  |            |
|----------------------------------------------------------------------------------------------------------------------------------|------------|
| <b>12 Incentive Models and Token Economics in Learning Networks</b>                                                              | <b>287</b> |
| <i>Raj Kishor Verma, Atul Kumar Rai, Kumar Dilip and Shivani Sharma</i>                                                          |            |
| 12.1 Introduction                                                                                                                | 288        |
| 12.1.1 Incentive Models in Learning Networks                                                                                     | 289        |
| 12.1.2 Token Economics in Learning Networks                                                                                      | 289        |
| 12.1.3 Emerging Challenges and Opportunities                                                                                     | 289        |
| 12.2 Background                                                                                                                  | 290        |
| 12.2.1 Early Developments: Social Incentives and Peer-to-Peer Networks                                                           | 290        |
| 12.2.2 The Coming of Distributed Computing and Game                                                                              | 291        |
| 12.2.3 Decentralization Federated Learning and the New Distributed Paradigm                                                      | 291        |
| 12.2.4 Token Economics                                                                                                           | 291        |
| 12.2.5 Game-Theoretic and AI-Enabled Incentive Models                                                                            | 292        |
| 12.2.6 Reputation- or Service-Based (and Hybrid) Incentives                                                                      | 292        |
| 12.2.7 Critical Issues: Fairness, Security and Robustness                                                                        | 292        |
| 12.3 Smart Contract Mechanisms                                                                                                   | 293        |
| 12.3.1 The Major Execution Differences That Matter between Smart Contract Platforms Generally Fall into the Following Categories | 294        |
| 12.3.1.1 Consensus Mechanism and Transaction Finality                                                                            | 294        |
| 12.3.1.2 Throughput and Scalability                                                                                              | 295        |
| 12.3.1.3 Programming and Virtual System Languages                                                                                | 295        |
| 12.3.1.4 Execution Costs                                                                                                         | 295        |
| 12.3.1.5 Security and Stability                                                                                                  | 295        |
| 12.3.1.6 Support for Ecosystem and Tools                                                                                         | 295        |
| 12.3.2 Tokenomics                                                                                                                | 296        |
| 12.3.3 Alignment-Based Rewards                                                                                                   | 298        |
| 12.3.4 Federated Learning                                                                                                        | 299        |
| 12.3.5 Token Economic Frameworks                                                                                                 | 301        |
| 12.3.6 Decentralized Governance                                                                                                  | 301        |
| 12.3.7 Persistent Incentivization                                                                                                | 302        |
| 12.4 Literature Review                                                                                                           | 303        |
| 12.5 Proposed Methodology                                                                                                        | 303        |
| 12.5.1 Algorithm Incentive Mechanism Learning Networks                                                                           | 307        |
| 12.5.2 Result Analysis                                                                                                           | 309        |

|           |                                                                         |            |
|-----------|-------------------------------------------------------------------------|------------|
| 12.6      | Conclusion and Future Scope                                             | 317        |
| 12.7      | Challenges                                                              | 319        |
|           | References                                                              | 320        |
| <b>13</b> | <b>Healthcare Applications of Blockchain–AI Collaboration</b>           | <b>323</b> |
|           | <i>Rishabh Kamal and Prashant Upadhyay</i>                              |            |
| 13.1      | Introduction                                                            | 324        |
| 13.1.1    | Synergy between Blockchain and AI in Healthcare                         | 325        |
| 13.1.2    | Design of a Blockchain and AI Cooperation<br>in Healthcare              | 326        |
| 13.1.3    | Blockchain for Secure and Interoperable Data                            | 326        |
| 13.1.4    | AI-Enhanced Clinical Decision Support                                   | 326        |
| 13.1.5    | Federated Learning for Privacy-Preserving<br>Analytics                  | 327        |
| 13.1.6    | Smart Contracts for Automated Healthcare<br>Operations                  | 328        |
| 13.1.7    | Blockchain-AI Synergy for Drug Discovery<br>and Clinical Trials         | 328        |
| 13.2      | Literature Review                                                       | 329        |
| 13.3      | Fundamentals of Blockchain and Artificial Intelligence                  | 332        |
| 13.3.1    | Blockchain Technology in Healthcare                                     | 332        |
| 13.3.2    | Artificial Intelligence in Healthcare                                   | 333        |
| 13.3.3    | Smart Contracts in Healthcare                                           | 333        |
| 13.3.4    | Machine Learning and Deep Learning in Clinical<br>Applications          | 334        |
| 13.4      | Applications of Blockchain and Artificial Intelligence<br>in Healthcare | 334        |
| 13.4.1    | Secure Medical Data Management                                          | 335        |
| 13.4.2    | Clinical Trials and Research Integrity                                  | 335        |
| 13.4.3    | Healthcare Interoperability                                             | 336        |
| 13.4.4    | Precision Medicine and Personalized Care                                | 336        |
| 13.4.5    | Supply Chain and Drug Authentication                                    | 337        |
| 13.4.6    | Fraud Detection and Billing                                             | 337        |
| 13.4.7    | Remote Patient Monitoring                                               | 337        |
| 13.4.8    | Telemedicine and Virtual Health                                         | 338        |
| 13.5      | Challenges in Integrating Blockchain and AI in Healthcare               | 338        |
| 13.5.1    | Scalability and Performance                                             | 338        |
| 13.5.2    | Data Quality and Bias                                                   | 339        |
| 13.5.3    | Privacy and Security Concerns                                           | 339        |
| 13.5.4    | Ethical and Regulatory Issues                                           | 339        |
| 13.5.5    | Interoperability Challenges                                             | 340        |

|           |                                                                        |            |
|-----------|------------------------------------------------------------------------|------------|
| 13.5.6    | Cost and Resource Constraints                                          | 340        |
| 13.6      | Future Directions in Healthcare Technology                             | 340        |
| 13.6.1    | Federated Learning and Decentralized AI                                | 341        |
| 13.6.2    | Blockchain-Oriented Internet of Medical Things                         | 342        |
| 13.6.3    | Patient-Centered Healthcare Systems                                    | 342        |
| 13.6.4    | Integration with Emerging Technologies                                 | 342        |
| 13.7      | Conclusion                                                             | 343        |
|           | References                                                             | 343        |
| <b>14</b> | <b>Financial Sector Use Cases—Privacy-Preserving Fraud Detection</b>   | <b>349</b> |
|           | <i>Ayush Tripathi, Prashant Upadhyay, Rupa Rani and Chadi Altrjman</i> |            |
| 14.1      | Introduction                                                           | 350        |
| 14.2      | Traditional vs. Decentralized Fraud Detection Systems                  | 353        |
| 14.3      | Federated Learning for Collaborative Fraud Detection                   | 357        |
| 14.4      | Privacy-Hyphenated Systems of Financial Fraud Detection                | 360        |
| 14.5      | Blockchain and Smart Contracts for Trustworthy Fraud Intelligence      | 363        |
| 14.6      | Regulatory and Ethical Aspects of Privacy                              | 369        |
| 14.7      | Future Scope                                                           | 372        |
| 14.8      | Conclusion                                                             | 373        |
|           | References                                                             | 374        |
| <b>15</b> | <b>Smart Cities through IoT, Blockchain, and AI Collaboration</b>      | <b>377</b> |
|           | <i>Vishal Jain, Sachin Jain and K. Ramkumar</i>                        |            |
| 15.1      | Introduction                                                           | 378        |
| 15.1.1    | The Genesis of Smart Cities                                            | 378        |
| 15.1.2    | The IoT Foundation: The City's Digital Nervous System                  | 379        |
| 15.1.3    | The Emerging Challenges: A Crisis of Centralization and Trust          | 379        |
| 15.1.4    | A New Paradigm of Decentralized Intelligence                           | 380        |
| 15.1.5    | Chapter Outline                                                        | 381        |
| 15.2      | Literature Review                                                      | 381        |
| 15.2.1    | Smart Cities and the IoT                                               | 381        |
| 15.2.2    | Blockchain in Urban Governance and Security                            | 382        |
| 15.2.3    | Artificial Intelligence in Smart City Operations                       | 382        |
| 15.2.4    | The Nascent Convergence: Combining Blockchain and AI                   | 383        |

|           |                                                                                            |            |
|-----------|--------------------------------------------------------------------------------------------|------------|
| 15.3      | The Collaborative Framework: Integrating IoT, Blockchain, and AI                           | 383        |
| 15.3.1    | Architectural Layers                                                                       | 384        |
| 15.3.2    | The Synergistic Loop: How the Components Collaborate                                       | 386        |
| 15.4      | Mathematical and Algorithmic Foundations                                                   | 387        |
| 15.4.1    | Blockchain Consensus for IoT: Proof of Verified Authority                                  | 387        |
| 15.4.2    | AI-Driven Predictive Analytics: LSTM for Traffic Flow                                      | 388        |
| 15.4.3    | Smart Contract Logic with AI Triggers                                                      | 389        |
| 15.4.4    | Security and Privacy Quantification: A Conceptual Trust Index                              | 392        |
| 15.5      | Graphical Representations of the Ecosystem                                                 | 392        |
| 15.6      | Case Studies: Practical Applications and Implementations                                   | 395        |
| 15.6.1    | Case Study 1: Smart Energy Grid Management                                                 | 395        |
| 15.6.2    | Case Study 2: Autonomous Traffic and Supply Chain Management                               | 396        |
| 15.7      | Challenges and Future Research Directions                                                  | 397        |
| 15.8      | Conclusion                                                                                 | 398        |
|           | References                                                                                 | 399        |
| <b>16</b> | <b>Legal and Regulatory Challenges of Cross-Border AI Collaboration</b>                    | <b>403</b> |
|           | <i>Sachin Jain, Vishal Jain, Danish Ather, Golnoosh Manteghi and Abu Bakar Abdul Hamid</i> |            |
| 16.1      | Introduction                                                                               | 404        |
| 16.1.1    | The Imperative of Global AI Collaboration                                                  | 404        |
| 16.1.2    | The Great Friction: Technology Unites, Law Divides                                         | 405        |
| 16.1.3    | Core Domains of Legal Conflict                                                             | 405        |
| 16.1.4    | Chapter Outline                                                                            | 406        |
| 16.2      | Literature Review: Mapping the Legal Minefield                                             | 406        |
| 16.2.1    | Data Governance and the “Splinternet”                                                      | 407        |
| 16.2.2    | Intellectual Property: The Enigma of Ownership                                             | 407        |
| 16.2.3    | Liability and Accountability: The Distributed Responsibility Problem                       | 408        |
| 16.2.4    | Summary of Key Literature                                                                  | 409        |
| 16.3      | Conceptual Models: Quantifying and Visualizing Legal Complexity                            | 409        |
| 16.3.1    | The Regulatory Friction Index                                                              | 409        |

|           |                                                                                                         |            |
|-----------|---------------------------------------------------------------------------------------------------------|------------|
| 16.3.2    | The Trust-Verification Matrix for Data Sharing                                                          | 412        |
| 16.4      | Descriptive Visualizations of the Legal Ecosystem                                                       | 413        |
| 16.5      | Case Studies: The Law in Action                                                                         | 415        |
| 16.5.1    | Case Study 1: The Global Pandemic Prediction Initiative (Scientific Collaboration)                      | 416        |
| 16.5.2    | Case Study 2: “AutonoDrive”—An EU–US Autonomous Vehicle Joint Venture (Commercial Collaboration)        | 417        |
| 16.5.3    | Case Study 3: The “AquaSecure” Critical Infrastructure AI (Geopolitical Collaboration)                  | 418        |
| 16.6      | Overarching Challenges and Future Research Directions                                                   | 419        |
| 16.6.1    | The Pacing Problem: Law Lagging Behind Technology                                                       | 419        |
| 16.6.2    | The “Black Box” Dilemma: Reconciling Opacity with Accountability                                        | 420        |
| 16.6.3    | Bridging the Divide: The Role of Technology and Diplomacy                                               | 420        |
| 16.7      | Conclusion                                                                                              | 421        |
|           | References                                                                                              | 422        |
| <b>17</b> | <b>Artificial Intelligence’s Ethical Consequences: Difficulties, Hazards, and Regulatory Viewpoints</b> | <b>425</b> |
|           | <i>Anita Pati Mishra, Mani Dublsh and Shailender Kumar Vats</i>                                         |            |
| 17.1      | Introduction                                                                                            | 426        |
| 17.2      | Mapping the Research Environment                                                                        | 427        |
| 17.3      | Digital Transformation, the Dangers of AI, and Ethical Concerns in Research Settings                    | 428        |
| 17.3.1    | Hypothesis H1                                                                                           | 429        |
| 17.4      | Research Theories and Conceptual Framework                                                              | 430        |
| 17.4.1    | Hypothesis H1                                                                                           | 431        |
| 17.4.2    | Hypothesis H2                                                                                           | 431        |
| 17.4.3    | Hypothesis H3                                                                                           | 432        |
| 17.5      | Privacy, Reliability, and Cognitive Preparedness                                                        | 432        |
| 17.6      | Results                                                                                                 | 435        |
| 17.7      | Analysis and Discussion                                                                                 | 437        |
| 17.7.1    | Consistent Perceptions of AI Pitfalls                                                                   | 438        |
| 17.7.2    | Findings That Do Not Match                                                                              | 438        |
| 17.8      | Conclusions                                                                                             | 439        |
| 17.8.1    | Theoretic Inferences                                                                                    | 440        |
| 17.8.2    | Restrictions and Additional Research                                                                    | 441        |
|           | References                                                                                              | 441        |

|           |                                                                                            |            |
|-----------|--------------------------------------------------------------------------------------------|------------|
| <b>18</b> | <b>Technical Challenges and System Limitations</b>                                         | <b>447</b> |
|           | <i>Sachin Jain, Vishal Jain, Danish Ather, Golnoosh Manteghi and Abu Bakar Abdul Hamid</i> |            |
| 18.1      | Introduction                                                                               | 448        |
| 18.1.1    | The Centralization Conundrum in the Age of AI                                              | 448        |
| 18.1.2    | The Promise of Decentralized Collaborative Learning                                        | 449        |
| 18.1.3    | The Hidden Complexities: Not a Privacy Panacea                                             | 449        |
| 18.1.4    | Chapter Outline                                                                            | 450        |
| 18.2      | Literature Review: A Landscape of Distributed Challenges                                   | 451        |
| 18.2.1    | The Challenge of Statistical Heterogeneity (Non-IID Data)                                  | 451        |
| 18.2.2    | The Communication Bottleneck                                                               | 452        |
| 18.2.3    | Security and Privacy Vulnerabilities                                                       | 452        |
| 18.2.4    | Summary of Key Literature                                                                  | 455        |
| 18.3      | Conceptual Models and Mathematical Formulations                                            | 455        |
| 18.3.1    | The Federated Averaging (FedAvg) Algorithm                                                 | 455        |
| 18.3.2    | Quantifying Statistical Heterogeneity                                                      | 456        |
| 18.3.3    | Modelling a Model Poisoning Attack                                                         | 456        |
| 18.3.4    | The Privacy-Utility Trade-Off with DP                                                      | 457        |
| 18.4      | Descriptive Visualizations of System Limitations                                           | 458        |
| 18.5      | Case Studies: Challenges in Real-World Application                                         | 458        |
| 18.5.1    | Case Study 1: Collaborative Cancer Detection in a Hospital Consortium                      | 459        |
| 18.5.2    | Case Study 2: Next-Word Prediction for a Mobile Keyboard Application                       | 460        |
| 18.5.3    | Case Study 3: Predictive Maintenance in a B2B Industrial IoT Consortium                    | 460        |
| 18.6      | System-Level Limitations and Future Research Directions                                    | 461        |
| 18.6.1    | The Centralized Orchestrator                                                               | 461        |
| 18.6.2    | The Right to be Forgotten and Machine “Unlearning”                                         | 462        |
| 18.6.3    | Systems Heterogeneity                                                                      | 462        |
| 18.6.4    | At the Cutting Edge: Integrating DCL with Other Technologies to Strengthen Privacy         | 463        |
| 18.7      | Conclusion                                                                                 | 463        |
|           | References                                                                                 | 464        |

|                                                                                  |            |
|----------------------------------------------------------------------------------|------------|
| <b>19 Trust by Design: AI's Evolution in Secure and Transparent Data Systems</b> | <b>467</b> |
| <i>Nandini Srivastava and Anuradha M. Dhumale</i>                                |            |
| 19.1 Introduction                                                                | 468        |
| 19.2 Evolution of AI in Data Security and Transparency                           | 470        |
| 19.2.1 Artificial Intelligence                                                   | 470        |
| 19.2.2 Early Artificial Intelligence Systems                                     | 473        |
| 19.2.3 Current Trends of AI                                                      | 475        |
| 19.2.3.1 Blockchain Technology                                                   | 475        |
| 19.2.3.2 Federated Learning                                                      | 477        |
| 19.3 Machine Learning                                                            | 477        |
| 19.3.1 Introduction                                                              | 477        |
| 19.3.2 Types of Machine Learning                                                 | 478        |
| 19.3.2.1 Supervised Learning                                                     | 478        |
| 19.3.2.2 Unsupervised Learning                                                   | 478        |
| 19.3.2.3 Semi-Supervised Learning                                                | 480        |
| 19.3.2.4 Reinforcement Learning                                                  | 480        |
| 19.3.3 Classification                                                            | 481        |
| 19.3.3.1 Lazy Learning                                                           | 481        |
| 19.3.3.2 Eager Learning                                                          | 482        |
| 19.4 Trust in AI                                                                 | 482        |
| 19.4.1 Trust                                                                     | 482        |
| 19.4.2 Bias and Discrimination                                                   | 482        |
| 19.4.3 Trust by Design Principle                                                 | 483        |
| 19.4.3.1 Transparent and Explainability                                          | 483        |
| 19.4.3.2 Accountability                                                          | 483        |
| 19.4.3.3 Privacy Preservation                                                    | 484        |
| 19.4.3.4 Security by Default                                                     | 484        |
| 19.4.3.5 Ethical AI Governance                                                   | 484        |
| 19.5 Comparison Table and Use Cases                                              | 484        |
| 19.5.1 AI in Healthcare                                                          | 484        |
| 19.5.2 AI in Education                                                           | 486        |
| 19.5.3 AI in Finance                                                             | 487        |
| 19.5.4 AI in Smart Cities                                                        | 487        |
| 19.5.5 AI Tools                                                                  | 487        |
| 19.6 Conclusion                                                                  | 488        |
| References                                                                       | 489        |

|           |                                                                                              |            |
|-----------|----------------------------------------------------------------------------------------------|------------|
| <b>20</b> | <b>Decentralized Intelligence: Redefining Learning through Secure AI and EoT Integration</b> | <b>491</b> |
|           | <i>Ravipalli Sri Santhi Nehru</i>                                                            |            |
| 20.1      | Introduction                                                                                 | 492        |
| 20.1.1    | The Changing Landscape of Education                                                          | 492        |
| 20.1.2    | Motivation for Decentralization and Intelligence Integration                                 | 493        |
| 20.1.3    | Objectives and Scope of the Chapter                                                          | 494        |
| 20.2      | Conceptual Foundations                                                                       | 494        |
| 20.2.1    | Decentralized Intelligence: What is It?                                                      | 494        |
| 20.2.2    | CLF Innovative Environments and EoT                                                          | 494        |
| 20.2.3    | Role of Secure AI in Modern Education                                                        | 495        |
| 20.2.4    | Summary of Privacy-Preserving Models and Trust-Based Learning Models                         | 495        |
| 20.3      | Architecture of the Decentralized Learning Ecosystem                                         | 496        |
| 20.3.1    | Integration of Blockchain and Distributed Ledger Technologies                                | 496        |
| 20.3.2    | AI-Driven Personalization and Adaptability                                                   | 496        |
| 20.3.3    | EoT Infrastructure: The Sensors, Edge Devices, and Data Flow                                 | 496        |
| 20.3.4    | Real-Time Data Processing Using Edge Computing and Associated Techniques                     | 497        |
| 20.4      | Foundational Technologies for Privacy-Preserving, Distributed Education                      | 497        |
| 20.4.1    | Blockchain for Learners' Identity and Attainment Records                                     | 497        |
| 20.4.2    | Data Sovereignty and Federated Learning                                                      | 497        |
| 20.4.3    | Thrustless Security Protocols and Homomorphic Encryption                                     | 498        |
| 20.4.4    | Smart Contracts and Educational Governance                                                   | 498        |
| 20.5      | Applications and Use Cases                                                                   | 498        |
| 20.5.1    | Smart Classrooms and Interactive Learning Environments                                       | 498        |
| 20.5.2    | Blockchain-Based Credentialing and Micro-Certification                                       | 499        |
| 20.5.3    | Context-Aware Learning Analytics and Feedback Systems                                        | 499        |
| 20.5.4    | Wearables and Mobile Devices in Adaptive Learning                                            | 499        |

|           |                                                                                                              |            |
|-----------|--------------------------------------------------------------------------------------------------------------|------------|
| 20.6      | Issues Related to the Technology and Their Solutions                                                         | 500        |
| 20.6.1    | Keeping Things the Same and in Synchronization within Distributed Frameworks                                 | 500        |
| 20.6.2    | Assuring the Data is Correct While Also Managing the Available Bandwidth                                     | 501        |
| 20.6.3    | Techniques on EoT Data Stream Compression                                                                    | 501        |
| 20.6.4    | Being Able to Manage Things in Learning Environments That are Constantly Changing                            | 502        |
| 20.7      | Social, Policy, and Ethical Aspects                                                                          | 502        |
| 20.7.1    | Algorithmic Equity and Reducing Bias                                                                         | 502        |
| 20.7.2    | The Digital Divide and Equitable Access                                                                      | 502        |
| 20.7.3    | Learner Privacy and Data Ethics                                                                              | 503        |
| 20.7.4    | Decentralized Education Policy Frameworks                                                                    | 503        |
| 20.8      | New Technologies and What to Expect in the Future                                                            | 503        |
| 20.8.1    | Advanced Security Models and Quantum Computing                                                               | 504        |
| 20.8.2    | Learning Ecosystems That Work Across Chains                                                                  | 504        |
| 20.8.3    | Interoperability and Standardization in Decentralized Education                                              | 504        |
| 20.8.4    | A Vision for Systems that are Totally Adaptive Learner-Centric                                               | 504        |
| 20.9      | Conclusion                                                                                                   | 505        |
|           | References                                                                                                   | 505        |
| <b>21</b> | <b>Fortifying Financial Systems: Privacy-Centric Collaborative Detection with Transparent Accountability</b> | <b>509</b> |
|           | <i>Jarnail Singh and Shelley Khosla</i>                                                                      |            |
| 21.1      | Introduction                                                                                                 | 510        |
| 21.2      | Literature Review                                                                                            | 511        |
| 21.2.1    | Federated Learning in Anomaly Detection                                                                      | 511        |
| 21.2.2    | Blockchain for Security and Transparency                                                                     | 512        |
| 21.2.3    | Privacy-Preserving Techniques                                                                                | 513        |
| 21.2.4    | Open Challenges                                                                                              | 514        |
| 21.3      | Methodology                                                                                                  | 514        |
| 21.3.1    | System Architecture                                                                                          | 514        |
| 21.3.2    | Local Autoencoder Model                                                                                      | 515        |
| 21.3.3    | Federated Learning Protocol                                                                                  | 516        |
| 21.3.4    | Privacy and Security                                                                                         | 516        |
| 21.3.5    | Handling Class Imbalance and Heterogeneity                                                                   | 516        |

## xxiv CONTENTS

|        |                                  |            |
|--------|----------------------------------|------------|
| 21.4   | Experimental Setup               | 516        |
| 21.4.1 | Evaluation Metrics               | 517        |
| 21.4.2 | Experimental Environment         | 517        |
| 21.5   | Results                          | 518        |
| 21.6   | Discussion                       | 520        |
| 21.7   | Challenges and Future Directions | 520        |
| 21.8   | Conclusion                       | 521        |
|        | Abbreviations                    | 522        |
|        | References                       | 523        |
|        | <b>Index</b>                     | <b>527</b> |

## 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