1.

Record Nr.	UNINA9910874662003321
Autore	Palle Ranadeep Reddy
Titolo	Privacy in the Age of Innovation : AI Solutions for Information Security
Pubbl/distr/stampa	Berkeley, CA : , : Apress L. P., , 2024 ©2024
ISBN	979-88-6880-461-8
Edizione	[1st ed.]
Descrizione fisica	1 online resource (205 pages)
Altri autori (Persone)	KathalaKrishna Chaitanya Rao
Disciplina	323.44/8
Soggetti	Data privacy Artificial intelligence
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Intro -- Table of Contents -- About the Authors -- About the Technical Reviewer -- Acknowledgments -- Chapter 1: Introduction -- 1.1 The Intersection of AI, Information Security, Data Privacy, and Data Security -- 1.2 Outline of the Book -- 1.3 Target Audiences/Readers -- 1.3.1 Who Can Read This Book? -- Chapter 2: Understanding AI and Ethics -- 2.1 Fundamentals of AI, Machine Learning, and Deep Learning -- 2.1.1 Defining Artificial Intelligence -- 2.1.2 The Evolution of AI: From Rule-Based Systems to Machine Learning -- 2.1.3 Unveiling the Power of Machine Learning -- 2.1.4 Delving Deeper: Understanding Deep Learning -- 2.1.5 Privacy-Preserving Techniques in Machine Learning and Deep Learning -- 2.1.6 Ethical Considerations in AI, Machine Learning, and Deep Learning -- 2.1.7 Striking the Right Balance: Innovation and Privacy -- 2.1.8 Case Studies: AI and Privacy in Action -- 2.2 The Ethics of AI in Privacy and Security -- 2.2.1 The Intersection of Innovation and Ethics -- 2.2.2 Bias and Fairness: Addressing Ethical Quandaries -- 2.2.3 Explainability and Transparency: Fostering Trust in AI Systems -- 2.2.4 Accountability in AI: Navigating the Complex Web -- 2.2.5 Striking the Right Balance: Ethical Decision-Making in Security -- 2.2.6 Case Studies: Navigating Ethical Challenges in AI Security Applications -- 2.2.7 Navigating the Ethical Landscape of AI in Privacy and Security -- Chapter 3: Information Security and Data Privacy Landscape -- 3.1 The Current State of Information Security

and Data Privacy -- 3.1.1 The Evolving Threat Landscape -- 3.1.2 Regulatory Frameworks and Compliance -- 3.1.3 Rise of Privacy-Preserving Technologies -- 3.1.4 Balancing Act: Innovation Versus Privacy -- 3.1.5 Increasing Awareness and Education -- 3.1.6 Cloud Security and the Remote Work Paradigm -- 3.1.7 Incident Response and Resilience.

Navigating the Complex Terrain -- 3.2 Key Challenges and Risks -- 3.2.1 Cybersecurity Threats: A Persistent Menace -- 3.2.2 Insider Threats: The Human Element -- 3.2.3 Regulatory Compliance Burden and Complexity of Privacy Regulations -- 3.2.4 Integration of Privacy-Preserving Technologies -- 3.2.5 Cloud Security Concerns -- 3.2.6 Advanced Persistent Threats (APTs): Stealthy Adversaries -- 3.2.7 Skills Shortage in Cybersecurity -- Navigating Complexity with Vigilance -- Chapter 4: AI for Threat Detection and Prevention -- 4.1 How AI Can Bolster Threat Detection and Mitigation -- 4.1.1 Advanced Threat Detection with Machine Learning -- 4.1.2 Predictive Analytics: Anticipating Threats Before They Manifest -- 4.1.3 Behavioral Analytics: Understanding the Human Element -- 4.1.4 Anomaly Detection: Uncovering Stealthy Threats -- 4.1.5 Natural Language Processing (NLP): Enhancing Contextual Understanding -- 4.1.6 Adversarial Machine Learning: A Cat-and-Mouse Game -- 4.1.7 Automation and Orchestration: Swift Response to Threats -- 4.1.8 Integration with Threat Intelligence Feeds -- Augmenting Security Defenses with AI -- 4.2 AI-Driven Cybersecurity Solutions -- 4.2.1 Machine Learning-Powered Endpoint Protection -- 4.2.2 Behavioral Analytics for User-Centric Security -- 4.2.3 Network Traffic Analysis with AI -- 4.2.4 Automated Threat Hunting and Incident Response -- 4.2.5 Predictive Analysis for Vulnerability Management -- 4.2.6 AI-Enhanced Phishing Detection -- 4.2.7 Autonomous Threat Intelligence Platforms -- 4.2.8 Continuous Adaptive Risk and Trust Assessment -- A Holistic Defense with AI -- 4.3 Case Studies of AI in Action -- 4.3.1 Case Study 1: Darktrace's Autonomous Response at Maersk -- 4.3.2 Case Study 2: Cylance's AI-Driven Endpoint Protection -- 4.3.3 Case Study 3: IBM Watson for Cyber Security at a Financial Institution.

4.3.4 Case Study 4: Palo Alto Networks Cortex XDR -- 4.3.5 Case Study 5: Google's AI for Phishing Detection -- 4.3.6 Case Study 6: FireEye's Helix Security Platform -- 4.3.7 Case Study 7: Symantec's AI-Enhanced Cloud Security -- Unleashing the Power of AI in Cybersecurity -- Chapter 5: Privacy-Preserving AI Techniques -- 5.1 Techniques for Preserving Privacy While Using AI -- 5.1.1 Homomorphic Encryption: Unlocking Secure Computations -- 5.1.2 Federated Learning: Decentralized Model Training -- 5.1.3 Differential Privacy: Adding Noise for Privacy Protection -- 5.1.4 Secure Multiparty Computation: Collaborative Data Analysis -- 5.1.5 Homomorphic Databases: Securing Query Processing -- 5.1.6 Zero-Knowledge Proofs: Verifying Without Revealing -- 5.1.7 Synthetic Data Generation: Mimicking Real Data Without Exposure -- Building a Privacy-Centric AI Landscape -- 5.2 Homomorphic Encryption, Differential Privacy, and Secure Multiparty Computation -- 5.2.1 Homomorphic Encryption: Preserving Confidentiality in Computation -- 5.2.2 Differential Privacy: Injecting Controlled Noise for Anonymity -- 5.2.3 Secure Multiparty Computation: Collaborative Insights Without Data Exposure -- 5.2.4 Real-World Application: Preserving Privacy in AI-Driven Healthcare Research -- 5.2.5 Overcoming Challenges: Trade-Offs and Computational Complexity -- Navigating the Privacy-AI Landscape -- 5.3 Implementing Federated Learning for Data Privacy -- 5.3.1 Understanding Federated Learning: Decentralized Intelligence -- 5.3.2 Preserving Privacy: Federated Learning in Action -- 5.3.3 Advantages of Federated Learning for Data Privacy -- 5.3.4 Real-World Applications: From Smartphones to Healthcare -- 5.3.5 Challenges and Considerations -- 5.3.6 Future Directions: Advancing Federated Learning for Privacy -- Empowering Privacy Through Federated Learning.

Chapter 6: Data Protection and Compliance -- 6.1 Regulations and Standards (e.g., GDPR, CCPA) Related to Data Privacy and Security -- 6.1.1 GDPR (General Data Protection Regulation): A Global Standard -- 6.1.2 Consumer Privacy Act of California (CCPA): Innovators in Privacy Legislation in the United States -- 6.1.3 Other International Data Protection Regulations and Standards -- 6.1.4 Navigating a Complex Environment: Compliance Challenges and Strategies -- 6.1.5 Future Legislative Trends in Data Protection -- Navigating the Regulatory Landscape -- 6.2 AI's Role in Achieving and Maintaining Compliance -- 6.2.1 Recognizing the Impact of AI on Compliance -- 6.2.2 Artificial Intelligence in Automated Data Governance -- 6.2.3 Artificial Intelligence-Driven Privacy Impact Assessments (PIAs) -- 6.2.4 Addressing Bias and Ethical Issues -- 6.2.5 Obstacles and Considerations -- 6.2.6 Future Trends: Evolution of AI-Driven Compliance -- A Synergistic Future of AI and Compliance -- Chapter 7: Securing AI Models -- 7.1 Best Practices for Securing AI Models -- 7.1.1 Strong Data Governance as the Basis -- 7.1.2 Model Development and Security Training -- 7.1.3 Operational Security and Deployment -- 7.1.4 Ethical Concerns and Bias Reduction -- 7.1.5 Education and Awareness of Users -- 7.1.6 Adherence to Regulatory Standards -- 7.1.7 Information Sharing and Collaboration -- 7.1.8 Incident Response and Recovery Planning -- 7.1.9 Emerging Technologies and Adaptive Security -- 7.1.10 Regular Security Assessments and Reviews -- A Holistic Approach to AI Model Security -- 7.2 Model Explainability and Fairness -- 7.2.1 The Importance of Model Explicability -- 7.2.2 Model Explainability Techniques -- 7.2.3 The Fairness Imperative in AI Models -- 7.2.4 Difficulties in Ensuring Model Fairness -- 7.2.5 Model Fairness Assurance Techniques.

7.2.6 Ongoing Monitoring and Bias Reduction -- 7.2.7 The Relationship Between Model Explainability and Fairness -- 7.2.8 The Way Forward: Ethical and Secure AI Models -- 7.3 Model Deployment Security -- 7.3.1 The Value of Model Deployment Security -- 7.3.2 Model Deployment Security Issues -- 7.3.3 Model Deployment Security Best Practices -- 7.3.4 Emerging Model Deployment Security Trends -- 7.3.5 Future Model Deployment Security Considerations -- Protecting AI Model Deployment's Future -- Chapter 8: Case Studies -- 8.1 Real-World Examples of AI Enhancing Information Security and Data Privacy -- 8.1.1 Healthcare Industry: Threat Prevention Using Predictive Analytics -- 8.1.2 Financial Institutions: Detection and Prevention of Fraud -- 8.1.3 E-commerce: Behavioral Analysis for Personalized Security -- 8.1.4 Manufacturing: Industrial Internet of Things Security -- 8.1.5 Government: Critical Infrastructure Protection -- 8.1.6 Social Media Platforms: Moderation of Content and User Privacy -- 8.1.7 Education Sector: Student Data Security -- 8.2 Success Stories and Lessons Learned -- 8.2.1 Financial Sector: Increasing Fraud Detection Efficiency -- 8.2.2 Technology Firm: Cloud Infrastructure Security -- 8.2.3 Healthcare Provider: AI for Patient Data Privacy Protection -- 8.2.4 Ecommerce Powerhouse: Customized Security Measures -- 8.2.5 Energy Sector: Artificial Intelligence for Predictive Maintenance and Security -- Adaptive Security Measures in Educational Institutions -- Chapter 9: AI in Data Privacy and Ethics -- 9.1 The Ethical Considerations of AI in Privacy -- 9.1.1 Balancing Innovation and Individual Anonymity Preservation -- 9.1.2 Informed Consent

and Transparency -- 9.1.3 Avoiding Discrimination and Bias -- 9.1.4 Reducing Invasion -- 9.1.5 Accountability and Responsibility -- 9.1.6 Global Standards and Compliance.
9.1.7 Public Involvement and Collaboration.

Sommario/riassunto	This book will help you comprehend the impact of artificial intelligence (AI) on information security, data privacy, and data security. The book starts by explaining the basics and setting the goals for a complete understanding of how AI, Information Security, Data Privacy, and Data Security all connect. Then, it gives you important information about the basics of AI, machine learning, and deep learning in simple terms. It also talks about the ethics of using AI in privacy and security, making sure you understand the power and responsibility that come with AI. Next, it takes you through the complex world of information security and data privacy. It covers everything from the current state of security to how AI can detect threats and protect privacy. Additionally, it delves into ethical considerations to ensure the responsible use of AI in managing data privacy. Later chapters discuss strategies and future trends in using AI for data security, finding the right balance between security and privacy, and giving useful advice for organizations. In the end, this book examines the current landscape and foresees the future, underscoring the vital importance of maintaining a balance between innovation and privacy in AI-powered security. What you will learn: How AI is being used to detect and prevent cyberattacks in real-time What are the AI-powered techniques for anonymizing and de-identifying data, What are the latest advancements in AI-powered privacy-enhancing technologies (PETs) How to find the right balance between security and privacy Who this book is for: Information security professionals, data scientists, and software developers seeking to gain an understanding of the latest trends and techniques in AI for information security.