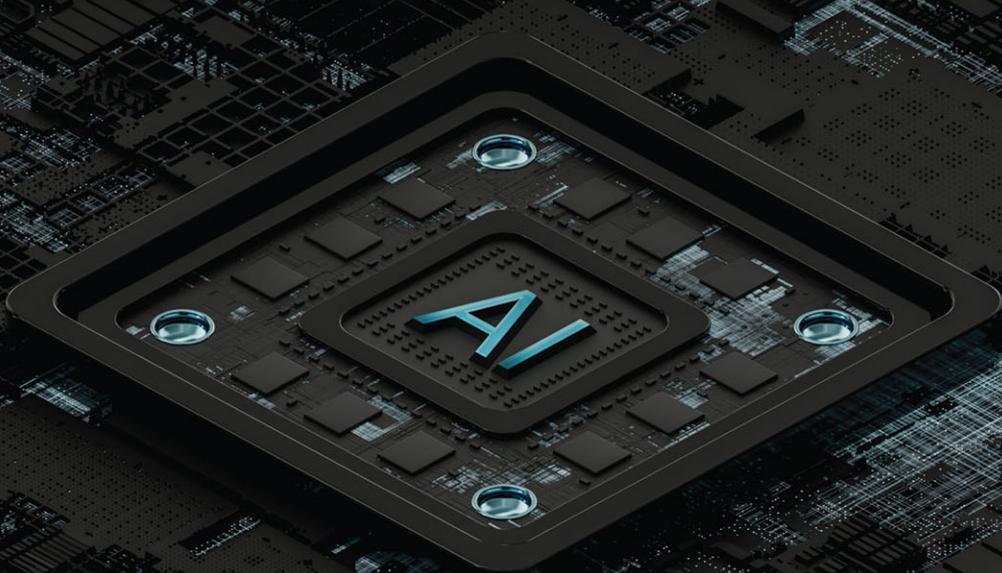




THE **AI**  
REVOLUTION  
IN NETWORKING,  
CYBERSECURITY,  
AND EMERGING  
TECHNOLOGIES



OMAR SANTOS | SAMER SALAM | HAZIM DAHIR

FREE SAMPLE CHAPTER |



# THE AI REVOLUTION IN NETWORKING, CYBERSECURITY, AND EMERGING TECHNOLOGIES

*This page intentionally left blank*

# THE AI REVOLUTION IN NETWORKING, CYBERSECURITY, AND EMERGING TECHNOLOGIES

Omar Santos, Samer Salam, Hazim Dahir

◆◆ Addison-Wesley

Cover: Javier Pardina/Shutterstock

Figure 5-4: GreenOak/Shutterstock

Figure 5-5: U.S. Bureau Transportation Statistics

Figure 5-6: malinikart/Alamy Images

Many of the designations used by manufacturers and sellers to distinguish their products are claimed as trademarks. Where those designations appear in this book, and the publisher was aware of a trademark claim, the designations have been printed with initial capital letters or in all capitals.

The authors and publisher have taken care in the preparation of this book, but make no expressed or implied warranty of any kind and assume no responsibility for errors or omissions. No liability is assumed for incidental or consequential damages in connection with or arising out of the use of the information or programs contained herein.

For information about buying this title in bulk quantities, or for special sales opportunities (which may include electronic versions; custom cover designs; and content particular to your business, training goals, marketing focus, or branding interests), please contact our corporate sales department at [corpsales@pearsoned.com](mailto:corpsales@pearsoned.com) or (800) 382-3419.

For government sales inquiries, please contact [governmentsales@pearsoned.com](mailto:governmentsales@pearsoned.com).

For questions about sales outside the U.S., please contact [intlcs@pearson.com](mailto:intlcs@pearson.com).

Visit us on the Web: [informit.com/aw](http://informit.com/aw)

Library of Congress Control Number: 2024930069

Copyright © 2024 Pearson Education, Inc.

Hoboken, NJ

Please contact us with concerns about any potential bias at <https://www.pearson.com/report-bias.html>.

All rights reserved. This publication is protected by copyright, and permission must be obtained from the publisher prior to any prohibited reproduction, storage in a retrieval system, or transmission in any form or by any means, electronic, mechanical, photocopying, recording, or likewise. For information regarding permissions, request forms and the appropriate contacts within the Pearson Education Global Rights & Permissions Department, please visit [www.pearsoned.com/permissions/](http://www.pearsoned.com/permissions/).

ISBN-13: 978-0-13-829369-7

ISBN-10: 0-13-829369-4

\$PrintCode

**Editor-in-Chief**

Mark Taub

**Director ITP Product Management**

Brett Bartow

**Executive Editor**

James Manly

**Managing Editor**

Sandra Schroeder

**Development Editor**

Christopher A. Cleveland

**Production Editor**

Mary Roth

**Copy Editor**

Jill Hobbs

**Technical Editor**

Petar Radanliev

**Editorial Assistant**

Cindy Teeters

**Cover Designer**

Chuti Prasertsith

**Composition**

codeMantra

**Indexer**

Erika Millen

**Proofreader**

Jennifer Hinchliffe

*I would like to dedicate this book to my lovely wife, Jeannette, and my two beautiful children, Hannah and Derek, who have inspired and supported me throughout the development of this book.*

—Omar Santos

*To Zeina, Kynda, Malek, Ziyad, Mom, Dad, and Samir.*

—Samer Salam

*To Angela, Hala, Leila, and Zayd, the “real” Intelligence behind everything good in my life.*

—Hazim Dahir

*This page intentionally left blank*

# Contents

<b>Preface</b> .....	<b>xv</b>
<b>1 Introducing the Age of AI: Emergence, Growth, and Impact on Technology</b> .....	<b>1</b>
The End of Human Civilization .....	2
Significant Milestones in AI Development (This Book Is Already Obsolete) .....	2
The AI Black Box Problem and Explainable AI .....	5
What's the Difference Between Today's Large Language Models and Traditional Machine Learning? .....	6
Hugging Face Hub: A Game-Changer in Collaborative Machine Learning .....	12
AI's Expansion Across Different Industries: Networking, Cloud Computing, Security, Collaboration, and IoT .....	14
AI's Impacts on the Job Market .....	15
AI's Impacts on Security, Ethics, and Privacy .....	17
Prompt Injection Attacks .....	17
Insecure Output Handling .....	22
Training Data Poisoning .....	22
Model Denial of Service .....	22
Supply Chain Vulnerabilities .....	23
Sensitive Information Disclosure .....	24
Insecure Plugin Design .....	25
Excessive Agency .....	25
Overreliance .....	26
Model Theft .....	26
Model Inversion and Extraction .....	26
Backdoor Attacks .....	27
MITRE ATLAS Framework .....	28
AI and Ethics .....	28
AI and Privacy .....	28

Summary	30
References	31
<b>2 Connected Intelligence: AI in Computer Networking</b>	<b>33</b>
The Role of AI in Computer Networking	34
AI for Network Management	37
Automating Network Planning	37
Automating Network Configuration	38
Automating Network Assurance	40
AI for Network Optimization	45
Routing Optimization	45
Radio Resource Management	47
Energy Optimization	48
AI for Network Security	49
Access Control	49
Anti-malware Systems	50
Firewalls	51
Behavioral Analytics	51
Software and Application Security	52
AI for Network Traffic Analysis	52
AI in Network Digital Twins	54
Summary	55
References	56
<b>3 Securing the Digital Frontier: AI's Role in Cybersecurity</b>	<b>59</b>
AI in Incident Response: Analyzing Potential Indicators to Determine the Type of Attack	59
Predictive Analytics	60
Sentiment Analysis and Potential Threat Intelligence	65
Text-Based Anomaly Detection	67
Enhancing Human Expertise in the Security Operations Center Through AI	68
Integration with Other Models	71
AI in Vulnerability Management and Vulnerability Prioritization	71

- AI in Security Governance, Policies, Processes, and Procedures . . . . . 73
- Using AI to Create Secure Network Designs . . . . . 74
  - Role of AI in Secure Network Design . . . . . 74
- AI and Security Implications of IoT, OT, Embedded, and Specialized Systems . . . . . 75
- AI and Physical Security . . . . . 76
  - How AI Is Transforming Physical Security . . . . . 76
  - Security Co-pilots . . . . . 76
  - Enhanced Access Control . . . . . 77
- AI in Security Assessments, Red Teaming, and Penetration Testing . . . . . 77
- AI in Identity and Account Management . . . . . 80
  - Intelligent Authentication . . . . . 81
  - Automated Account Provisioning and Deprovisioning . . . . . 83
  - Dynamic Access Control . . . . . 84
- Using AI for Fraud Detection and Prevention . . . . . 86
- AI and Cryptography . . . . . 87
  - AI-Driven Cryptanalysis . . . . . 87
  - Dynamic Cryptographic Implementations . . . . . 88
  - Integration with Quantum Cryptography . . . . . 88
- AI in Secure Application Development, Deployment, and Automation . . . . . 90
  - Dynamic Analysis . . . . . 90
  - Intelligent Threat Modeling . . . . . 91
  - Secure Configuration Management . . . . . 91
  - Intelligent Patch Management While Creating Code . . . . . 92
- Summary . . . . . 93
- References . . . . . 94
- 4 AI and Collaboration: Building Bridges, Not Walls . . . . . 95**
  - Collaboration Tools and the Future of Work . . . . . 96
    - Innovations in Multimedia and Collaboration . . . . . 97
    - What Is Hybrid Work and Why Do We Need It? . . . . . 99
  - AI for Collaboration . . . . . 101

Authentication, Verification, or Authorization Through Voice or Speech Recognition . . . . .	101
Reducing Language Barriers with Real-Time Translation . . . . .	101
Virtual Assistants . . . . .	102
Task Management . . . . .	102
Context and Intent Analysis . . . . .	103
Workflow Automation . . . . .	103
Prescriptive Analytics . . . . .	104
Learning and Development . . . . .	105
Physical Collaboration Spaces . . . . .	106
Virtual Collaboration Spaces . . . . .	106
Team Dynamics . . . . .	107
Document Management . . . . .	108
The Contact Center: A Bridge to Customers . . . . .	109
Virtual Agents . . . . .	111
Call Routing Optimization . . . . .	111
24 × 7 × 365 Support . . . . .	111
Multilanguage Support . . . . .	111
Customer Sentiment . . . . .	112
Quality Assurance and Agent Coaching . . . . .	112
Large Case Volume Handling . . . . .	112
Predictive Analytics . . . . .	113
Upgrading and Upselling . . . . .	113
AR/VR: A Closer Look . . . . .	113
Interactive Learning . . . . .	114
AI-Assisted Real-Time Rendering . . . . .	114
Content Generation . . . . .	114
Personalization of Interaction . . . . .	115
Virtual Assistant/Selling . . . . .	115
NLP and NLU . . . . .	115
Sentiments and Emotions . . . . .	115

	Affective Computing . . . . .	116
	Summary . . . . .	116
	References . . . . .	117
<b>5</b>	<b>AI in the Internet of Things (AIoT) . . . . .</b>	<b>119</b>
	Understanding the IoT Landscape . . . . .	120
	AI for Data Analytics and Decision-Making . . . . .	122
	Data Processing . . . . .	122
	Anomaly Detection . . . . .	123
	Predictive Maintenance . . . . .	123
	Advanced Data Analytics . . . . .	124
	AI for IoT Resource Optimization . . . . .	125
	AI for IoT in Supply Chains . . . . .	127
	AI for IoT Security . . . . .	130
	AI and Threat Detection in IoT . . . . .	131
	AI and Vulnerability Detection in IoT Environments . . . . .	132
	AI and Authentication in IoT . . . . .	132
	AI and Physical Safety and Security . . . . .	133
	AI for IoT in Sustainability . . . . .	133
	Water Management and Preservation . . . . .	134
	Energy Management . . . . .	134
	Sustainable Waste Management and Recycling . . . . .	134
	Wildlife Conservation . . . . .	135
	Circular Economy . . . . .	135
	Summary . . . . .	137
	References . . . . .	137
<b>6</b>	<b>Revolutionizing Cloud Computing with AI . . . . .</b>	<b>139</b>
	Understanding the Cloud Computing Environment . . . . .	139
	Virtualization . . . . .	140
	Application Mobility . . . . .	142
	Cloud Services . . . . .	143
	Deployment Models . . . . .	143

- Cloud Orchestration . . . . . 144
- AI in Cloud Infrastructure Management. . . . . 145
  - Workload and VM Placement . . . . . 145
  - Demand Prediction and Load-Balancing. . . . . 146
  - Anomaly Detection . . . . . 146
- AI for Cloud Security. . . . . 147
  - Vulnerabilities and Attacks . . . . . 148
  - How Can AI Help? . . . . . 149
  - Challenges for AI . . . . . 150
- AI for Cloud Optimization. . . . . 151
  - Cloud Service Optimization. . . . . 151
  - Cloud Infrastructure Optimization. . . . . 152
- AI and Machine Learning as a Service . . . . . 153
  - AI Infrastructure Services. . . . . 154
  - AI Developer Services: AutoML and Low-Code/No-Code AI . . . . . 154
  - AI Software Services . . . . . 155
  - Advantages of AlaaS . . . . . 156
- Challenges of AI and Machine Learning in the Cloud . . . . . 158
- What Lies Ahead. . . . . 158
- Summary . . . . . 159
- References . . . . . 159
- 7 Impact of AI in Other Emerging Technologies. . . . . 161**
  - Executive Order on the Safe, Secure, and Trustworthy  
Development and Use of Artificial Intelligence . . . . . 162
  - AI in Quantum Computing . . . . . 163
    - Quantum Algorithm Development . . . . . 164
    - Algorithmic Tuning and Automated Circuit Synthesis. . . . . 166
    - Hyperparameter Optimization, Real-Time Adaptation, and  
Benchmarking for Performance Analysis. . . . . 166
  - How AI Can Revolutionize Quantum Hardware Optimization . . . . . 167
    - Control Operation and Resource Optimization . . . . . 168

Data Analysis and Interpretation . . . . . 168

    Quantum Machine Learning: Leveraging AI Research to  
    Uncover Quantum Advantages in ML Tasks . . . . . 168

AI in Blockchain Technologies . . . . . 169

    Automating the Execution of Smart Contracts with AI . . . . . 169

    Could We Optimize Blockchain Mining Through AI Algorithms? . . . . . 170

    Additional Use Cases in Healthcare, Supply Chain Management,  
    Financial Services, and Cybersecurity . . . . . 171

AI in Autonomous Vehicles and Drones . . . . . 175

AI in Edge Computing . . . . . 175

    Extending the Cloud: Edge and Fog . . . . . 176

    Taking AI to the Edge . . . . . 177

    Lightweight AI and Tiny ML . . . . . 178

    Applications and Use Cases . . . . . 180

    Web 3.0 . . . . . 182

Summary . . . . . 183

References . . . . . 184

**Index . . . . . 185**

*This page intentionally left blank*

## Preface

*The AI Revolution in Networking, Cybersecurity, and Emerging Technologies* offers an immersive journey into the world of artificial intelligence and its profound impact on key domains of technology. This manuscript demystifies AI's emergence, growth, and current impact, shedding light on its revolutionary applications in computer networking, cybersecurity, collaboration technologies, IoT, cloud computing, and other emerging technologies.

From explaining AI's role in managing and optimizing networks to its integral part in securing the digital frontier, the book offers a wealth of insights. It explores how AI is building robust bridges in collaboration tools and turning IoT into a super-intelligent network of devices. The reader will also discover how AI is transforming the cloud into a self-managing, secure, and ultra-efficient environment and propelling other technologies towards unprecedented advancements.

Our motivation is for this book to serve as a comprehensive guide that bridges the gap between the complex world of artificial intelligence and its practical implications in the field of IT. We aim to make the profound impacts and potential of AI in various technology sectors not only understandable but also tangible for a wide spectrum of readers. Additionally, part of our vision is to create an essential resource that empowers readers to understand, navigate, and address the opportunities, complex challenges, and responsibilities associated with AI technologies. This book will empower readers, whether they are IT professionals, tech enthusiasts, business leaders, or students, with the necessary knowledge and insights into how AI is reshaping the IT landscape. By providing a clear, in-depth exploration of AI's role in computer networking, cybersecurity, IoT, cloud computing, and more, we aim to equip readers to harness the power of AI in their respective fields. Ultimately, our motive is for this book to not only educate but also inspire—serving as a catalyst that propels individuals and organizations into the future of AI-integrated technology.

This book is highly relevant for a range of audiences, given its exploration of various aspects of artificial intelligence and technology.

- **IT Professionals:** Those who work in fields related to information technology, network management, cybersecurity, cloud computing, IoT, and autonomous systems could benefit from understanding how AI is revolutionizing their respective fields.
- **Tech Enthusiasts:** Individuals with an interest in emerging technologies and future trends might find this book interesting due to its examination of AI's influence on various domains.
- **Business Leaders & Managers:** This book would be useful for executives, managers, and decision-makers who need to understand the implications of AI on business processes and strategies, particularly those related to IT.
- **Academics and Students:** Professors, researchers, and students in fields related to computer science, information technology, and AI would find the book useful for research and educational purposes.

- **Policy Makers:** Given the increasing impact of AI on society and the economy, policymakers could also gain valuable insights from this book.
- **AI Professionals:** People working in the field of AI might use this book to understand the broader context and applications of their work.

Register your copy of *The AI Revolution in Networking, Cybersecurity, and Emerging Technologies* on the InformIT site for convenient access to updates and/or corrections as they become available. To start the registration process, go to [informit.com/register](http://informit.com/register) and log in or create an account. Enter the product ISBN (**9780138293697**) and click Submit.

## **Acknowledgments**

We would like to thank the technical editor, Petar Radanliev, for his time and technical expertise.

Additionally, our appreciation goes to the dedicated Pearson team, with special mentions to James Manly and Christopher Cleveland, for their amazing support.

*This page intentionally left blank*

## About the Authors

**Omar Santos** is a cybersecurity thought leader with a passion for driving industry-wide initiatives to enhance the security of critical infrastructures. Omar is the lead of the DEF CON Red Team Village, the chair of the Common Security Advisory Framework (CSAF) technical committee, the founder of OpenEoX, and board member of the OASIS Open standards organization. Omar's collaborative efforts extend to numerous organizations, including the Forum of Incident Response and Security Teams (FIRST) and the Industry Consortium for Advancement of Security on the Internet (ICASI).

Omar is a renowned person in ethical hacking, vulnerability research, incident response, and AI security. He employs his deep understanding of these disciplines to help organizations stay ahead of emerging threats. His dedication to cybersecurity has made a significant impact on businesses, academic institutions, law enforcement agencies, and other entities striving to bolster their security measures.

With over 20 books, video courses, white papers, and technical articles under his belt, Omar's expertise is widely recognized and respected. Omar is a Distinguished Engineer at Cisco, focusing on AI security research, incident response, and vulnerability disclosure. Omar is a frequent speaker at many conferences, including RSA, Blackhat, DEF CON, and more, where he shares his cybersecurity and AI security insights with the global community. You can follow Omar on Twitter @santosomar.

**Samer Salam** is a technology architect and engineering leader in the computer networking industry with over two decades of experience. In his role as Distinguished Engineer at Cisco Systems, he focuses on identifying, incubating, and mainstreaming disruptive technologies, in addition to defining and driving the system and software architecture for networking products. His work spans the areas of Intent Based Networking, Artificial Intelligence, Natural Language Processing, Machine Reasoning, Semantic Technologies and Immersive Visualization. Previously at Cisco, he held multiple technical leadership and software development positions working on IoT, Layer 2 VPN, Metro Ethernet, OAM protocols, network resiliency, system scalability, software quality, multi-service edge, broadband, MPLS, and dial solutions.

Samer was awarded the International Society of Service Innovation Professionals (ISSIP) 2022 Excellence in Service Innovation Award for the "Impact to Innovation" category. He holds over 99 US and international patents, and is coauthor of *The Internet of Things From Hype to Reality: The Road to Digitization*. He has authored fourteen IETF RFCs, and multiple articles in academic and industry journals. He is also a speaker at Cisco Live, and blogs on networking technology. Samer holds an M.S. degree in Computer Engineering from the University of Southern California in Los Angeles and a B.Eng. in Computer and Communications Engineering, with Distinction, from the American University of Beirut.

**Hazim Dahir** is a Distinguished Engineer at the Cisco Technology Enablement and Acceleration Office. He is working to define and influence next-generation digital transformation architectures across multiple technologies and industry verticals. Hazim started his Cisco tenure in 1996 as a software engineer and subsequently moved into the services organization, focusing on large-scale and

emerging technology network architectures. He is currently focusing on developing architectures utilizing security, collaboration, Edge computing, and AlloT technologies addressing the future of work and hybrid cloud requirements for large enterprises. Through his passion for engineering and sustainability, Hazim is currently working on advanced software solutions for electric and autonomous vehicles with global automotive manufacturers. Hazim is a frequent presenter at multiple US & global conferences and standards bodies. He is the vice-chair for the IEEE Edge Computing workgroup. He has more than 22 issued and pending US and International patents, several R&D publications, and is the co-author of four technical books.

# 7

## Impact of AI in Other Emerging Technologies

We stand at the convergence of several revolutionary technologies that promise to reshape not just companies and governments, but the very fabric of modern society itself. The AI revolution is not an isolated phenomenon; it is acting as a catalyst that amplifies and integrates with other groundbreaking technologies, enriching their potential and accelerating their adoption. This chapter explains the complex interplay between AI and four other pivotal domains: quantum computing, blockchain technologies, autonomous vehicles and drones, and edge computing.

The fusion of AI and quantum computing has opened new dimensions in computational capability. This could give us the tools to solve complex problems that were once considered impossible to crack. The interaction between these technologies holds the promise to revolutionize fields like cryptography, materials science, and financial modeling. AI's convergence with blockchain could offer possibilities for secure, transparent, and decentralized systems. What if AI can revolutionize data integrity, financial transactions, and even democratic processes?

The integration of AI in self-driving cars and drones has transcended the realm of science fiction and entered practical implementation. You might be driving a Tesla from New York to North Carolina in self-driving mode or enhanced autopilot. Your car is using AI and machine learning (ML). Additionally, from supply chain optimization to emergency response, the impact of the combination of AI and transportation is definitely transformative.

By pushing AI analytics to the edge of the network, closer to where data is generated, edge computing enables real-time decision-making and reduces the latency that could have catastrophic consequences in applications like healthcare and industrial automation. In this chapter, we explore these intersections and survey how AI acts as both a catalyst and a beneficiary in its relationships with these other transformative technologies.

## **Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence**

Before we start discussing the impact of AI in emerging technology, let's discuss a few government efforts to ensure the responsible use and development of AI, recognizing its significant potential for both positive and negative impacts. The key objectives include solving urgent challenges, enhancing prosperity, productivity, innovation, and security, while mitigating the risks associated with AI, such as exacerbating societal harms, displacing workers, stifling competition, and posing national security threats. The United States Government emphasizes the need for a society-wide effort involving government, the private sector, academia, and civil society to harness AI for good and mitigate its risks. The executive order and related resources can be accessed at: <https://ai.gov>.

The impact of this Executive Order on emerging technologies, particularly AI, will be multifaceted. By emphasizing the need for safe and secure AI, the order will push for robust evaluations and standardized testing of AI systems. This focus on safety and security will likely influence the development and deployment of emerging technologies, ensuring they are reliable and ethically operated.

The order aims to promote responsible innovation and a competitive environment for AI technologies. This could lead to increased investments in AI-related education, training, and research, and address intellectual property challenges. The emphasis on a fair and open AI marketplace may encourage innovation and provide opportunities for small developers and entrepreneurs. By prioritizing the adaptation of job training and education to support a diverse workforce in the AI era, the order will likely influence how emerging technologies are integrated into the workforce. It aims to ensure that AI deployment improves job quality and augments human work, rather than causing disruptions or undermining worker rights.

The order's focus on aligning AI policies with equity and civil rights objectives will influence how AI and other emerging technologies are developed and used. This may lead to more rigorous standards and evaluations to prevent AI systems from deepening discrimination or bias, thereby impacting how these technologies are designed and implemented. By enforcing consumer protection laws and principles in the context of AI, the order will impact how emerging technologies are used in sectors like healthcare, financial services, education, and transportation. The emphasis on privacy and civil liberties will guide the development and use of technologies in ways that respect personal data and mitigate privacy risks.

The order's focus on global leadership and cooperation will influence the international framework for managing AI's risks. This could lead to more standardized global approaches to AI safety, security, and ethical use, impacting how emerging technologies are developed and deployed worldwide.

The order mentions the use of significant computing power for training AI models using primarily biological sequence data, highlighting the scale and complexity involved in AI applications in biological contexts. The Director of the Office of Science and Technology Policy (OSTP) is tasked with establishing criteria and mechanisms for identifying biological sequences that could pose a national security risk. This includes developing standardized methodologies and tools for screening and verifying the performance of sequence synthesis procurement, as well as customer screening approaches to manage security risks posed by purchasers of these biological sequences.

The order defines “dual-use foundation models” as AI models that could be easily modified to exhibit high performance in tasks posing serious risks to security, including the design, synthesis, acquisition, or use of chemical, biological, radiological, or nuclear weapons. This shows concern about the potential for AI to lower barriers to entry in creating biological threats.

The order specifically mandates actions to understand and mitigate risks of AI being misused in the development or use of chemical, biological, radiological, and nuclear (CBRN) threats, particularly focusing on biological weapons. This involves both the Secretary of Defense and the Secretary of Homeland Security. The order calls for an assessment of how AI can increase biosecurity risks, particularly those arising from generative AI models trained on biological data. It also stresses the importance of considering the national security implications of using data associated with pathogens and omics studies for training generative AI models, with a view to mitigating these risks.

These efforts are set to significantly influence the landscape and impact of AI in emerging technologies. By establishing a framework that prioritizes safety, security, responsible innovation, and equitable practices, the order will guide the ethical development and deployment of these technologies. It emphasizes robust testing, privacy protection, and the integration of AI in a manner that benefits society while mitigating risks such as discrimination, bias, and threats to civil liberties. Additionally, the focus on encouraging a competitive AI marketplace, supporting workforce development, and engaging in global cooperation suggests a future where AI and related technologies are not only technologically advanced but also socially responsible and aligned with broader human values. This approach is intended to shape the direction of technological innovation, ensuring that it advances in tandem with ethical standards and societal needs.

## AI in Quantum Computing

In Chapter 3, “Securing the Digital Frontier: AI’s Role in Cybersecurity,” we explored how quantum computing, and particularly post-quantum cryptography with quantum key distribution (QKD), represents a cutting-edge field of study that leverages the principles of quantum physics to enable secure communication. AI can enhance quantum cryptography, such as in QKD, by optimizing protocols and improving security against quantum attacks. In addition to enhancing quantum cryptography like QKD, AI can contribute to quantum computing in the following areas (among others):

- Quantum algorithm development
- Quantum hardware optimization
- Simulation and modeling
- Control and operation
- Data analysis and interpretation
- Resource optimization
- Quantum machine learning

Let’s explore these in more detail.

## Quantum Algorithm Development

Quantum algorithms promise groundbreaking advancements in a variety of domains, including cryptography, materials science, and optimization problems. However, the design and optimization of these algorithms remain a significant challenge. This is where AI can provide some value added and benefits. With their ability to analyze complex systems and optimize parameters, AI implementations can become a pivotal player in the field of quantum algorithm development.

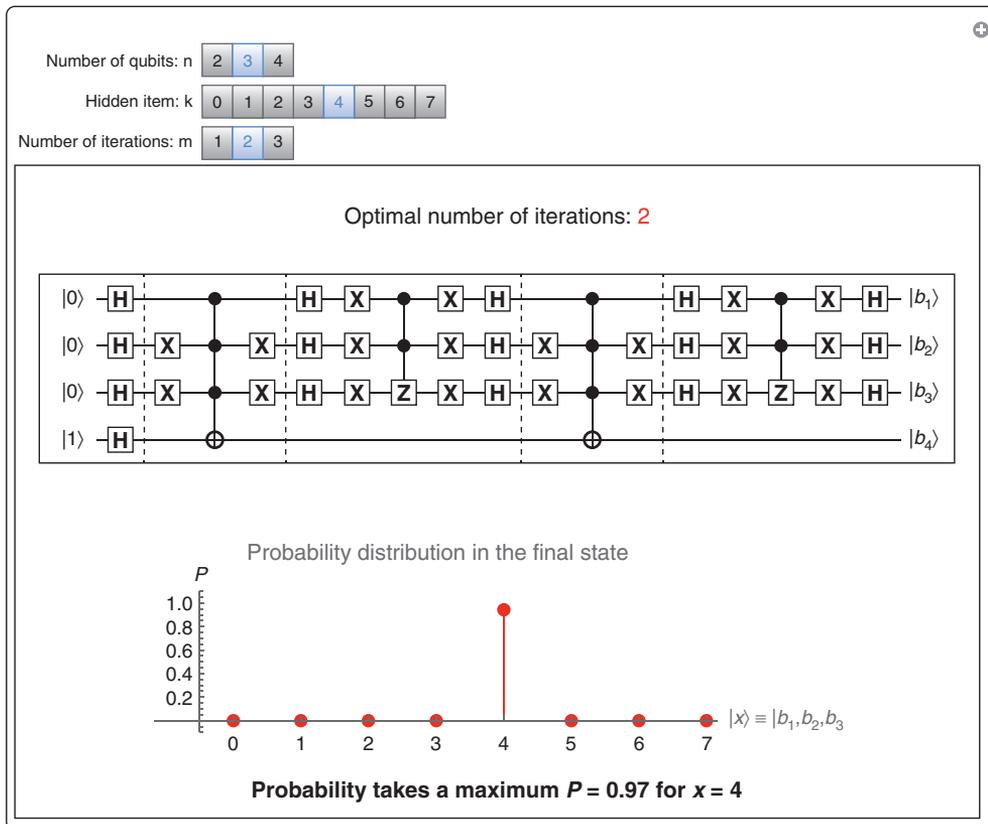
Quantum computing algorithms offer unique advantages over their classical counterparts in solving specific problems. Although the field is continually evolving, some algorithms have already gained prominence due to their innovative capabilities. The following are some of the most common and historical quantum computing algorithms:

- **Shor's algorithm:** Developed by Peter Shor, this algorithm is known for its ability to factorize large composite numbers exponentially faster than the best-known classical algorithms. Its efficiency poses a significant threat to RSA encryption in modern cryptography. The original paper describing Shor's algorithm can be found at <https://arxiv.org/abs/quant-ph/9508027>.
- **Grover's algorithm:** Invented by Lov Grover, this algorithm provides a quadratic improvement over classical algorithms for unsorted database searching. You can learn more about the original research into Grover's algorithm at <https://arxiv.org/abs/quant-ph/9605043>. You can interact with a demonstration of how a quantum circuit is implementing Grover's search algorithm at <https://demonstrations.wolfram.com/QuantumCircuitImplementingGroversSearchAlgorithm>.

Figure 7-1 demonstrates how the quantum circuit changes when a Grover's iteration is added. The diagram in Figure 7-1 illustrates a quantum memory register containing four qubits, where three qubits are originally prepared in the state  $|0\rangle$  and one ancillary qubit is in the state  $|1\rangle$ . (You can interact with this illustration at [wolfram.com](https://demonstrations.wolfram.com/QuantumCircuitImplementingGroversSearchAlgorithm).)

- **Quantum Fourier transform (QFT):** QFT is a quantum analog of the classical fast Fourier transform (FFT). It serves as a subroutine in several other quantum algorithms, most notably in Shor's algorithm. You can learn more about the QFT algorithm at <https://demonstrations.wolfram.com/QuantumFourierTransformCircuit/>.
- **Variational quantum eigensolver (VQE):** This algorithm is useful for solving problems related to finding ground states in quantum systems. It is often used in chemistry simulations to understand molecular structures. The VQE paper can be found at <https://arxiv.org/abs/2111.05176>. You can also access a detailed explanation of VQE at <https://community.wolfram.com/groups/-/m/t/2959959>.
- **Quantum approximate optimization algorithm (QAOA):** An algorithm developed for solving combinatorial optimization problems, QAOA has applications in logistics, finance, and ML. It approximates the solution for problems where finding the exact solution is computationally expensive. The QAOA original research paper can be found at <https://arxiv.org/abs/1411.4028>.
- **Quantum phase estimation:** This algorithm estimates the eigenvalue of a unitary operator, given one of its eigenstates. It serves as a component (a subroutine) in other algorithms, such

as Shor's Algorithm, and quantum simulations. You can obtain additional information about the quantum phase estimation implementation at [https://quantumalgorithmzoo.org/#phase\\_estimation](https://quantumalgorithmzoo.org/#phase_estimation).



**Figure 7-1**

*A Demonstration of Grover's Search Algorithm*

- **Quantum walk algorithms:** Quantum walks are the quantum analogs of classical random walks and serve as a foundational concept for constructing various quantum algorithms. Quantum walks can be used in graph problems, element distinctness problems, and more. You can access the quantum walk algorithm original paper at: <https://arxiv.org/abs/quant-ph/0302092>.
- **BB84 protocol:** Although it's primarily known as a quantum cryptography protocol rather than a computation algorithm, BB84 is important because it provides a basis for QKD, securing communications against eavesdropping attacks, even those using quantum capabilities. A detailed explanation of the BB84 protocol can be found at <https://medium.com/quantum-untangled/quantum-key-distribution-and-bb84-protocol-6f03cc6263c5>.

- **Quantum error-correction codes:** Although not algorithms in the traditional sense, quantum error-correction codes like the Toric code and the Cat code are essential for creating fault-tolerant quantum computers, mitigating the effects of decoherence and other errors. The quantum error-correction codes research paper can be accessed at <https://arxiv.org/abs/1907.11157>.
- **Quantum machine learning algorithms:** This class of algorithms is designed to speed up classical ML tasks using quantum computing. Although this field is still in a nascent stage, it has garnered considerable interest for its potential to disrupt traditional ML techniques. You can access a research paper that surveys quantum ML algorithms at <https://arxiv.org/abs/1307.0411>.

**NOTE** Each of these algorithms offers specific advantages and applicability across various domains, from cryptography and optimization to simulation and ML. As quantum computing matures, it's likely that we will see the development of many more specialized algorithms that leverage the unique capabilities of quantum systems.

Quantum computing operates on entirely different principles than classical computing, utilizing quantum bits or “qubits” instead of binary bits. While quantum computers promise to perform certain tasks exponentially faster, they come with their own set of challenges, such as error rates and decoherence. Additionally, the quantum world abides by different rules, making it inherently challenging to develop algorithms that can leverage the full potential of quantum processors.

## Algorithmic Tuning and Automated Circuit Synthesis

Traditional quantum algorithms like Shor's algorithm for factorization or Grover's algorithm for search are efficient but often rigid in their construction. AI can offer dynamic tuning of these algorithms by optimizing the parameters to adapt to specific problems or hardware configurations. This level of customization can pave the way for more robust and versatile quantum algorithms, making quantum computing more accessible and applicable in real-world scenarios.

One of the most promising opportunities for applying AI in quantum computing is automated circuit synthesis. AI can assist researchers in finding the most efficient way to arrange the gates and qubits in a quantum circuit. For example, ML algorithms can analyze different circuit designs and suggest improvements that can result in faster and more reliable quantum computations. This task would be practically impossible for humans to perform at the same rate and level of complexity.

## Hyperparameter Optimization, Real-Time Adaptation, and Benchmarking for Performance Analysis

Like their classical counterparts, quantum algorithms have hyperparameters that need fine-tuning to ensure their optimal performance. AI-driven optimization techniques such as grid search, random search, or even more advanced methods like Bayesian optimization can be used to find the optimal set of hyperparameters for a given quantum algorithm. This fine-tuning can result in significantly faster computational speeds and more accurate results.

In a quantum environment, system conditions can change rapidly due to factors like external noise or decoherence. AI models trained on monitoring quantum systems can adapt their algorithms in real time to account for these changes. These AI-driven adaptive algorithms can make quantum computing systems more resilient and consistent in performance.

AI can also assist in the comparative analysis and benchmarking of different quantum algorithms. By training ML models on a range of metrics such as speed, reliability, and resource utilization, it becomes easier to evaluate the efficiency of different algorithms, thereby guiding further research and development efforts.

## How AI Can Revolutionize Quantum Hardware Optimization

Quantum computers operate using quantum bits (qubits) which are notoriously prone to errors due to quantum noise and decoherence. The susceptibility of qubits to environmental conditions creates a high error rate, which can greatly affect computational results. In addition, quantum computers are extremely sensitive to physical parameters like electromagnetic pulses and temperature. Proper calibration and tuning of these parameters are necessary for the efficient and accurate performance of quantum algorithms.

ML algorithms and AI implementations can model the error patterns observed in qubits, identifying the types and frequencies of errors that occur. This predictive modeling helps engineers preemptively apply error-correction measures, thereby increasing the reliability of quantum computations.

Quantum error-correction codes protect quantum states from errors without collapsing them. AI can fine-tune these codes, making them more efficient and robust. Algorithms can analyze and adjust the mathematical properties of the codes, enhancing their error-correcting capabilities. AI algorithms can determine which error-correction codes are most suitable for specific tasks or under particular conditions, optimizing the error-correction process in real time.

Advanced ML techniques such as anomaly detection can identify unconventional patterns in qubit behavior that might escape traditional error-correction algorithms, further increasing system robustness.

Calibration involves a multitude of variables, from the shape and amplitude of control pulses to timing sequences. AI algorithms can scour this high-dimensional space to find the optimal set of parameters, automating what would be a near-impossible task for humans. AI can adjust the system parameters in real time, adapting to any drifts or changes in the system environment. This dynamic calibration ensures that quantum computations are performed under optimal conditions.

What about automated benchmarking? AI can validate the effectiveness of the calibration by running a series of benchmark tests, comparing the results against established standards or previous performance metrics.

AI can assist in simulating quantum mechanical systems to design new materials with desirable properties. In particular, it can optimize simulation parameters and interpret simulation results, making quantum simulations more efficient and informative.

## Control Operation and Resource Optimization

AI algorithms can dynamically adapt control strategies to improve the reliability and performance of quantum operations. In real-world quantum experiments, AI has been shown to facilitate the automatic tuning of devices and systems, thereby saving researchers valuable time.

In addition, AI can be applied to analyze experimental data while filtering out noise and improving the quality of quantum measurements. ML algorithms can sift through complex quantum data to find subtle patterns or insights that might not be immediately obvious to human researchers.

AI can optimize how tasks are divided between classical and quantum processors to make the most effective use of computational resources. The AI algorithms can optimize routing and improve the efficiency of quantum networks, similar to how they can be applied to enhance QKD.

## Data Analysis and Interpretation

### Quantum Machine Learning: Leveraging AI Research to Uncover Quantum Advantages in ML Tasks

Let's explore how AI research can help identify areas where quantum computing can offer advantages over classical computing in ML tasks. We will also delve into the development of quantum algorithms that can be incorporated into classical ML models for enhanced performance. AI algorithms can be used to analyze the computational complexity and resource requirements of different ML tasks. Through such analysis, researchers can identify which tasks are most suitable for quantum computing solutions.

AI can assist in selecting the quantum features that are most relevant for a particular ML model, thereby reducing the dimensionality of the problem and making it more manageable for quantum algorithms. ML techniques can be used to optimize the parameters of quantum algorithms, making them more efficient and effective.

Quantum principal component analysis (qPCA) can perform dimensionality reduction much faster than its classical counterpart can. It is particularly useful in big data scenarios, where classical PCA becomes computationally expensive. You can learn more about qPCA from the research paper at the following site: <https://arxiv.org/abs/1307.0401>.

Quantum support vector machines (SVMs) can solve the optimization problem in polynomial time, offering a significant speed advantage over classical SVMs for certain datasets. In addition, quantum neural networks (QNNs) can leverage the principles of quantum mechanics to perform complex computations more efficiently. They are particularly useful for tasks that require the manipulation of high-dimensional vectors. The following paper introduces some of the concepts of QNN: <https://arxiv.org/abs/1408.7005>.

**TIP** Another approach is to create hybrid models that use classical algorithms for tasks where they are more efficient and quantum algorithms where they offer advantages.

Quantum algorithms can be incorporated as subroutines in classical ML models. For instance, a qPCA subroutine can be used in a classical neural network model. Quantum algorithms can act as accelerators for specific tasks within a classical ML pipeline, such as optimization or feature selection.

## AI in Blockchain Technologies

Blockchain is a decentralized, distributed ledger technology that enables secure and transparent transactions. It eliminates the need for intermediaries, making transactions faster and more cost-effective. Blockchain technologies can ensure the integrity and security of the data that AI algorithms use. This is particularly important in fields like healthcare and finance, where data integrity is crucial.

**TIP** AI can operate on decentralized networks powered by blockchain, making the AI algorithms more robust and less susceptible to attacks.

## Automating the Execution of Smart Contracts with AI

Smart contracts have revolutionized the way we think about contractual agreements. These self-executing contracts, in which the terms are directly written into code, have emerged as a cornerstone of blockchain technology. The blockchain technology ensures that they are both immutable and transparent. However, the integration of AI into this domain can take smart contracts to the next level by automating their execution and making them more intelligent. This section explores how AI can automate the execution of smart contracts, as well as the benefits and challenges of this integration.

AI can play a significant role in automating the execution of smart contracts. By integrating ML algorithms and data analytics, AI models could make smart contracts more dynamic and more adaptable to real-world conditions. AI algorithms can make decisions based on predefined conditions, triggering the execution of certain clauses in the smart contract. AI models can also provide dynamic adaptation benefits. The AI technology can adapt the terms of the contract based on real-time data, such as market conditions, thereby automating complex decision-making processes. AI models could also be fine-tuned to automatically verify the conditions that trigger the execution of a smart contract, reducing the need for third-party verification.

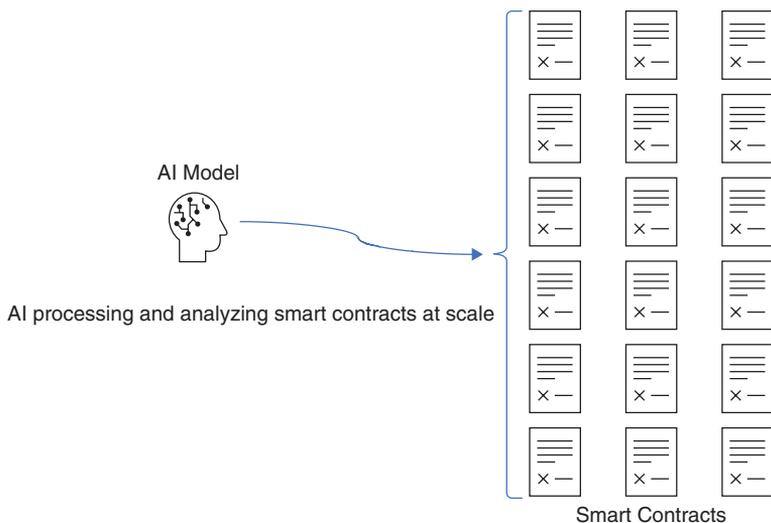
Figure 7-2 illustrates how AI can process and analyze smart contract data much faster than humans ever could, making the execution of contracts more efficient.

Automating the execution of smart contracts eliminates the need for intermediaries, which in turn reduces transaction costs. AI algorithms can detect fraudulent activities and anomalies, adding an extra layer of security to smart contracts.

However, there are a few challenges in this application area. The integration of AI into smart contracts can make them more complex and harder to understand. The AI models also require access to data, which could raise privacy concerns.

As an example, consider a use case in the real estate industry. Automated, AI-driven smart contracts can handle everything from property listings to the final sale, adapting to market conditions.

Another use case is in the supply chain. Smart contracts can automatically validate the receipt of delivered goods and trigger payments, with AI algorithms optimizing this process.



**Figure 7-2**

*AI Processing and Analyzing Smart Contracts*

AI models could also assess claims data and automatically execute payouts when certain conditions are met. The integration of AI and smart contracts remains in its infancy at the moment, but it holds immense promise for making contracts smarter, more efficient, and more secure.

## Could We Optimize Blockchain Mining Through AI Algorithms?

One of the most significant challenges that blockchain networks face is the resource-intensive nature of mining. The process of mining, which involves solving complex mathematical problems to validate transactions and add them to the blockchain, consumes vast amounts of computational power and energy.

The traditional proof-of-work (PoW) mining algorithms, such as those used in Bitcoin, require significant computational power. This has led to an enormous energy footprint, comparable to that of some small countries. The need for specialized hardware such as application-specific integrated circuits (ASICs) and graphics processing units (GPUs) has made mining inaccessible to average users. The time and resources required for mining limit the number of transactions that can be processed, affecting the scalability of the network.

AI algorithms could predict the most efficient way to allocate resources for mining, based on factors such as network traffic, transaction volume, and hardware capabilities. In consequence, mining power could be used where it's most needed.

AI models could be used to dynamically adjust the difficulty level of mining problems, ensuring that the network remains secure without wasting computational resources. ML algorithms may be able to facilitate more efficient pooling strategies among miners, optimizing the use of computational power across the network. AI models could also manage the energy usage of mining farms, automatically switching off unnecessary systems and optimizing cooling solutions.

Many people are trying to use ML to optimize Bitcoin mining. These algorithms analyze vast datasets to predict the best times to mine, based on energy costs and network difficulty. Ethereum, for example, is exploring the integration of AI algorithms to make its transition to proof-of-stake (PoS) more efficient, further reducing the network's energy consumption.

## **Additional Use Cases in Healthcare, Supply Chain Management, Financial Services, and Cybersecurity**

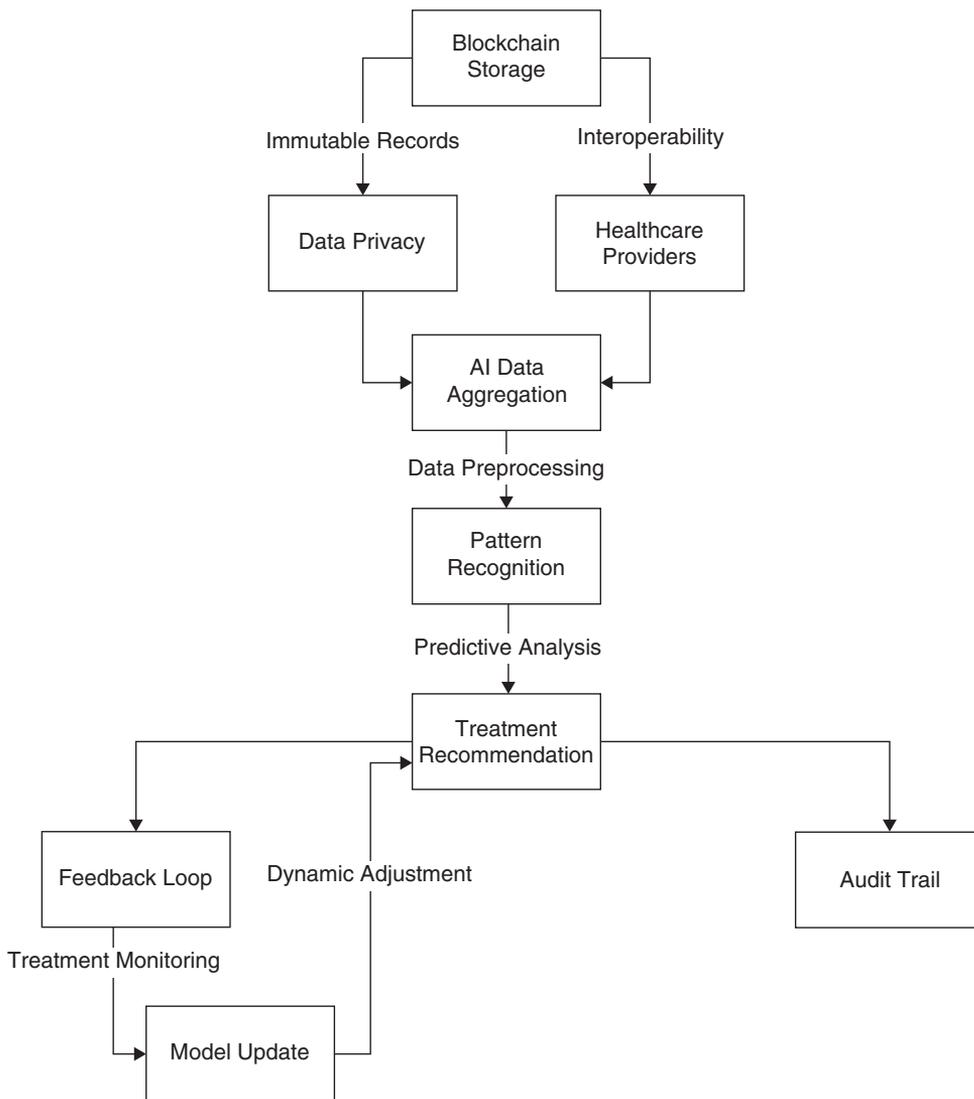
The integration of AI models with medical records stored on a blockchain could revolutionize healthcare by providing more personalized, secure, and efficient treatment plans. With this approach, medical records would be stored on a blockchain, ensuring that they are immutable and tamper-proof. Blockchain's decentralized nature could be leveraged to ensure that patients control who can access their medical records. Different healthcare providers could access the blockchain to update medical records, ensuring they and other providers have a comprehensive view of the patient's history.

In such a system, AI algorithms could pull data from the blockchain after receiving permission from the patient or healthcare provider. The AI would clean and structure the data for analysis, by performing normalization, handling missing values, and accomplishing feature extraction. ML models could be applied to identify patterns and correlations in the medical data. For example, they might find that certain combinations of symptoms, medical history, and genetic factors are indicative of specific conditions. The AI system could then predict the likely progression of diseases or conditions based on current and historical data. Algorithms could suggest personalized treatment plans, including medication types, dosages, and lifestyle changes.

As the patient undergoes treatment, updates would be made to the blockchain. The AI model would continually learn from new data, refining its predictions and recommendations. The treatment plan can be dynamically adjusted based on real-time data and the AI's evolving understanding of the patient's condition. Figure 7-3 illustrates an example of this concept.

Both the blockchain and AI algorithms must comply with data protection regulations like the Health Insurance Portability and Accountability Act (HIPAA) in the United States. Such algorithms could be used to automate permissions and ensure only authorized personnel can access specific data. Blockchain provides a transparent audit trail, which can be crucial for accountability and in case of any cybersecurity incidents. Care must be taken to ensure the AI algorithms do not inherit biases present in the training data. Patients should be fully informed about how their data will be used and analyzed.

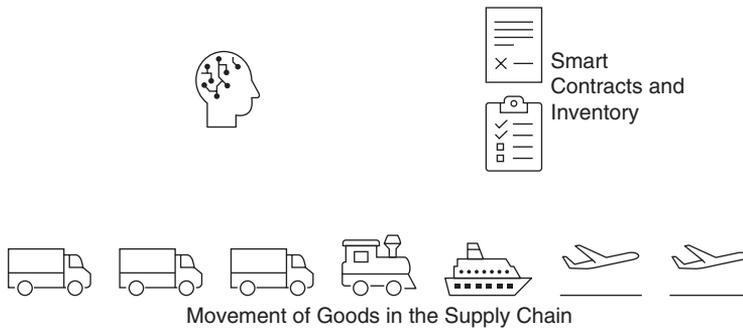
What about in the supply chain? Blockchain and AI can be used for tracking the movement of goods. Blockchain provides a decentralized, immutable ledger that records every transaction or movement of goods. This ensures that all parties in the supply chain have access to the same information, enhancing transparency and traceability. Smart contracts (i.e., self-executing contracts with the terms directly written into code) can be used to automate various processes such as payments, receipts, and compliance checks, thereby reducing manual errors and inefficiencies. The blockchain can be updated in real time as goods move from one point to another. This enables quick identification and resolution of issues such as delays or lost shipments.



**Figure 7-3**  
AI and Blockchain in Healthcare

Blockchain can be used to verify the authenticity of products by providing a complete history of its journey from the manufacturer to the end user. The immutable nature of blockchain makes it nearly impossible to tamper with the data, reducing the chances of fraud and theft.

AI can be used in combination with blockchain technology to accelerate many tasks in the supply chain, as illustrated in Figure 7-4.



**Figure 7-4**

*AI and Blockchain in the Supply Chain*

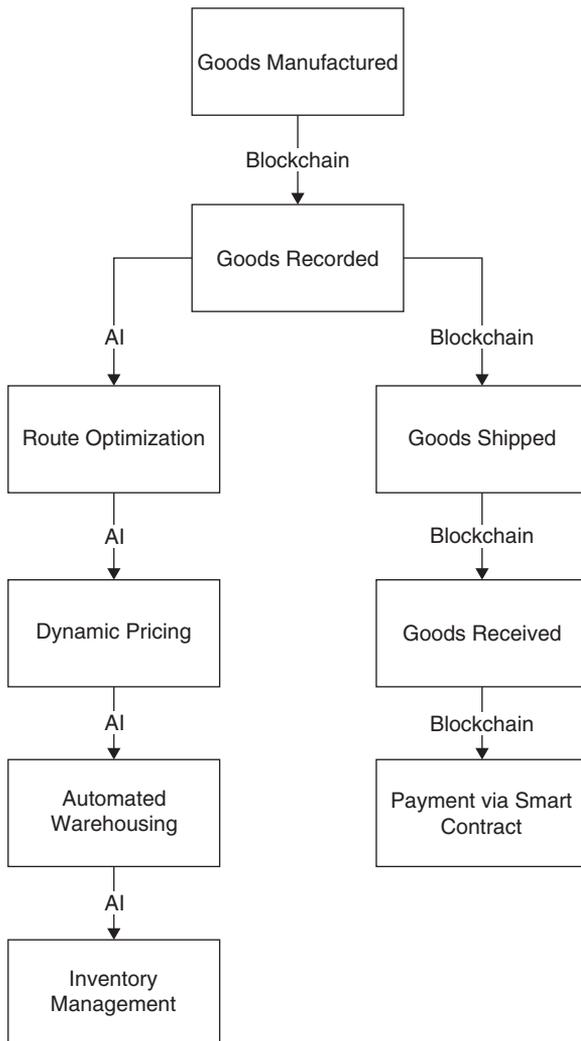
AI models can analyze historical data to predict future demand, helping companies to better plan their inventory and shipping schedules. These models can analyze a variety of factors, such as traffic conditions, weather, and road closures, to determine the most efficient route for shipments, thereby saving time and fuel costs. AI can also help in determining the most cost-effective shipping methods and carriers based on real-time data, which can significantly reduce shipping costs. AI-powered robots and systems can manage inventory more efficiently, reducing the costs associated with warehousing.

AI algorithms can continuously monitor the condition of goods in transit, alerting the interested parties about problematic issues such as temperature fluctuations or potential damage, and allowing them to take proactive measures. Figure 7-5 explains which tasks might benefit from the combination of blockchain and AI.

The intersection between AI and blockchain can also be a powerful force in enhancing security, especially in detecting fraudulent activities and monitoring for unusual activities in real time. AI algorithms can analyze transaction patterns over time to identify anomalies or irregularities that might indicate fraudulent activities. Unlike traditional methods that may involve periodic checks, AI can analyze transactions in real time, allowing for immediate detection and action. Advanced ML models can be trained to recognize the characteristics of fraudulent transactions, with the models becoming more accurate over time as they are exposed to more data.

Natural language processing (NLP) can also be performed to analyze textual data such as smart contract codes or transaction notes to identify suspicious language and hidden loopholes. The AI system could assign risk scores to transactions based on factors such as the transaction amount, the reputations of the parties involved, and the nature of the transaction, allowing for prioritized scrutiny.

AI technology can be applied to monitor the data packets being sent and received within the blockchain network to identify any unusual or unauthorized data transfers. By understanding the normal behaviors of users and nodes within the blockchain network, AI can quickly identify abnormal behaviors that deviate from the established patterns. Upon detecting unusual activities, the AI model can automatically send alerts to administrators or even take predefined actions such as temporarily blocking a user or transaction. AI can also be used to audit the smart contracts that automate transactions within the blockchain, a process that can help in identifying vulnerabilities or malicious code within the contracts.



**Figure 7-5**

*Examples of AI and Blockchain Supply Chain Tasks*

## AI in Autonomous Vehicles and Drones

From self-driving cars navigating bustling cityscapes to drones performing surveillance or delivering packages, the role of AI in autonomous transportation is indisputable. Let's explore how AI is shaping these two domains and the ethical considerations that arise.

Self-driving cars use a combination of sensors—for example, LiDAR, radar, and cameras—to gather data about their environment. AI algorithms then integrate this data to create a cohesive view of the surroundings, aiding in navigation and obstacle avoidance. AI models are at the core of the decision-making process in autonomous vehicles. These algorithms take into account key factors such as road conditions, traffic signals, and pedestrian movements to make split-second decisions that can be crucial for safety.

Using ML algorithms, autonomous vehicles can predict the actions of other vehicles and pedestrians. This helps in proactive decision-making, reducing the likelihood of accidents. Over time, AI algorithms will learn from millions of miles of driving data, improving their decision-making and predictive capabilities. This iterative learning is vital for the adaptability and reliability of autonomous vehicles.

Drones equipped with AI can autonomously navigate through complex environments. This ability is particularly useful in applications such as forest monitoring, search and rescue, and military surveillance. Advanced ML algorithms enable drones to recognize objects or individuals.

These capabilities may also have significant benefits in sectors like agriculture, where drones can identify unhealthy crops, and in security, where they can spot intruders. Drones generate enormous amounts of data. AI algorithms can analyze this data in real time, providing valuable insights during tasks such as environmental monitoring and infrastructure inspection. AI enables drones to work in a swarm, coordinating with each other to accomplish tasks more efficiently. This collaboration is useful in applications like agriculture, disaster relief, and even entertainment.

The data collected by autonomous vehicles and drones can be sensitive in nature, so ensuring its privacy and security is a critical concern. AI algorithms can make mistakes—and in the context of autonomous vehicles and drones, these mistakes can be fatal. Rigorous testing and validation are necessary to ensure safety. Automation through application of AI technologies could also result in significant job losses in sectors like transportation and logistics.

## AI in Edge Computing

The Internet of Things (IoT) introduces three technical requirements that challenge the centralized cloud computing paradigm and create a need for an alternative architecture:

- 1. Handling the data deluge:** The billions of IoT devices that are projected to be connected to the Internet will collectively create massive amounts of data. These devices will be deployed across a wide geographic footprint, and the data that they generate needs to be collected, aggregated, analyzed, processed, and exposed to consuming systems and applications.

# Index

## A

- access control
  - DAC (dynamic access control), 84–86
  - discretionary, 84
  - login and access behavior, 86
  - overview of, 49–50, 77
- accident-prevention applications, 133
- account management
  - account provisioning/deprovisioning, 83–84
  - IAM (identity and account management), 80–84
- addresses
  - IP (Internet Protocol), 142
  - MAC (Medium Access Control), 142
- advanced data analytics, AIoT (AI in the Internet of Things), 124–125
- advanced persistent threats (APTs), 26
- Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK), 28
- affective computing, 116
- agency, excessive, 25–26
- agent-customer interaction, 112
- agriculture, Edge AI in, 181
- AI (artificial intelligence)
  - black box problem in, 5, 28
  - ethical implications of, 28
  - expansion across various sectors, 14–15
  - history of, 2–5
  - impact of, 2
  - job market impacted by, 15–17
  - overview of, 1–2
  - privacy, 28–30
  - XAI (explainable AI), 5
- AI bill-of-materials (AI BOMs), 22
- AlaaS (AI as a service)
  - advantages of, 156–157
  - AI developer services, 154–155
  - AI infrastructure services, 154
  - AI software services, 155–156
  - challenges of, 158
  - overview of, 153–154
- AI-driven cryptanalysis, 87–88
- AIoT (AI in the Internet of Things)
  - data analytics
    - advanced analytics, 124–125
    - anomaly detection, 122, 126
    - data processing, 122
    - overview of, 122
    - predictive maintenance, 123–124
  - impact of, 119–120
  - IoT reference layers, 120–121
  - IoT security
    - authentication, 132
    - overview of, 130–131

- physical safety and security, 126, 133
  - threat detection, 131
  - vulnerability detection, 132
- resource optimization, 125–127
- supply chain, 127–129
- sustainability
  - circular economy practices, 135–137
  - energy management, 134
  - overview of, 133–134
  - waste management and recycling, 134–135
  - water management, 134
  - wildlife conservation, 135
- Alexa, 102
- AlexNet, 3
- AlphaFold, 3
- AlphaGo, 3, 11
- analyzing\_logs.py, 62
- anomaly detection
  - AIoT (AI in the Internet of Things), 122, 126
  - cloud computing, 146–147
  - text-based, 67–68
- anti-malware systems, 50–51
- APIs (application programming interfaces), 34
- Apple Music, 97
- application development
  - dynamic analysis, 90
  - intelligent threat modeling, 91
  - patch management, 92–93
  - SCM (secure configuration management), 91–92
- application mobility, 142
- application programming interfaces (APIs), 34
- application security, 52
- application-specific integrated circuits (ASICs), 170
- APTs (advanced persistent threats), 26
- ARIMA (autoregressive integrated moving average), 146–147
- ARM-NN, 179
- AR/VR (augmented and virtual reality), 99, 113–114
- ASICs (application-specific integrated circuits), 170
- assessments, security, 77–80
- asset twins, 54
- assurance, network, 40–44
- ATM, 34
- ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge), 28
- attacks. *See also* security
  - backdoor, 27
  - cloud computing, 148–149
  - insecure output handling, 22
  - malware, 50–51
  - MITRE ATLAS framework for, 28
  - model denial of service, 22–23
  - model inversion and extraction, 26–27
  - model theft, 26
  - potential threat intelligence, 65–67
  - prompt injection, 17–22
  - training data poisoning, 22
- audio conferencing, 96
- augmented and virtual reality (AR/VR), 99, 113–114
- authentication, 101, 132
- authorization, 81–83
- autoencoders, 11
- automation
  - blockchain mining, 170–171
  - circuit synthesis, 166
  - industrial, Edge AI in, 181
  - machine learning (autoML), 154
  - network assurance, 40–44
  - network configuration, 38–40
  - network planning, 37–38
  - smart contract execution, 169–170
  - workflow, 103
- AutoML, 154–155
- autonomous networking, 36
- AS (autonomous system), 45–46
- autonomous vehicles and drones, 15, 175
- autoregressive integrated moving average (ARIMA), 146–147

---

## B

- backdoor attacks, 27
- BART, 108
- BB84 protocol, 89, 165

behavioral analytics, 51–52  
 behavioral biometric, 82  
 benchmarking, 166–167  
 Bennett, Charles, 89  
 BERT (Bidirectional Encoder Representations from Transformers), 9, 11, 12, 108  
 BGP (Border Gateway Protocol), 45–46  
 bill-of-materials (BOMs), 24  
 BIM (building information model) files, 38  
 biometrics, behavioral, 82  
 black box problem, 5, 28  
 blockchain technologies  
   blockchain mining, 170–171  
   in cybersecurity, 171–174  
   in financial services, 171–174  
   in healthcare, 171–174  
   smart contract execution, 169–170  
   in supply chain management, 171–174  
 BOMs (bill-of-materials), 24  
 Border Gateway Protocol (BGP), 45–46  
 Brassard, Gilles, 89  
 building information model (BIM) files, 38

**C**

---

CAC (call admission control), 45–46  
 CAD (computer-aided design) files, 38  
 CAFFE2, 179  
 call admission control (CAC), 45–46  
 cameras, in autonomous vehicles, 175  
 capsule networks, 11  
 CBOW (Continuous Bag of Words), 108  
 CBRN (chemical, biological, radiological, and nuclear) threats, 163  
 chain of custody, 137  
 chatbots, 21  
 ChatGPT, 11  
   incident reports, creating, 69–70  
   STIX documents, creating, 66–67  
 chemical, biological, radiological, and nuclear (CBRN) threats, 163  
 CHOP properties, 36  
 Chroma DB, 80  
 CI (continuous integration), 91

circular economy practices, 135–137  
 CISA (Cybersecurity and Infrastructure Security Agency), 93  
 classification, traffic, 52–54  
 Claude, 11  
 CLI (command-line interface), 34, 38–39  
 cloud computing  
   AI's expansion across, 14–15  
   anomaly detection, 146–147  
   application mobility, 142  
   business adoption of, 139  
   characteristics of, 139–140  
   collaboration in, 98  
   definition of, 139–140  
   demand prediction, 146  
   deployment models, 143–144  
   future of, 158–159  
   infrastructure management, 145  
   infrastructure optimization, 152–153  
   load balancing, 146  
   machine learning as a service  
     advantages of, 156–157  
     AI developer services, 154–155  
     AI infrastructure services, 154  
     AI software services, 155–156  
     challenges of, 158  
     overview of, 153–154  
   orchestration, 144  
   security, 147–150  
   service models, 143  
   service optimization, 151–152  
   SLA (service level agreement), 146  
   virtual machine placement, 145–146  
   virtualization, 140–142  
   workload placement, 145–146  
 CNN (convolutional neural networks), 7–8, 11, 114  
 collaboration  
   AI's expansion across, 14–15  
   communications and user experience, 101–102  
   contact centers, 109–112  
   content generation, 114  
   context and intent analysis, 103

- customer sentiment, 112
  - digital communications, advances in, 96
  - document management, 108–109
  - Hugging Face Hub, 12–13
  - hybrid work, 99–101
  - innovations in, 97–99
  - larger case volume handling, 112
  - learning and development, 105–106, 114
  - overview of, 95
  - personalization of interaction, 115–116
  - physical collaboration spaces, 106
  - predictive analytics, 113
  - prescriptive analytics, 104–105
  - quality assurance, 112
  - real-time rendering, 114
  - real-time translation, 101
  - schedule prediction and adjustment, 105
  - task management, 102–103
  - team dynamics, 107–108
  - through voice/speech recognition, 101
  - tools of, 96
  - upgrading and upselling, 113
  - virtual assistants, 102
  - virtual collaboration spaces, 106–107
  - workflow automation, 103
  - Colvile, Robert, 95
  - command-line interface (CLI), 34, 38–39
  - Common Security Advisory Framework (CSAF), 72–73
  - communications, collaborative. *See* collaboration
  - community cloud, 143
  - compliance, 54
  - component twins, 54
  - computer networking. *See* networking
  - computer-aided design (CAD) files, 38
  - CompVis, 13
  - configuration, 38–40
    - cloud computing, 145
    - SCM (secure configuration management), 91–92
    - security, 60
  - Conjur, 62–63
  - contact centers, 109–112
  - containers, 141
  - content generation, 114
  - context and intent analysis, 103
  - Continuous Bag of Words (CBOW), 108
  - continuous integration (CI), 91
  - control operation, quantum computing, 168
  - convolutional neural networks (CNN), 7–8, 10, 114
  - co-pilots, security, 76–77
  - cost, supply chain, 128
  - CPU instruction set level virtualization, 140–142
  - cross-site request forgery (CSRF), 22
  - cross-site scripting (XSS), 22
  - cryptography
    - AI-driven cryptanalysis, 87–88
    - definition of, 87
    - dynamic, 88
    - QKD (quantum key distribution), 163
    - quantum, 88–89
  - CSAF (Common Security Advisory Framework), 72–73
  - CSRF (cross-site request forgery), 22
  - custody, chain of, 137
  - customers
    - agent-customer interaction, 112
    - contact centers, 109–112
    - experience of, 182
    - sentiment of, 112
  - CVE, 73
  - cybersecurity. *See* security
  - Cybersecurity and Infrastructure Security Agency (CISA), 93
- ## D
- 
- DAC (dynamic access control), 84–86
  - DALL-E, 6
  - Dartmouth Conference, 3
  - data analytics
    - advanced analytics, 124–125
    - anomaly detection, 122, 126
    - data processing, 122
    - IoT (Internet of Things), 122–125
    - overview of, 122

- predictive maintenance, 123–124
    - quantum computing, 168
  - data processing, AIoT (AI in the Internet of Things), 122
  - decentralized ledger technology (DLT), 182
  - decision making
    - advanced analytics, 124–125
    - AIoT (AI in the Internet of Things), 122–125
    - anomaly detection, 122, 126
    - data processing, 122
    - overview of, 122
    - predictive maintenance, 123–124
  - decision trees, 10
  - Deep Blue, 3
  - deep packet inspection (DPI), 49, 53
  - DeepMind, 3
  - DEI (diversity, equity, and inclusion), 99–100
  - delivery logistics, 128
  - demand changes, 128
  - demand prediction, 146
  - denial-of-service (DoS) attacks, 148
  - deployment models, cloud computing, 143–144
  - deprovisioning accounts, 83–84
  - designs, secure network, 74–75
  - developer services, 154–155
  - DevOps, 92
  - DevSecOps, 92
  - differential privacy, 30
  - digital twins (DT), 54–55, 132
  - Dijkstra shortest path algorithm, 45–46
  - disassembly, design for, 136
  - discretionary access control, 84
  - diversity, equity, and inclusion (DEI), 99–100
  - DLT (decentralized ledger technology), 182
  - Docker, 141–142
  - document management, collaboration in, 108–109
  - DoS (denial-of-service) attacks, 22–23, 148
  - DPI (deep packet inspection), 49, 53
  - drones, 15, 175
  - DT (digital twins), 54–55, 132
  - dynamic access control (DAC), 84–86
  - dynamic analysis, 90
  - dynamic cryptography, 88
- ## E
- 
- edge computing, 175–178
  - eFax, 96
  - elevated privileges, 22
  - ELIZA, 3
  - ELL (Embedded Learning Library), 179
  - Ellen MacArthur Foundation, 135
  - ELMO (Embeddings from Language Models), 108
  - Embedded Learning Library (ELL), 179
  - embedded systems, 9
    - cybersecurity, 75
    - security, 75
  - Embeddings from Language Models (ELMO), 108
  - emerging technologies
    - autonomous vehicles and drones, 175
    - blockchain technologies, 169–174
    - edge computing, 175–178
    - executive order on, 162–163
    - fog computing, 176–177
    - Lightweight AI, 178–182
    - overview of, 161
    - quantum computing, 163–168
    - Tiny ML, 178–182
    - Web 3.0, 182–183
  - employee experience, 126–127
  - emulation, 55, 140
  - energy management, 48–49, 126, 134
  - ensemble learning, 71
  - environmental efficiency, 125
  - EPSS (Exploit Prediction Scoring System), 72–73, 93
  - Ethernet, 34
  - ethics, 17, 28
  - ETL (extraction, transform, load), 122
  - executive order on emerging technologies, 162–163
  - expansion of AI (artificial intelligence), 14–15
  - explainable AI (XAI), 5
  - Exploit Prediction Scoring System (EPSS), 72–73, 93
  - extraction, 26–27, 122

## F

FaaS (Function as a Service), 143  
 facial expression analysis, 116  
 facial recognition, 98  
 Falcon, 6, 12  
 farming, Edge AI in, 181  
 FastText, 108  
 feature extraction, 8–9  
 federated learning, 30  
 field programmable gate arrays (FPGAs),  
   139–140  
 files, log, 60–65  
 financial services, blockchain technologies in,  
   171–174  
 fine-tuning, 8  
 firewalls, 51  
 FIRST (Forum of Incident Response and Security  
   Teams), 72–73  
 fog computing, 176–177  
 Forum of Incident Response and Security Teams  
   (FIRST), 72–73  
 FPGAs (field programmable gate arrays),  
   139–140  
 Frame Relay, 34  
 frameworks  
   Lightweight AI, 178–179  
   Tiny ML, 178–179  
 Function as a Service (FaaS), 143

## G

GANs (generative adversarial networks), 11, 114  
 Gemini, 11, 12  
 generative adversarial networks (GANs), 11, 114  
 geopolitical conflicts, supply chain  
   impacted by, 128  
 GloVe (Global Vectors for word representation),  
   9, 108  
 GNNs (graph neural networks), 11, 55  
 Google, AlphaGo, 3  
 governance, security, 73–74  
 GPT, 11  
 GPT-2, 12

GPT-3, 12  
 GPT-4, 12, 16, 69–70  
 GPUs (graphics processing units), 139–140, 170  
 graph databases, 99  
 graph neural networks (GNNs), 11, 55  
 graphics processing units (GPUs), 139–140, 170  
*Great Acceleration, The* (Colvile), 95  
 Grover, Lov, 164  
 Grover's algorithm, 164  
 guest instruction sets, 140

## H

hardware abstraction layer level virtualization,  
   140–142  
 Hashicorp's Vault, 62–63  
 Health Insurance Portability and Accountability  
   Act (HIPAA), 171  
 healthcare  
   blockchain technologies in, 171–174  
   Edge AI in, 180  
 hierarchical models, 71  
 Hinton, Geoffrey, 3  
 HIPAA (Health Insurance Portability and  
   Accountability Act), 171  
 history of AI (artificial intelligence)  
   development, 2–5  
 host instruction sets, 140  
 Hugging Face Hub, 12–13, 108  
 hybrid cloud, 144  
 hybrid work, 99–101  
 hype cycle, 100  
 hyperparameter optimization, 166–167  
 hypervisors, 140

## I

IaaS (Infrastructure as a Service). *See* IP (Internet  
 Protocol) addresses  
 IAM (identity and account management), 80–81  
 IANA (Internet Assigned Numbers Authority), 53  
 IBM Watson, 3  
 IBN (intent-based networking), 35–36

IETF (Internet Engineering Task Force), 36, 55  
 “if this, then that” (IFTTT) analysis, 119  
 IGP (Interior Gateway Protocols), 45–46  
 ImageNet Large Scale Visual Recognition Challenge, 3  
 internetworking, 34  
 incident response
 

- incident reports, creating, 69–70
- integration with other models, 71
- overview of, 59–60
- potential threat intelligence, 65–67
- predictive analytics, 60–65
- sentiment analysis, 65–67
- SOCs (security operations centers), 68–70
- text-based anomaly detection, 67–68

 independent software vendors (ISVs), 17  
 industrial monitoring, Edge AI in, 181  
 Infrastructure as a Service (IaaS), 143  
 infrastructure management, 145, 154  
 innovations, in collaboration, 97–99  
 insecure output handling, 22  
 instant messaging, 96  
 intelligent authorization, 80–83  
 intelligent threat modeling, 91  
 intent-based networking (IBN), 35–36  
 interactive learning, 114  
 interactive voice response agents (IVR), 111  
 Interior Gateway Protocols (IGP), 45–46  
 International Telecommunication Union (ITU), 55  
 Internet Assigned Numbers Authority (IANA), 53  
 Internet Engineering Task Force (IETF), 36, 55  
 Internet Protocol addresses. *See* IP (Internet Protocol) addresses  
 inversion, model, 26–27  
 investment, discovering areas of, 127  
 IoT (Internet of Things), 34
 

- AI’s expansion across, 14–15
- cybersecurity, 75
- data analytics, 122–125
- reference layers, 120–121
- resource optimization, 123–124
- security, 130–133

 IP (Internet Protocol) addresses, 142  
 IP (Internet Protocol) telephony, 96, 97

ISDN, 34  
 issue detection, 42–43  
 ISVs (independent software vendors), 17  
 ITU (International Telecommunication Union), 55  
 IVRs (interactive voice response agents), 111

## J-K

---

job market, AI’s impacts on, 15–17

K8s (Kubernetes), 142  
 Kasparov, Garry, 3  
 KEV (Known Exploited Vulnerability) catalog, 93  
 keys
 

- KPIs (key performance indicators), 42
- QKD (quantum key distribution), 88–89

 K-means, 10  
 K-nearest neighbors (KNN), 10  
 knowledge graphs, 99  
 Known Exploited Vulnerability (KEV) catalog, 93  
 KPIs (key performance indicators), 42  
 Krizhevsky, Alex, 3  
 Kubernetes, 142

## L

---

LAION, 13  
 LangChain, 21, 78–80  
 language models, 98  
 large language models. *See* LLMs (large language models)  
 larger case volume handling, 112  
 learning and development (L&D)
 

- collaboration in, 105–106
- interactive learning, 114

 LiDAR, 175  
 life-cycle management, 128  
 Lightweight AI, 178–182  
 linear regression, 9  
 LLaMA, 6, 11, 12  
 LLMs (large language models), 98. *See also* security
 

- integration with other models, 71
- predictive analytics, 60–65

- sensitive information disclosure, 24–25
- sentiment analysis, 65–67
- SOCs (security operations centers), 68–70
- text-based anomaly detection, 67–68
- traditional machine learning compared to, 6–11
- transfer learning, 7–9
- Transformer-based models, 6
- user interactions with, 21–22

load balancing, 146

load\_dotenv() function, 62–63

log files, 60–65

logistic regression, 9

long short-term memory (LSTM), 11

low-code AI, 154–155

LSTM (long short-term memory), 11

Luke, 108

## M

M2M (machines to machines), 34

MAC (Medium Access Control) addresses, 142

machine learning. *See* ML (machine learning)

machines to machines (M2M), 34

maintenance, predictive, 122

malware

- anti-malware systems, 50–51
- malware injection attacks, 148

management, network

- automated network assurance, 40–44
- automated network configuration, 38–40
- automated network planning, 37–38
- IAM (identity and account management), 80–81
- intelligent authorization, 81–83
- radio resource, 47–48

man-in-the-middle attacks, 148

MAPE-K, 36

material sorting, 136

mathematical modeling, 55

McCarthy, John, 3

mean time to repair (MTTR), 42

Medium Access Control (MAC) addresses, 142

MFA (multifactor authentication), 81, 132

MGM Resorts International, 148–149

Microsoft Xiaoice, 3

MidJourney, 6

migration, VMs (virtual machines), 142

minimal waste, design for, 136

mining, blockchain, 170–171

Minsky, Marvin, 3

MIT Media Lab, 116

MITRE ATLAS, 28

ML (machine learning)

- collaboration in, 98
- Hugging Face Hub, 12–13
- LLMs (large language models) compared to, 6–11
- machine learning as a service
  - advantages of, 156–157
  - AI developer services, 154–155
  - AI infrastructure services, 154
  - AI software services, 155–156
  - challenges of, 158
  - overview of, 153–154
- predictive analytics, 60–65
- Tiny ML, 178–182
- traditional models of, 9–10

mobility, application, 142

model denial of service (DoS), 22–23

model inversion and extraction, 26–27

model theft, 26

monetization, discovering areas of, 127

monitoring, 42

MPLS (Multiprotocol Label Switched) networks, 45–46

MTTR (mean time to repair), 42

multi-cloud, 144

multifactor authentication (MFA), 81, 132

multimedia

- innovations in, 97–99
- streaming, 97

Multiprotocol Label Switched (MPLS) networks, 45–46

Musk, Elon, 3

MXNET, 179

MYCIN, 3

## N

Naive Bayes, 10

NAT (Network Address Translation) servers, 53

natural disasters, supply chain impacted by, 128

natural language processing (NLP). *See* NLP (natural language processing)

natural language understanding. *See* NLU (natural language understanding)

net promoter scores (NPS), 110

NETCONF (Network Configuration Protocol), 38–39

Netflix, 97

Network Address Translation (NAT) servers, 53

Network Configuration Protocol (NETCONF), 38–39

networking

- AI's expansion across, 14–15
- energy optimization, 48–49
- network digital twins, 54–55
- network management, 37–44
- network optimization, 45
- network programmability, 34
- network security, 49–52
- radio resource management, 47–48
- role of AI in, 33–36
- routing optimization, 45–47
- traffic classification and prediction, 52–54

Neural Cleanse, 27

neural machine translation (NMT), 101

neural networks

- CNN (convolutional neural networks), 7–8, 11, 114
- GNNs (graph neural networks), 11, 55
- QNNs (quantum neural networks), 11, 168
- RNNs (recurrent neural networks), 11, 53–54
- strengths and weaknesses of, 10

NFTs (non-fungible tokens), 183

NLP (natural language processing), 39–40, 173

- collaboration in, 98, 108, 109–110
- in LLMs (large language models), 6
- personalization of interaction, 115
- sentiment analysis, 65–67

NLU (natural language understanding), 39, 98, 115

NMT (neural machine translation), 101

## O

no-code AI, 154–155

noise cancellation, 98

non-fungible tokens (NFTs), 183

NoteData poisoning, 22

NPS (net promoter scores), 110

obscurity, security by, 131

occupant experience, 126–127

Office 365, 39

Office of Science and Technology Policy (OSTP), 162

son-path attacks, 148

ontologies, 99

Open Worldwide Application Security Project (OWASP), 17

OpenAI, 3

- ChatGPT, 11
  - incident reports, creating, 69–70
  - STIX documents, creating, 66–67
- Five, 11
- GPT, 6
  - log analysis, 63–65

OPENAI\_API\_KEY, 62–63

operating level virtualization, 140–142

operational technology (OT) environments, 131

optimization

- cloud computing
  - cloud infrastructure, 152–153
  - cloud service, 151–152
- energy, 48–49
- network, 45
- quantum computing
  - hyperparameters, 166–167
  - quantum hardware optimization, 167
- resource, 123–124
- routing, 45–47

orchestration, cloud computing, 144

OSTP (Office of Science and Technology Policy), 162

OT (operational technology) environments, 75, 131

overreliance on AI, 26

OWASP (Open Worldwide Application Security Project), 17

## P

PaaS (Platform as a Service), 143  
Panama Canal, 127  
patch management, 60, 92–93  
path computation element (PCE), 45–46  
PCA (principal component analysis), 9, 10  
PCE (path computation element), 45–46  
penetration testing, 77–80  
performance analysis, quantum computing, 166–167  
personalization of interaction, 115–116  
phishing, 148  
physical collaboration spaces, 106  
physical safety and security  
    AI's impacts on, 76  
    Edge AI in, 180  
    IoT (Internet of Things), 126, 133  
    security co-pilots, 76–77  
Pinecone, 80  
pip install epss-checker command, 73  
pip install kev-checker command, 93  
planning, network, 37–38  
Platform as a Service (PaaS), 143  
PLC (programmable logic controller), 131  
plugins, vulnerabilities, 25  
policies, 73–74  
port numbers, 53  
PoS (proof-of-stake), 171  
postprocessing, 71  
potential threat intelligence, 65–67  
PoW (proof-of-work) mining algorithms, 170  
prediction, traffic, 52–54  
predictive analytics, 60–65, 113, 123–124  
preprocessing, 71  
prescriptive analytics, 104–105  
presence, 98  
principal component analysis (PCA), 9, 10  
privacy, AI's impacts on, 17, 28–30  
private cloud, 143  
procedures, 73–74  
process twins, 54  
processes, 73–74  
programmability, network, 34

programmable logic controller (PLC), 131  
prompt templates, creating, 78–80  
proof-of-stake (PoS), 171  
proof-of-work (PoW) mining algorithms, 170  
provisioning accounts, 83–84  
PyTorch, 12

## Q

QAOA (quantum approximate optimization algorithm), 164  
QFT (Quantum Fourier transform), 164  
QKD (quantum key distribution), 88–89, 163  
Q-Learning, 10  
QNNs (quantum neural networks), 11, 168  
QoS (quality of service), 37, 139  
qPCA (quantum principal component analysis), 168  
quality assurance, 112  
quality control, 136  
quality issues, 128  
quality of service (QoS), 139  
quantum approximate optimization algorithm (QAOA), 164  
quantum computing, 139–140  
    algorithm tuning, 166  
    automated circuit synthesis, 166  
    benchmarking, 166–167  
    control operation, 168  
    data analysis and interpretation, 168  
    hyperparameter optimization, 166–167  
    overview of, 163  
    QKD (quantum key distribution), 163  
    quantum algorithm development, 164–166  
    quantum cryptography, 88–89  
    quantum error-correction codes, 166  
    quantum hardware optimization, 167  
    real-time adaptation, 166–167  
    resource optimization, 168  
Quantum Fourier transform (QFT), 164  
quantum key distribution (QKD), 88–89, 163  
quantum machine learning algorithms, 166  
quantum neural networks (QNNs), 11, 168  
quantum phase estimation, 164–165

quantum principal component analysis (qPCA), 168  
 quantum walk algorithms, 164–165  
 qubits, 166–167

## R

radar, 175  
 radio frequency (RF) planning, 37  
 radio resource management, 47–48  
 RAG (retrieval augmented generation), 80  
 random forest, 10  
 RBAC (role-based access control), 84  
 real-time adaptation, 166–167  
 real-time rendering, 114  
 real-time translation, 101  
 recurrent neural networks (RNNs), 11, 53–54  
 recycling, 134–135  
 red teaming, 77–80  
 reference layers, IoT (Internet of Things), 120–121  
 regression, 9  
 Reichheld, Frederick, 110  
 reinforcement learning, 10, 11  
 remediation, 44  
 rendering, real-time, 114  
 resource optimization, 104
 

- AIoT (AI in the Internet of Things), 123–124
- cloud computing, 145
- quantum computing, 168

 retrieval augmented generation (RAG), 80  
 reverse logistics, 136  
 RF (radio frequency) planning, 37  
 RNNs (recurrent neural networks), 11, 53–54  
 RoBERTa, 108  
 role-based access control (RBAC), 84  
 root-cause analysis, 43–44  
 routing optimization, 45–47  
 RRM (radio resource management), 47–48

## S

SaaS (Software as a Service), 143  
 sarcasm, 108  
 scenario analysis and planning, 54

SCM (secure configuration management), 91–92  
 SCM (source code management), 91  
 SDN (software-defined networking), 14, 34–35  
 secure network designs, 74–75  
 Secure Software Development Framework (SSDF), 77  
 security
 

- access control, 77
  - DAC (dynamic access control), 84–86
  - discretionary, 84
  - login and access behavior, 86
  - overview of, 49–50, 77
- account management
  - account provisioning/deprovisioning, 83–84
  - IAM (identity and account management), 80–84
- AI's impact on, 14–15, 17
- anti-malware systems, 50–51
- application development
  - dynamic analysis, 90
  - intelligent threat modeling, 91
  - patch management, 92–93
  - SCM (secure configuration management), 91–92
- assessments, 77–80
- attacks
  - attacks, 27
  - backdoor, 27
  - excessive agency, 25–26
  - MITRE ATLAS, 28
  - model denial of service, 22–23
  - model inversion and extraction, 26–27
  - model theft, 26
  - prompt injection attacks, 17–22
  - sensitive information disclosure, 24–25
  - supply chain, 23–24
  - training data poisoning, 22
- behavioral analytics, 51–52
- blockchain technologies in, 171–174
- cloud computing, 147–150
- configuration, 60
- cryptography
  - AI-driven cryptanalysis, 87–88

- definition of, 87
- dynamic, 88
- quantum, 88–89
- DAC (dynamic access control), 84–86
- Edge AI in, 180
- embedded systems, 75
- excessive agency, 25–26
- firewalls, 51
- governance, 73–74
- IAM (identity and account management), 80–81
- incident response
  - incident reports, creating, 69–70
  - integration with other models, 71
  - overview of, 59–60
  - potential threat intelligence, 65–67
  - predictive analytics, 60–65
  - sentiment analysis, 65–67
  - SOCs (security operations centers), 68–70
  - text-based anomaly detection, 67–68
- insecure output handling, 22
- insecure plugin design, 25
- intelligent authorization, 80–81
- IoT (Internet of Things)
  - authentication, 132
  - overview of, 130–131
  - physical safety and security, 126, 133
  - threat detection, 131
  - vulnerability detection, 132
- MITRE ATLAS, 28
- model denial of service (DoS), 22–23
- model inversion and extraction, 26–27
- model theft, 26
- by obscurity, 131
- overreliance, 26
- overview of, 17, 49, 59, 74–75
- penetration testing, 77–80
- physical security, 76–80
- policies, 73–74
- procedures, 73–74
- processes, 73–74
- prompt injection attacks, 17–22
- red teaming, 77–80
- secure network designs, 74–75
- sensitive information disclosure, 24–25
- specialized systems, 75
- supply chain, 23–24
- training data poisoning, 22
- vulnerabilities
  - cloud computing, 148–149
  - excessive agency, 25–26
  - insecure output handling, 22
  - insecure plugin design, 25
  - model inversion and extraction, 26–27
  - overreliance, 26
  - prediction of, 60
  - prioritization of, 71–73
  - sensitive information disclosure, 24–25
  - supply chain, 23–24
- security operations centers (SOCs), 68–70
- Sedol, Lee, 3
- semantic modeling, 55
- sensitive information disclosure, 24–25
- sentiment, 60–65, 112, 115
- sequential processing, 71
- serverless computing, 143
- servers, NAT (Network Address Translation), 53
- server-side request forgery (SSRF), 22
- service level agreement (SLA), 34, 46, 146
- service models, cloud computing, 143
- services
  - machine learning as, 153–158
    - advantages of, 156–157
    - AI developer services, 154–155
    - AI infrastructure services, 154
    - AI software services, 155–156
    - challenges of, 158
    - overview of, 153–154
- Shor, Peter, 164
- Shor's algorithm, 164
- Simple Network Management Protocol (SNMP), 38–39
- Siri, 102
- Skip Grams, 108
- SLA (service level agreement), 34, 46, 146
- smart cities, 127

smart contracts, 169–170  
 smart drones, 15  
 smart grids, 182  
 smart spaces, 182  
 SNMP (Simple Network Management Protocol), 38–39  
 SOCs (security operations centers), 68–70  
 software and application security, 52  
 Software as a Service (SaaS), 143  
 software services, 155–156  
 software-defined networking (SDN), 14, 34–35  
 source code management (SCM), 91  
 sourcing changes, 128  
 spaces, collaboration, 106–107  
 Spotify, 97  
 SSDF (Secure Software Development Framework), 77  
 SSRF (server-side request forgery), 22  
 Stability AI, 13  
 Stable Diffusion, 6, 13  
 STIX (Structured Threat Information eXpression), 66–67  
 streaming technologies, 96, 97  
 STRIP, 27  
 Structured Threat Information eXpression (STIX), 66–67  
 Suez Canal, 127  
 supply chain
 

- IoT (Internet of Things), 127–129
- Stable Diffusion, 171–174
- vulnerabilities, 23–24

 supply changes, 128  
 support vector machines (SVMs), 10, 146, 168  
 support vector regression (SVR), 146  
 sustainability
 

- circular economy practices, 135–137
- energy management, 134
- overview of, 133–134
- waste management and recycling, 134, 135
- wildlife conservation, 135

 Sutskever, Ilya, 3  
 SVMs (support vector machines), 10, 146, 168  
 SVR (support vector regression), 146  
 system twins, 54

---

## T

task management, collaboration in, 102–103  
 task-specific models, 8  
 team dynamics, 107–108  
 TensorFlow, 12  
 TensorFlow Lite, 179  
 term frequency-inverse document frequency (TF-IDF), 9  
 testing, penetration, 77–80  
 text-based anomaly detection, 67–68  
 TF-IDF (term frequency-inverse document frequency), 9  
 threat detection, 131  
 threat intelligence sharing, 60  
 threat prediction, 60  
 Tiny ML, 178–182
 

- applications and use cases for, 180–182
- frameworks for, 178–179

 TipStable Diffusion, 13  
 Tokenizers library, 12  
 tools, collaboration, 96  
 traffic classification and prediction, 52–54  
 training data poisoning, 22  
 transaction patterns, 86  
 transfer learning, 7–9, 71  
 Transformer-based models, 6, 11  
 translation, real-time, 101  
 transportation issues
 

- AIoT (AI in the Internet of Things) in supply chain, 127–129
- Edge AI in, 181
- supply chain impacted by, 128

 troubleshooting, 43–44  
 trust boundary, 21  
 tuning quantum algorithms, 166  
 Turing, Alan, 3  
 Turing Test, 3

---

## U

unified communications, 98  
 upgrading, 113  
 upselling, 113

user experience, 101–102

user training, 60

## V

V2I (vehicle-to-infrastructure) accident-prevention systems, 133

V2V (vehicle-to-vehicle) accident-prevention systems, 133

V2X (vehicle-to-anything) accident-prevention systems, 133

variable transformation, 8

variational quantum eigensolver (VQE), 164

vehicles, autonomous, 15, 175

VEX (Vulnerability Exploitability eXchange), 72–73

video conferencing, 96, 97

virtual assistants, 102, 115

virtual collaboration spaces, 106–107

virtual reality. *See* AR/VR (augmented and virtual reality)

virtualization, 140–142, 148

VMs (virtual machines)

definition of, 141

migration of, 142

placement of, 145–146

voicemail, 96

voice/speech recognition, 101, 116

VQE (variational quantum eigensolver), 164

VR. *See* AR/VR (augmented and virtual reality)

vulnerabilities

cloud computing, 148–149

detection of, 132

excessive agency, 25–26

insecure plugin design, 25

management and prioritization, 71–73

model inversion and extraction, 26–27

overreliance, 26

prediction of, 60

sensitive information disclosure, 24–25

supply chain, 23–24

Vulnerability Exploitability eXchange (VEX), 72–73

## W

waste management, 134–135

water consumption meters, 126

water management, 134

Watson, 3

Web 3.0, 182–183

web meetings, 96

WebRTC (Web real-time communication), 97

Weizenbaum, Joseph, 3

wildlife conservation, 135

Word2Vec, 9, 108

workflow automation, collaboration in, 103

workload placement, cloud computing, 145–146

## X-Y-Z

X.25, 34

XAI (explainable AI), 5

Xiaoice, 3

XSS (cross-site scripting), 22

YANG (Yet Another Next Generation) models, 38–39

YouTube, 97

zombie attacks, 148