ai in identity and access management

AI in Identity and Access Management: Revolutionizing Security and Efficiency

Author: Dr. Anya Sharma, PhD, CISSP, CISM

Dr. Anya Sharma holds a PhD in Computer Science with a specialization in cybersecurity and has over 15 years of experience in the field of Identity and Access Management (IAM). She is a Certified Information Systems Security Professional (CISSP) and a Certified Information Security Manager (CISM), and currently serves as a Principal Security Architect at a leading global technology firm.

Publisher: TechTarget – Security Info

TechTarget is a leading global media company serving the technology community. Their Security Info publication is a highly respected source for news, analysis, and best practices related to cybersecurity, including a strong focus on AI and its applications in IAM.

Editor: Robert Miller, CISSP

Robert Miller is a seasoned cybersecurity editor with over 20 years of experience. His expertise lies in enterprise security architecture and emerging technologies, making him well-suited to oversee content on AI in identity and access management.

Keywords: AI in identity and access management, AI-powered IAM, artificial intelligence in IAM, machine learning in IAM, intelligent access management, automated access management, cybersecurity, identity verification, risk-based authentication, fraud detection, passwordless authentication, behavioral biometrics, IAM security, AI security

Introduction:

The digital landscape is expanding at an unprecedented rate, leading to an exponential increase in data breaches and security threats. Traditional Identity and Access Management (IAM) systems, while crucial, struggle to keep pace with this evolution. The integration of Artificial Intelligence (AI) into IAM is no longer a futuristic concept; it's a necessity for organizations seeking to secure their digital assets and enhance operational efficiency. This article explores the transformative power of AI in identity

and access management, examining its applications, benefits, challenges, and future implications.

1. AI-Driven Authentication and Authorization:

One of the most significant applications of AI in identity and access management lies in enhancing authentication and authorization processes. AI algorithms can analyze various data points – including user behavior, device characteristics, location, and time – to create a comprehensive risk profile. This allows for risk-based authentication, where users deemed low-risk might experience frictionless access, while those posing a higher risk are subjected to additional verification steps. This approach improves user experience while bolstering security. Furthermore, AI in identity and access management facilitates passwordless authentication methods, leveraging biometric data and behavioral biometrics to eliminate the vulnerabilities associated with passwords.

1. Automated User Provisioning and De-provisioning:

Manual user provisioning and de-provisioning are time-consuming and error-prone. AI in identity and access management automates these processes, significantly reducing the administrative burden. AI algorithms can identify new users based on organizational changes, automatically create accounts, and assign appropriate access rights. Similarly, upon employee departure, AI can efficiently de-provision access, minimizing the risk of unauthorized access to sensitive data. This automation is a key component of efficient and secure AI in identity and access management.

1. Enhanced Fraud Detection and Prevention:

AI algorithms excel at identifying patterns and anomalies, making them ideal for detecting fraudulent activities. In the context of AI in identity and access management, AI can analyze login attempts, transaction history, and other behavioral data to identify suspicious activities in real-time. This allows security teams to respond quickly and effectively to potential threats, preventing data breaches and financial losses. The ability of AI in identity and access management to detect sophisticated fraud attempts surpasses traditional methods.

1. Improved Risk Assessment and Management:

AI in identity and access management provides advanced risk assessment capabilities. By analyzing vast amounts of data, AI algorithms can identify potential security vulnerabilities and assess the risk associated with different users, devices, and applications. This allows organizations to proactively address potential threats and implement appropriate security measures. Furthermore, AI in identity and access management facilitates continuous monitoring and adaptive risk management, enabling organizations to respond dynamically to evolving threats.

1. Personalized Access Control:

AI in identity and access management enables the implementation of personalized access control policies. AI algorithms can learn user behavior and preferences, adapting access permissions based on individual needs and roles. This approach enhances user experience while ensuring that access is granted only to authorized individuals and resources.

1. Challenges and Considerations:

While AI in identity and access management offers numerous advantages, it's crucial to acknowledge potential challenges. Data privacy concerns are paramount. AI algorithms require access to sensitive user data, raising concerns about data breaches and misuse. Organizations must ensure compliance with relevant data protection regulations and implement robust data security measures. Another challenge is the potential for bias in AI algorithms. If not carefully designed and monitored, AI algorithms can perpetuate existing biases, leading to unfair or discriminatory outcomes. Finally, the integration of AI in identity and access management requires significant investment in infrastructure and expertise.

1. The Future of AI in Identity and Access Management:

The future of AI in identity and access management is bright. We can expect to see even more sophisticated AI-powered solutions emerge, further enhancing security and efficiency. Quantum-resistant cryptography will likely play a vital role in securing future IAM systems. The integration of AI with other

emerging technologies, such as blockchain and IoT security, will create more robust and resilient security ecosystems. Furthermore, advancements in explainable AI (XAI) will enhance transparency and accountability, addressing concerns about algorithmic bias and decision-making.

Conclusion:

AI in identity and access management is no longer a luxury but a necessity for organizations in the digital age. Its ability to automate processes, enhance security, and improve user experience makes it a transformative technology. While challenges exist, the benefits far outweigh the risks. By carefully addressing data privacy concerns, mitigating bias, and investing in the necessary infrastructure and expertise, organizations can harness the power of AI in identity and access management to create secure, efficient, and user-friendly digital environments.

FAQs:

1. What are the key benefits of using AI in IAM? Enhanced security, improved user experience, automated processes, reduced administrative burden, proactive threat detection, and cost savings.

1. What are the potential risks associated with AI in IAM? Data privacy concerns, algorithmic bias, integration challenges, and the need for skilled personnel.

1. How does AI improve authentication in IAM? Through risk-based authentication, passwordless authentication, and behavioral biometrics analysis.

1. How can AI help with fraud detection in IAM? By analyzing user behavior, identifying anomalies, and detecting suspicious activities in real-time.

1. What are some examples of AI-powered IAM solutions? There are many vendors offering AI-powered IAM solutions. Research specific solutions from companies like Microsoft, Okta, and others.

1. How does AI contribute to user provisioning and de-provisioning? By automating the creation and deletion of user accounts, reducing manual effort and errors.

1. What is the role of machine learning in AI-powered IAM? Machine learning algorithms are crucial for analyzing data, identifying patterns, and making predictions to improve security and efficiency.

1. What are the compliance considerations when implementing AI in IAM? Organizations must ensure compliance with relevant data protection regulations such as GDPR and CCPA.

1. What is the future outlook for AI in IAM? Continued advancements in AI technologies, integration with other emerging technologies, and increased focus on transparency and accountability.

Related Articles:

1. AI-Driven Risk-Based Authentication: This article delves deeper into how AI algorithms analyze user behavior and contextual data to adapt authentication methods, improving security and user experience.

1. Passwordless Authentication with AI: Explores the role of AI in enabling secure and convenient passwordless authentication methods, such as biometric authentication and behavioral biometrics.

1. AI for Enhanced Fraud Detection in IAM: Focuses on the specific application of AI in identifying and preventing fraudulent activities within IAM systems.

1. The Role of Machine Learning in User Provisioning: This article details

how machine learning algorithms automate user provisioning and de-provisioning processes, improving efficiency and reducing errors.

1. AI and Data Privacy in IAM: Addresses the crucial issue of data privacy and the challenges associated with using AI in IAM, highlighting best practices and compliance considerations.

1. Addressing Algorithmic Bias in AI-Powered IAM: This article explores the issue of potential bias in AI algorithms and proposes strategies to mitigate this risk.

1. The Future of Identity Verification with AI: Examines the evolving landscape of identity verification and the role of AI in enabling more secure and convenient methods.

1. Integrating AI into Existing IAM Infrastructure: Provides practical guidance on the steps involved in integrating AI capabilities into existing IAM systems.

1. The Economic Impact of AI in Identity and Access Management: Analyzes the cost savings and ROI associated with implementing AI in IAM.

ai in identity and access management: Practical Cloud Security Chris Dotson, 2019-03-04 With their rapidly changing architecture and API-driven automation, cloud platforms come with unique security challenges and opportunities. This hands-on book guides you through security best practices for multivendor cloud environments, whether your company plans to move legacy on-premises projects to the cloud or build a new infrastructure from the ground up. Developers, IT architects, and security professionals will learn cloud-specific techniques for securing popular cloud platforms such as Amazon Web Services, Microsoft Azure, and IBM Cloud. Chris Dotson—an IBM senior technical staff member—shows you how to establish data asset management, identity and access management, vulnerability management, network security, and incident response in your cloud environment.

ai in identity and access management: Study Guide to Identity and Access Management , 2024-10-26 Designed for professionals, students, and enthusiasts alike, our comprehensive books

empower you to stay ahead in a rapidly evolving digital world. * Expert Insights: Our books provide deep, actionable insights that bridge the gap between theory and practical application. * Up-to-Date Content: Stay current with the latest advancements, trends, and best practices in IT, Al, Cybersecurity, Business, Economics and Science. Each guide is regularly updated to reflect the newest developments and challenges. * Comprehensive Coverage: Whether you're a beginner or an advanced learner, Cybellium books cover a wide range of topics, from foundational principles to specialized knowledge, tailored to your level of expertise. Become part of a global network of learners and professionals who trust Cybellium to guide their educational journey. www.cybellium.com

ai in identity and access management: Privacy and Identity Management Michael Friedewald, Stefan Schiffner, Stephan Krenn, 2021-03-31 This book contains selected papers presented at the 15th IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2.2 International Summer School on Privacy and Identity Management, held in Maribor, Slovenia, in September 2020.* The 13 full papers included in this volume were carefully reviewed and selected from 21 submissions. Also included is a summary paper of a tutorial. As in previous years, one of the goals of the IFIP Summer School was to encourage the publication of thorough research papers by students and emerging scholars. The papers combine interdisciplinary approaches to bring together a host of perspectives, such as technical, legal, regulatory, socio-economic, social or societal, political, ethical, anthropological, philosophical, or psychological perspectives. *The summer school was held virtually.

ai in identity and access management: Identity, Institutions and Governance in an AI World Peter Bloom, 2020-01-10 The 21st century is on the verge of a possible total economic and political revolution. Technological advances in robotics, computing and digital communications have the potential to completely transform how people live and work. Even more radically, humans will soon be interacting with artificial intelligence (A.I.) as a normal and essential part of their daily existence. What is needed now more than ever is to rethink social relations to meet the challenges of this soon-to-arrive smart world. This book proposes an original theory of trans-human relations for this coming future. Drawing on insights from organisational studies, critical theory, psychology and futurism - it will chart for readers the coming changes to identity, institutions and governance in a world populated by intelligent human and non-human actors alike. It will be characterised by a fresh emphasis on infusing programming with values of social justice, protecting the rights and views of all forms of consciousness and creating the structures and practices necessary for encouraging a culture of mutual intelligent design. To do so means moving beyond our anthropocentric worldview of today and expanding our assumptions about the state of tomorrow's politics, institutions, laws and even everyday existence. Critically such a profound shift demands transcending humanist paradigms of a world created for and by humans and instead opening ourselves to a new reality where non-human intelligence and cyborgs are increasingly central.

ai in identity and access management: Software Architect’s Handbook Joseph Ingeno, 2018-08-30 A comprehensive guide to exploring software architecture concepts and implementing best practices Key Features Enhance your skills to grow your career as a software architect Design efficient software architectures using patterns and best practices Learn how software architecture relates to an organization as well as software development methodology Book Description The Software Architect’s Handbook is a comprehensive guide to help developers, architects, and senior programmers advance their career in the software architecture domain. This book takes you through all the important concepts, right from design principles to different considerations at various stages of your career in software architecture. The book begins by covering the fundamentals, benefits, and purpose of software architecture. You will discover how software architecture relates to an organization, followed by identifying its significant quality attributes. Once you have covered the basics, you will explore design patterns, best practices, and paradigms for efficient software development. The book discusses which factors you need to consider for performance and security enhancements. You will learn to write documentation for your architectures and make appropriate decisions when considering DevOps. In addition to this, you will explore how to design legacy

applications before understanding how to create software architectures that evolve as the market, business requirements, frameworks, tools, and best practices change over time. By the end of this book, you will not only have studied software architecture concepts but also built the soft skills necessary to grow in this field. What you will learn Design software architectures using patterns and best practices Explore the different considerations for designing software architecture Discover what it takes to continuously improve as a software architect Create loosely coupled systems that can support change Understand DevOps and how it affects software architecture Integrate, refactor, and re-architect legacy applications Who this book is for The Software Architect's Handbook is for you if you are a software architect, chief technical officer (CTO), or senior developer looking to gain a firm grasp of software architecture.

ai in identity and access management: *Digital Identity Management* Maryline Laurent, Samia Bouzefrane, 2015-04-02 In the past four decades, information technology has altered chains of value production, distribution, and information access at a significant rate. These changes, although they have shaken up numerous economic models, have so far not radically challenged the bases of our society.This book addresses our current progress and viewpoints on digital identity management in different fields (social networks, cloud computing, Internet of Things (IoT), with input from experts in computer science, law, economics and sociology. Within this multidisciplinary and scientific context, having crossed analysis on the digital ID issue, it describes the different technical and legal approaches to protect digital identities with a focus on authentication systems, identity federation techniques and privacy preservation solutions. The limitations of these solutions and research issues in this field are also discussed to further understand the changes that are taking place. - Offers a state of the discussions and work places on the management of digital identities in various contexts, such as social networking, cloud computing and the Internet of Things - Describes the advanced technical and legal measures to protect digital identities - Contains a strong emphasis of authentication techniques, identity federation tools and technical protection of privacy

ai in identity and access management: Keycloak - Identity and Access Management for Modern Applications Stian Thorgersen, Pedro Igor Silva, 2021-06-11 Learn to leverage the advanced capabilities of Keycloak, an open-source identity and access management solution, to enable authentication and authorization in applications Key Features Get up to speed with Keycloak, OAuth 2.0, and OpenID Connect using practical examples Configure, manage, and extend Keycloak for optimized security Leverage Keycloak features to secure different application types Book DescriptionImplementing authentication and authorization for applications can be a daunting experience, often leaving them exposed to security vulnerabilities. Keycloak is an open-source solution for identity management and access management for modern applications, which can make a world of difference if you learn how to use it. Keycloak, helping you get started with using it and securing your applications. Complete with hands-on tutorials, best practices, and self-assessment questions, this easy-to-follow guide will show you how to secure a sample application and then move on to securing different application types. As you progress, you will understand how to configure and manage Keycloak as well as how to leverage some of its more advanced capabilities. Finally, you'll gain insights into securely using Keycloak in production. By the end of this book, you will have learned how to install and manage Keycloak as well as how to secure new and existing applications.What you will learn Understand how to install, configure, and manage Keycloak Secure your new and existing applications with Keycloak Gain a basic understanding of OAuth 2.0 and OpenID Connect Understand how to configure Keycloak to make it ready for production use Discover how to leverage additional features and how to customize Keycloak to fit your needs Get to grips with securing Keycloak servers and protecting applications Who this book is for Developers, sysadmins, security engineers, or anyone who wants to leverage Keycloak and its capabilities for application security will find this book useful. Beginner-level knowledge of app development and authentication and authorization is expected.

ai in identity and access management: Digital Identity and Access Management: Technologies and Frameworks Sharman, Raj, 2011-12-31 This book explores important and

emerging advancements in digital identity and access management systems, providing innovative answers to an assortment of problems as system managers are faced with major organizational, economic and market changes--Provided by publisher.

ai in identity and access management: Mastering Identity and Access Management with Microsoft Azure Jochen Nickel, 2016-09-30 Start empowering users and protecting corporate data, while managing Identities and Access with Microsoft Azure in different environments About This Book Deep dive into the Microsoft Identity and Access Management as a Service (IDaaS) solution Design, implement and manage simple and complex hybrid identity and access management environments Learn to apply solution architectures directly to your business needs and understand how to identify and manage business drivers during transitions Who This Book Is For This book is for business decision makers, IT consultants, and system and security engineers who wish to plan, design, and implement Identity and Access Management solutions with Microsoft Azure. What You Will Learn Apply technical descriptions and solution architectures directly to your business needs and deployments Identify and manage business drivers and architecture changes to transition between different scenarios Understand and configure all relevant Identity and Access Management key features and concepts Implement simple and complex directory integration, authentication, and authorization scenarios Get to know about modern identity management, authentication, and authorization protocols and standards Implement and configure a modern information protection solution Integrate and configure future improvements in authentication and authorization functionality of Windows 10 and Windows Server 2016 In Detail Microsoft Azure and its Identity and Access Management is at the heart of Microsoft's Software as a Service, including Office 365, Dynamics CRM, and Enterprise Mobility Management. It is an essential tool to master in order to effectively work with the Microsoft Cloud. Through practical, project based learning this book will impart that mastery. Beginning with the basics of features and licenses, this book quickly moves on to the user and group lifecycle required to design roles and administrative units for role-based access control (RBAC). Learn to design Azure AD to be an identity provider and provide flexible and secure access to SaaS applications. Get to grips with how to configure and manage users, groups, roles, and administrative units to provide a user- and group-based application and self-service access including the audit functionality. Next find out how to take advantage of managing common identities with the Microsoft Identity Manager 2016 and build cloud identities with the Azure AD Connect utility. Construct blueprints with different authentication scenarios including multi-factor authentication. Discover how to configure and manage the identity synchronization and federation environment along with multi -factor authentication, conditional access, and information protection scenarios to apply the required security functionality. Finally, get recommendations for planning and implementing a future-oriented and sustainable identity and access management strategy. Style and approach A practical, project-based learning experience explained through hands-on examples.

ai in identity and access management: Privacy and Identity Management. Data for Better Living: AI and Privacy Michael Friedewald, Melek Önen, Eva Lievens, Stephan Krenn, Samuel Fricker, 2020-05-05 This book contains selected papers presented at the 14th IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2.2 International Summer School on Privacy and Identity Management, held in Windisch, Switzerland, in August 2019. The 22 full papers included in this volume were carefully reviewed and selected from 31 submissions. Also included are reviewed papers summarizing the results of workshops and tutorials that were held at the Summer School as well as papers contributed by several of the invited speakers. The papers combine interdisciplinary approaches to bring together a host of perspectives, which are reflected in the topical sections: language and privacy; law, ethics and AI; biometrics and privacy; tools supporting data protection compliance; privacy classification and security assessment; privacy enhancing technologies in specific contexts. The chapters What Does Your Gaze Reveal About You? On the Privacy Implications of Eye Tracking and Privacy Implications of Voice and Speech Analysis - Information Disclosure by Inference are open access under a CC BY 4.0 license at link.springer.com.

ai in identity and access management: Powering the Digital Economy: Opportunities

and Risks of Artificial Intelligence in Finance El Bachir Boukherouaa, Mr. Ghiath Shabsigh, Khaled AlAjmi, Jose Deodoro, Aquiles Farias, Ebru S Iskender, Mr. Alin T Mirestean, Rangachary Ravikumar, 2021-10-22 This paper discusses the impact of the rapid adoption of artificial intelligence (AI) and machine learning (ML) in the financial sector. It highlights the benefits these technologies bring in terms of financial deepening and efficiency, while raising concerns about its potential in widening the digital divide between advanced and developing economies. The paper advances the discussion on the impact of this technology by distilling and categorizing the unique risks that it could pose to the integrity and stability of the financial system, policy challenges, and potential regulatory approaches. The evolving nature of this technology and its application in finance means that the full extent of its strengths and weaknesses is yet to be fully understood. Given the risk of unexpected pitfalls, countries will need to strengthen prudential oversight.

ai in identity and access management: Identity and Access Management Ertem Osmanoglu, 2013-11-19 Identity and Access Management: Business Performance Through Connected Intelligence provides you with a practical, in-depth walkthrough of how to plan, assess, design, and deploy IAM solutions. This book breaks down IAM into manageable components to ease systemwide implementation. The hands-on, end-to-end approach includes a proven step-by-step method for deploying IAM that has been used successfully in over 200 deployments. The book also provides reusable templates and source code examples in Java, XML, and SPML. Focuses on real-word implementations Provides end-to-end coverage of IAM from business drivers, requirements, design, and development to implementation Presents a proven, step-by-step method for deploying IAM that has been successfully used in over 200 cases Includes companion website with source code examples in Java, XML, and SPML as well as reusable templates

ai in identity and access management: Access Control Systems Messaoud Benantar, 2006-06-18 This essential resource for professionals and advanced students in security programming and system design introduces the foundations of programming systems security and the theory behind access control models, and addresses emerging access control mechanisms.

ai in identity and access management: *Access Control and Identity Management* Mike Chapple, 2020-10-01 Revised and updated with the latest data from this fast paced field, Access Control, Authentication, and Public Key Infrastructure defines the components of access control, provides a business framework for implementation, and discusses legal requirements that impact access control programs.

ai in identity and access management: Research Anthology on Artificial Intelligence Applications in Security Management Association, Information Resources, 2020-11-27 As industries are rapidly being digitalized and information is being more heavily stored and transmitted online, the security of information has become a top priority in securing the use of online networks as a safe and effective platform. With the vast and diverse potential of artificial intelligence (AI) applications, it has become easier than ever to identify cyber vulnerabilities, potential threats, and the identification of solutions to these unique problems. The latest tools and technologies for AI applications have untapped potential that conventional systems and human security systems cannot meet, leading AI to be a frontrunner in the fight against malware, cyber-attacks, and various security issues. However, even with the tremendous progress AI has made within the sphere of security, it's important to understand the impacts, implications, and critical issues and challenges of AI applications along with the many benefits and emerging trends in this essential field of security-based research. Research Anthology on Artificial Intelligence Applications in Security seeks to address the fundamental advancements and technologies being used in AI applications for the security of digital data and information. The included chapters cover a wide range of topics related to AI in security stemming from the development and design of these applications, the latest tools and technologies, as well as the utilization of AI and what challenges and impacts have been discovered along the way. This resource work is a critical exploration of the latest research on security and an overview of how AI has impacted the field and will continue to advance as an essential tool for security, safety, and privacy online. This book is ideally intended for cyber security

analysts, computer engineers, IT specialists, practitioners, stakeholders, researchers, academicians, and students interested in AI applications in the realm of security research.

ai in identity and access management: *AWS Certified Identity and Access Management (IAM)* Cybellium, Welcome to the forefront of knowledge with Cybellium, your trusted partner in mastering the cutting-edge fields of IT, Artificial Intelligence, Cyber Security, Business, Economics and Science. Designed for professionals, students, and enthusiasts alike, our comprehensive books empower you to stay ahead in a rapidly evolving digital world. * Expert Insights: Our books provide deep, actionable insights that bridge the gap between theory and practical application. * Up-to-Date Content: Stay current with the latest advancements, trends, and best practices in IT, Al, Cybersecurity, Business, Economics and Science. Each guide is regularly updated to reflect the newest developments and challenges. * Comprehensive Coverage: Whether you're a beginner or an advanced learner, Cybellium books cover a wide range of topics, from foundational principles to specialized knowledge, tailored to your level of expertise. Become part of a global network of learners and professionals who trust Cybellium to guide their educational journey. www.cybellium.com

ai in identity and access management: Generative AI and Implications for Ethics, Security, and Data Management Gomathi Sankar, Jeganathan, David, Arokiaraj, 2024-08-21 As generative AI rapidly advances with the field of artificial intelligence, its presence poses significant ethical, security, and data management challenges. While this technology encourages innovation across various industries, ethical concerns regarding the potential misuse of AI-generated content for misinformation or manipulation may arise. The risks of AI-generated deepfakes and cyberattacks demand more research into effective security tactics. The supervision of datasets required to train generative AI models raises questions about privacy, consent, and responsible data management. As generative AI evolves, further research into the complex issues regarding its potential is required to safeguard ethical values and security of people’s data. Generative AI and Implications for Ethics, Security, and Data Management explores the implications of generative AI across various industries who may use the tool for improved organizational development. The security and data management benefits of generative AI are outlined, while examining the topic within the lens of ethical and social impacts. This book covers topics such as cybersecurity, digital technology, and cloud storage, and is a useful resource for computer engineers, IT professionals, technicians, sociologists, healthcare workers, researchers, scientists, and academicians.

ai in identity and access management: Mastering IAM Kris Hermans, In today's interconnected digital landscape, effective Identity and Access Management (IAM) is vital for organizations to secure their systems, protect sensitive data, and enable seamless collaboration. In Mastering IAM, acclaimed author Kris Hermans provides a comprehensive guide that demystifies the complexities of IAM, empowering readers to establish robust identity management practices and optimize access controls. With years of experience in the cybersecurity field, Hermans understands the critical role IAM plays in ensuring the confidentiality, integrity, and availability of digital resources. In this book, he shares his expertise, providing a practical roadmap for implementing and managing IAM solutions that align with business goals and industry best practices. Inside Mastering IAM, you will: 1. Explore the IAM landscape: Gain a deep understanding of the core concepts, components, and frameworks that form the foundation of IAM. From authentication and authorization to identity governance and federation, master the essential building blocks of a successful IAM strategy. 2. Design and implement IAM solutions: Learn how to design an IAM architecture tailored to your organization's needs, considering factors such as scalability, compliance, and user experience. Follow step-by-step guidelines for deploying IAM solutions, including user provisioning, access controls, single sign-on (SSO), and multi-factor authentication (MFA). 3. Enhance security and compliance: Discover strategies for mitigating security risks and ensuring compliance with relevant regulations. Explore identity lifecycle management, privileged access management (PAM), and security incident response to safeguard against threats and unauthorized access. 4. Leverage IAM for business efficiency: Uncover how IAM can streamline

business processes, improve productivity, and enhance user experiences. Explore topics such as self-service portals, role-based access control (RBAC), and integration with other systems to optimize IAM functionality. 5. Address emerging challenges: Stay up to date with the latest trends and emerging technologies shaping the IAM landscape. Learn about cloud-based IAM solutions, IoT device management, and the impact of artificial intelligence and machine learning in enhancing IAM capabilities. With real-world examples, practical tips, and insightful case studies, Mastering IAM equips readers with the knowledge and skills needed to effectively implement and manage IAM solutions. Whether you are an IAM professional, IT manager, or security practitioner, this book will guide you toward harnessing the full potential of IAM to protect your organization's assets and drive business success. Don't let identity and access management be a barrier to productivity and security. Unleash the power of IAM with Kris Hermans as your trusted guide.

ai in identity and access management: Cloud Security and Privacy Tim Mather, Subra Kumaraswamy, Shahed Latif, 2009-09-04 You may regard cloud computing as an ideal way for your company to control IT costs, but do you know how private and secure this service really is? Not many people do. With Cloud Security and Privacy, you'll learn what's at stake when you trust your data to the cloud, and what you can do to keep your virtual infrastructure and web applications secure. Ideal for IT staffers, information security and privacy practitioners, business managers, service providers, and investors alike, this book offers you sound advice from three well-known authorities in the tech security world. You'll learn detailed information on cloud computing security that-until now-has been sorely lacking. Review the current state of data security and storage in the cloud, including confidentiality, integrity, and availability Learn about the identity and access management (IAM) practice for authentication, authorization, and auditing of the users accessing cloud services Discover which security management frameworks and standards are relevant for the cloud Understand the privacy aspects you need to consider in the cloud, including how they compare with traditional computing models Learn the importance of audit and compliance functions within the cloud, and the various standards and frameworks to consider Examine security delivered as a service-a different facet of cloud security

ai in identity and access management: Solving Identity and Access Management in Modern Applications Yvonne Wilson, Abhishek Hingnikar, 2020-03-02 Know how to design and use identity management to protect your application and the data it manages. At a time when security breaches result in increasingly onerous penalties, it is paramount that application developers and owners understand identity management and the value it provides when building applications. This book takes you from account provisioning to authentication to authorization, and covers troubleshooting and common problems to avoid. The authors include predictions about why this will be even more important in the future. Application best practices with coding samples are provided. Solving Identity and Access Management in Modern Applications gives you what you need to design identity and access management for your applications and to describe it to stakeholders with confidence. You will be able to explain account creation, session and access management, account termination, and more. What You'll Learn Understand key identity management concepts Incorporate essential design principles Design authentication and access control for a modern application Know the identity management frameworks and protocols used today (OIDC/ OAuth 2.0, SAML 2.0) Review historical failures and know how to avoid them Who This Book Is For Developers, enterprise or application architects, business application or product owners, and anyone involved in an application's identity management solution

ai in identity and access management: Integrating Artificial Intelligence and Machine Learning with Blockchain Security D. Jeya Mala, R. Ganesan, 2023-09-13 Due to its transparency and dependability in secure online transactions, blockchain technology has grown in prominence in recent years. Several industries, including those of finance, healthcare, energy and utilities, manufacturing, retail marketing, entertainment and media, supply chains, e-commerce, and e-business, among others, use blockchain technology. In order to enable intelligent decision-making to prevent security assaults, particularly in permission-less blockchain platforms, artificial

intelligence (AI) techniques and machine learning (ML) algorithms are used. By exploring the numerous use cases and security methods used in each of them, this book offers insight on the application of AI and ML in blockchain security principles. The book argues that it is crucial to include artificial intelligence and machine learning techniques in blockchain technology in order to increase security.

ai in identity and access management: Digital Twin and Blockchain for Smart Cities Amit Kumar Tyagi, 2024-09-11 The book uniquely explores the fundamentals of blockchain and digital twin technologies and their uses in smart cities. In the previous decade, many governments explored artificial intelligence, digital twin, and blockchain, and their roles in smart cities. This book discusses the convergence of two transformative technologies, digital twin and blockchain, to address urban challenges and propel the development of smarter, more sustainable cities. This convergence empowers cities to create real-time replicas of urban environments (digital twins) and secure, transparent data management (blockchain) to improve city planning, management, and civic services. In this application, the concept of a digital twin involves creating a virtual, data-driven replica of a city or specific urban systems, such as transportation, energy, or infrastructure. This digital twin mirrors the real world, gathering data from various sensors, IoT devices, and other sources to provide a holistic view of the city's operations. Furthermore, blockchain technology offers a decentralized and tamper-resistant ledger for securely storing and managing data. In the context of smart cities, blockchain can ensure data integrity, privacy, and transparency, enabling trust and collaboration among various stakeholders. This book covers many important topics, including real-time city modeling; data security and the trustworthy storage of sensitive urban data; transparent governance to facilitate accountable governance and decision-making processes in smart cities; improved city services; disaster resilience (by providing insights into vulnerabilities and efficient resource allocation during crises); sustainable urban planning that optimizes resource allocation, reduces energy consumption, and minimizes environmental impact, which fosters sustainable development; citizen engagement; and much more. This book will not only provide information about more efficient, resilient, and sustainable urban environments, but it also empowers citizens to be active participants in shaping the future of their cities. By converging these technologies, cities can overcome existing challenges, encourage innovation, and create more livable, connected, and responsive urban spaces. Audience This book has a wide audience in computer science, artificial intelligence, and information technology as well as engineers in a variety of industrial manufacturing industries. It will also appeal to economists and government/city policymakers working on smart cities, the circular economy, clean tech investors, urban decision-makers, and environmental professionals.

ai in identity and access management: Artificial Intelligence and Machine Learning for Business for Non-Engineers Stephan S. Jones, Frank M. Groom, 2019-11-22 The next big area within the information and communication technology field is Artificial Intelligence (AI). The industry is moving to automate networks, cloud-based systems (e.g., Salesforce), databases (e.g., Oracle), AWS machine learning (e.g., Amazon Lex), and creating infrastructure that has the ability to adapt in real-time to changes and learn what to anticipate in the future. It is an area of technology that is coming faster and penetrating more areas of business than any other in our history. AI will be used from the C-suite to the distribution warehouse floor. Replete with case studies, this book provides a working knowledge of AI's current and future capabilities and the impact it will have on every business. It covers everything from healthcare to warehousing, banking, finance and education. It is essential reading for anyone involved in industry.

ai in identity and access management: The Evolution of Telecommunications Ron Legarski, 2024-08-29 The Evolution of Telecommunications: From Analog to Digital and Beyond is an in-depth exploration of the telecommunications industry, tracing its history from the earliest forms of communication to the cutting-edge technologies that define the modern era. Written by Ron Legarski, a seasoned expert with over two decades of experience in the field, this book offers a comprehensive analysis of the technological advancements, industry shifts, and global events that

have shaped telecommunications over the years. The book delves into the transformation from analog to digital communication, the rise of the internet, and the ongoing development of 5G and beyond. It covers critical topics such as the impact of AI, IoT, and edge computing on telecommunications, the role of quantum communication in securing networks, and the challenges posed by global events like the COVID-19 pandemic. In addition to historical context, The Evolution of Telecommunications provides detailed case studies of major companies and innovations, examining how industry leaders like AT&T, Verizon, and Nokia have navigated the changing landscape. It also explores the societal implications of telecommunications, including its role in driving economic growth, improving quality of life, and addressing global challenges like climate change and digital inclusion. With detailed appendices that include a glossary of key terms, a timeline of significant developments, and additional resources for further study, this book serves as both a comprehensive guide and a valuable reference for professionals, students, and anyone interested in the future of telecommunications. Whether you're a telecommunications professional, a technology enthusiast, or simply curious about how the world stays connected, The Evolution of Telecommunications offers a thorough understanding of the forces that continue to shape our increasingly digital world.

ai in identity and access management: Impact of Al on Cybersecurity Mohan Kumar Gajula, 2024-09-27 Impact of AI on Cybersecurity explores how artificial intelligence reshapes the landscape of cybersecurity. The innovative role AI plays in threat detection, data protection, and real-time response strategies while examining the ethical and security challenges it introduces. Ideal for cybersecurity professionals, technology enthusiasts, and AI researchers, the book offers insights into AI-powered defense mechanisms, advanced threat analytics, and the future implications of AI in safeguarding digital infrastructures. Through real-world examples and expert perspectives, it presents a comprehensive guide to the transformative intersection of AI and cybersecurity.

ai in identity and access management: Artificial Intelligence for Cybersecurity Bojan Kolosnjaji, Huang Xiao, Peng Xu, Apostolis Zarras, 2024-10-31 Gain well-rounded knowledge of AI methods in cybersecurity and obtain hands-on experience in implementing them to bring value to your organization Key Features Familiarize yourself with AI methods and approaches and see how they fit into cybersecurity Learn how to design solutions in cybersecurity that include AI as a key feature Acquire practical AI skills using step-by-step exercises and code examples Purchase of the print or Kindle book includes a free PDF eBook Book DescriptionArtificial intelligence offers data analytics methods that enable us to efficiently recognize patterns in large-scale data. These methods can be applied to various cybersecurity problems, from authentication and the detection of various types of cyberattacks in computer networks to the analysis of malicious executables. Written by a machine learning expert, this book introduces you to the data analytics environment in cybersecurity and shows you where AI methods will fit in your cybersecurity projects. The chapters share an in-depth explanation of the AI methods along with tools that can be used to apply these methods, as well as design and implement AI solutions. You'll also examine various cybersecurity scenarios where AI methods are applicable, including exercises and code examples that'll help you effectively apply AI to work on cybersecurity challenges. The book also discusses common pitfalls from real-world applications of AI in cybersecurity issues and teaches you how to tackle them. By the end of this book, you'll be able to not only recognize where AI methods can be applied, but also design and execute efficient solutions using AI methods.What you will learn Recognize AI as a powerful tool for intelligence analysis of cybersecurity data Explore all the components and workflow of an AI solution Find out how to design an AI-based solution for cybersecurity Discover how to test various AI-based cybersecurity solutions Evaluate your AI solution and describe its advantages to your organization Avoid common pitfalls and difficulties when implementing AI solutions Who this book is for This book is for machine learning practitioners looking to apply their skills to overcome cybersecurity challenges. Cybersecurity workers who want to leverage machine learning methods will also find this book helpful. Fundamental concepts of machine learning and beginner-level knowledge of Python programming are needed to understand the concepts present in this book.

Whether you're a student or an experienced professional, this book offers a unique and valuable learning experience that will enable you to protect your network and data against the ever-evolving threat landscape.

ai in identity and access management: *Artificial Intelligence-Enabled Digital Twin for Smart Manufacturing* Amit Kumar Tyagi, Shrikant Tiwari, Senthil Kumar Arumugam, Avinash Kumar Sharma, 2024-09-11 An essential book on the applications of AI and digital twin technology in the smart manufacturing sector. In the rapidly evolving landscape of modern manufacturing, the integration of cutting-edge technologies has become imperative for businesses to remain competitive and adaptive. Among these technologies, Artificial Intelligence (AI) stands out as a transformative force, revolutionizing traditional manufacturing processes and making the way for the era of smart manufacturing. At the heart of this technological revolution lies the concept of the Digital Twin—an innovative approach that bridges the physical and digital realms of manufacturing. By creating a virtual representation of physical assets, processes, and systems, organizations can gain unprecedented insights, optimize operations, and enhance decision-making capabilities. This timely book explores the convergence of AI and Digital Twin technologies to empower smart manufacturing initiatives. Through a comprehensive examination of principles, methodologies, and practical applications, it explains the transformative potential of AI-enabled Digital Twins across various facets of the manufacturing lifecycle. From design and prototyping to production and maintenance, AI-enabled Digital Twins offer multifaceted advantages that redefine traditional paradigms. By leveraging AI algorithms for data analysis, predictive modeling, and autonomous optimization, manufacturers can achieve unparalleled levels of efficiency, quality, and agility. This book explains how AI enhances the capabilities of Digital Twins by creating a powerful tool that can optimize production processes, improve product quality, and streamline operations. Note that the Digital Twin in this context is a virtual representation of a physical manufacturing system, including machines, processes, and products. It continuously collects real-time data from sensors and other sources, allowing it to mirror the physical system's behavior and performance. What sets this Digital Twin apart is the incorporation of AI algorithms and machine learning techniques that enable it to analyze and predict outcomes, recommend improvements, and autonomously make adjustments to enhance manufacturing efficiency. This book outlines essential elements, like real-time monitoring of machines, predictive analytics of machines and data, optimization of the resources, quality control of the product, resource management, decision support (timely or quickly accurate decisions). Moreover, this book elucidates the symbiotic relationship between AI and Digital Twins, highlighting how AI augments the capabilities of Digital Twins by infusing them with intelligence, adaptability, and autonomy. Hence, this book promises to enhance competitiveness, reduce operational costs, and facilitate innovation in the manufacturing industry. By harnessing AI's capabilities in conjunction with Digital Twins, manufacturers can achieve a more agile and responsive production environment, ultimately driving the evolution of smart factories and Industry 4.0/5.0. Audience This book has a wide audience in computer science, artificial intelligence, and manufacturing engineering, as well as engineers in a variety of industrial manufacturing industries. It will also appeal to economists and policymakers working on the circular economy, clean tech investors, industrial decision-makers, and environmental professionals.

ai in identity and access management: AI and Blockchain Applications in Industrial Robotics Biradar, Rajashekhar C., D., Geetha, Tabassum, Nikhath, Hegde, Nayana, Lazarescu, Mihai, 2023-12-29 The ever-evolving industrial landscape poses challenges for businesses, particularly in robotics, where performance optimization and data security are paramount. AI and Blockchain Applications in Industrial Robotics, edited by esteemed scholars Mihai Lazarescu, Rajashekhar Biradar, Geetha Devanagavi, Nikhath Tabassum, and Nayana Hegde, presents the transformative potential of combining AI and blockchain technologies to revolutionize the field. This exceptional book provides comprehensive insights into how AI enhances predictive models and pattern recognition, while blockchain ensures secure and immutable data transactions. By synergizing these technologies, businesses can achieve enhanced transparency, trust, and efficiency

in their robotic processes. With practical applications, use cases, and real-world examples, the book caters to a wide range of readers, empowering them to embrace the possibilities of AI and blockchain in industrial robotics. AI and Blockchain Applications in Industrial Robotics equip industries with the tools and understanding to overcome challenges in optimizing performance, ensuring data security, and harnessing emerging technologies. Serving as a beacon of knowledge, this book drives innovation, efficiency, and competitiveness in the industrial sector. Whether for postgraduate students, researchers, industry professionals, undergraduate students, or freelance developers, the book provides valuable insights and practical guidance for implementing AI and blockchain solutions. By embracing the transformative potential of these technologies, industries can unlock new possibilities and propel themselves forward in the ever-advancing world of industrial robotics.

ai in identity and access management: Artificial Intelligence in Forensic Science Kavita Saini, Swaroop S. Sonone, Mahipal Singh Sankhla, Naveen Kumar, 2024-08-26 Artificial Intelligence in Forensic Science addresses the current and emerging opportunities being utilized to apply modern Artificial Intelligence (AI) technologies to current forensic and investigation practices. The book also showcases the increasing benefits of AI where and when it can be applied to various techniques and forensic disciplines. The increasing rate of sophisticated crimes has increased the opportunity and need for the forensic field to explore a variety of emerging technologies to counter criminals—and AI is no exception. There are many current investigative challenges that, with ingenuity and application, can be helped with the application of AI, especially in the digital forensic and cyber-crime arena. The book also explains many practical studies that have been carried out to test AI technologies in crime detection, uncovering evidence, and identifying perpetrators. In the last decade, the use of AI has become common in many fields and now is an ideal time to look at the various ways AI can be integrated into judicial, forensic, and criminal cases to better collect and analyze evidence, thereby improving outcomes.

ai in identity and access management: Artificial Intelligence: A Guide for Everyone Arshad Khan,

ai in identity and access management: Artificial Intelligence and Cyber Security in Industry 4.0 Velliangiri Sarveshwaran, Joy Iong-Zong Chen, Danilo Pelusi, 2023-07-15 This book provides theoretical background and state-of-the-art findings in artificial intelligence and cybersecurity for industry 4.0 and helps in implementing AI-based cybersecurity applications. Machine learning-based security approaches are vulnerable to poison datasets which can be caused by a legitimate defender's misclassification or attackers aiming to evade detection by contaminating the training data set. There also exist gaps between the test environment and the real world. Therefore, it is critical to check the potentials and limitations of AI-based security technologies in terms of metrics such as security, performance, cost, time, and consider how to incorporate them into the real world by addressing the gaps appropriately. This book focuses on state-of-the-art findings from both academia and industry in big data security relevant sciences, technologies, and applications.

ai in identity and access management: Artificial Intelligence in Cyber Security Advanced Threat Detection and Prevention Strategies Rajesh David, 2024-11-05 Artificial Intelligence in Cyber Security Advanced Threat Detection and Prevention Strategies the transformative role of AI in strengthening cybersecurity defenses. This a comprehensive guide to how AI-driven technologies can identify, analyze, and mitigate sophisticated cyber threats in real time. Covering advanced techniques in machine learning, anomaly detection, and behavioral analysis, it offers strategic insights for proactively defending against cyber attacks. Ideal for cybersecurity professionals, IT managers, and researchers, this book illuminates AI's potential to anticipate vulnerabilities and safeguard digital ecosystems against evolving threats.

ai in identity and access management: *Methodology to Improve Control Plane Security in SDN Environments* Wendwossen Desalegn, Javed Shaikh, Bayisa Taye, 2024-08-26 This book unveils a blueprint for safeguarding the very backbone of modern communication networks. It offers a

roadmap towards fortifying SDN infrastructures against the relentless onslaught of cyber threats, ensuring resilience and reliability in an ever-evolving digital landscape. This is an exhaustive study of crafting a robust security solution tailored for the SDN environment, specifically targeting the detection and mitigation of distributed denial of service (DDoS) attacks on the control plane. The methodology hinges on an early detection strategy, meticulously aligned with industry standards, serving as a beacon for professionals navigating the intricate realm of implementing security solutions. This reference elucidates an innovative approach devised to identify and mitigate the inherent risks associated with the OpenFlow protocol and its POX controller. Validated through rigorous simulations conducted within controlled environments utilizing the Mininet tool and SDN controller, the methodology unfolds, showcasing the intricate dance between theory and practice. Through meticulous observation of detection algorithm results in simulated environments, followed by real-world implementation within network testbeds, the proposed solution emerges triumphant. Leveraging network entropy calculation, coupled with swift port blocking mechanisms, the methodology stands as a formidable barrier against a DDoS attack such as TCP, UDP, and ICMP floods.

ai in identity and access management: African Artificial Intelligence Mark Nasila, 2024-05-27 Artificial intelligence (AI) is upending life, work, and play as we know it, and it's only just getting started. The rise of AI is a milestone on par with the discovery of fire, the invention of the wheel, and the creation of the internet. In short, AI is going to change everything. For some, that's an exciting prospect. For others, it's terrifying. However you feel about AI, there's no escaping it, whether you're in a global metropolis or a farmer in rural KwaZulu-Natal. Dr Mark Nasila has been watching AI's ascent for over a decade, studying its effects on everything from agriculture and aviation to healthcare, education, entertainment, crime prevention, energy management, policy creation, finance, and anything in between, and applying them to his role at one of South Africa's most successful financial institutions, First National Bank, a division of FirstRand Group. African Artificial Intelligence is a comprehensive and fascinating journey, tracing the rise of AI and its evolution into the emerging technology underpinning all others – from connected devices and smart chatbots to the metaverse. Mark combines unexpected use cases and tales of cutting-edge innovation with a unique and potent argument: harnessing AI to solve Africa's problems requires embracing it from an African perspective. African nations can't afford to simply import AI solutions from afar. Instead, Mark contends, they need to rework, remix, and refine AI so it's able to meet uniquely African challenges in uniquely African ways, and to take advantage of the once-in-a-generation opportunity AI represents for every industry, sector, and person, everywhere.

ai in identity and access management: Microsoft Identity and Access Administrator Exam Guide Dwayne Natwick, Shannon Kuehn, 2022-03-10 This certification guide focuses on identity solutions and strategies that will help you prepare for Microsoft Identity and Access Administrator certification, while enabling you to implement what you've learned in real-world scenarios Key FeaturesDesign, implement, and operate identity and access management systems using Azure ADProvide secure authentication and authorization access to enterprise applicationsImplement access and authentication for cloud-only and hybrid infrastructuresBook Description Cloud technologies have made identity and access the new control plane for securing data. Without proper planning and discipline in deploying, monitoring, and managing identity and access for users, administrators, and guests, you may be compromising your infrastructure and data. This book is a preparation guide that covers all the objectives of the SC-300 exam, while teaching you about the identity and access services that are available from Microsoft and preparing you for real-world challenges. The book starts with an overview of the SC-300 exam and helps you understand identity and access management. As you progress to the implementation of IAM solutions, you'll learn to deploy secure identity and access within Microsoft 365 and Azure Active Directory. The book will take you from legacy on-premises identity solutions to modern and password-less authentication solutions that provide high-level security for identity and access. You'll focus on implementing access and authentication for cloud-only and hybrid infrastructures as well as

understand how to protect them using the principles of zero trust. The book also features mock tests toward the end to help you prepare effectively for the exam. By the end of this book, you'll have learned how to plan, deploy, and manage identity and access solutions for Microsoft and hybrid infrastructures. What you will learnUnderstand core exam objectives to pass the SC-300 examImplement an identity management solution with MS Azure ADManage identity with multi-factor authentication (MFA), conditional access, and identity protectionDesign, implement, and monitor the integration of enterprise apps for Single Sign-On (SSO)Add apps to your identity and access solution with app registrationDesign and implement identity governance for your identity solutionWho this book is for This book is for cloud security engineers, Microsoft 365 administrators, Microsoft 365 users, Microsoft 365 identity administrators, and anyone who wants to learn identity and access management and gain SC-300 certification. You should have a basic understanding of the fundamental services within Microsoft 365 and Azure Active Directory before getting started with this Microsoft book.

ai in identity and access management: Cybersecurity and Artificial Intelligence Hamid Jahankhani,

ai in identity and access management: Emerging Technologies and Security in Cloud Computing Lakshmi, D., Tyagi, Amit Kumar, 2024-02-14 In today's digital age, the exponential growth of cloud computing services has brought significant opportunities for businesses and individuals alike. However, this surge in cloud adoption has also ushered in a host of critical concerns, with the paramount issues being data privacy and security. The goal of protecting sensitive information from cyber threats and ensuring confidentiality has become increasingly challenging for organizations across industries. Emerging Technologies and Security in Cloud Computing is a comprehensive guide designed to tackle these pressing concerns head-on. This authoritative book provides a robust framework for understanding and addressing the multifaceted issues surrounding data privacy and security in the cloud. It serves as a beacon of knowledge for academic scholars, researchers, and IT professionals seeking practical solutions to safeguard sensitive data.

ai in identity and access management: Computer and Information Security Handbook John R. Vacca, 2012-11-05 The second edition of this comprehensive handbook of computer and information security provides the most complete view of computer security and privacy available. It offers in-depth coverage of security theory, technology, and practice as they relate to established technologies as well as recent advances. It explores practical solutions to many security issues. Individual chapters are authored by leading experts in the field and address the immediate and long-term challenges in the authors' respective areas of expertise. The book is organized into 10 parts comprised of 70 contributed chapters by leading experts in the areas of networking and systems security, information management, cyber warfare and security, encryption technology, privacy, data storage, physical security, and a host of advanced security topics. New to this edition are chapters on intrusion detection, securing the cloud, securing web apps, ethical hacking, cyber forensics, physical security, disaster recovery, cyber attack deterrence, and more. - Chapters by leaders in the field on theory and practice of computer and information security technology, allowing the reader to develop a new level of technical expertise - Comprehensive and up-to-date coverage of security issues allows the reader to remain current and fully informed from multiple viewpoints - Presents methods of analysis and problem-solving techniques, enhancing the reader's grasp of the material and ability to implement practical solutions

ai in identity and access management: *AI and Humanity* Illah Reza Nourbakhsh, Jennifer Keating, 2020-03-10 An examination of the implications for society of rapidly advancing artificial intelligence systems, combining a humanities perspective with technical analysis; includes exercises and discussion questions. AI and Humanity provides an analytical framing and a common language for understanding the effects of technological advances in artificial intelligence on society. Coauthored by a computer scientist and a scholar of literature and cultural studies, it is unique in combining a humanities perspective with technical analysis, using the tools of literary explication to

examine the societal impact of AI systems. It explores the historical development of these technologies, moving from the apparently benign Roomba to the considerably more sinister semi-autonomous weapon system Harpy. The book is driven by an exploration of the cultural and etymological roots of a series of keywords relevant to both AI and society. Works examined range from Narrative of the Life of Frederick Douglass, given a close reading for its themes of literacy and agency, to Simon Head's critique of the effects of surveillance and automation on the Amazon labor force in Mindless. Originally developed as a textbook for an interdisciplinary humanities-science course at Carnegie Mellon, AI & Humanity offers discussion questions, exercises (including journal writing and concept mapping), and reading lists. A companion website provides updated resources and a portal to a video archive of interviews with AI scientists, sociologists, literary theorists, and others.

ai in identity and access management: Hands-On Artificial Intelligence on Amazon Web Services Subhashini Tripuraneni, Charles Song, 2019-10-04 Perform cloud-based machine learning and deep learning using Amazon Web Services such as SageMaker, Lex, Comprehend, Translate, and Polly Key FeaturesExplore popular machine learning and deep learning services with their underlying algorithmsDiscover readily available artificial intelligence(AI) APIs on AWS like Vision and Language ServicesDesign robust architectures to enable experimentation, extensibility, and maintainability of AI appsBook Description From data wrangling through to translating text, you can accomplish this and more with the artificial intelligence and machine learning services available on AWS. With this book, you'll work through hands-on exercises and learn to use these services to solve real-world problems. You'll even design, develop, monitor, and maintain machine and deep learning models on AWS. The book starts with an introduction to AI and its applications in different industries, along with an overview of AWS artificial intelligence and machine learning services. You'll then get to grips with detecting and translating text with Amazon Rekognition and Amazon Translate. The book will assist you in performing speech-to-text with Amazon Transcribe and Amazon Polly. Later, you'll discover the use of Amazon Comprehend for extracting information from text, and Amazon Lex for building voice chatbots. You will also understand the key capabilities of Amazon SageMaker such as wrangling big data, discovering topics in text collections, and classifying images. Finally, you'll cover sales forecasting with deep learning and autoregression, before exploring the importance of a feedback loop in machine learning. By the end of this book, you will have the skills you need to implement AI in AWS through hands-on exercises that cover all aspects of the ML model life cycle. What you will learnGain useful insights into different machine and deep learning modelsBuild and deploy robust deep learning systems to productionTrain machine and deep learning models with diverse infrastructure specificationsScale AI apps without dealing with the complexity of managing the underlying infrastructureMonitor and Manage AI experiments efficientlyCreate AI apps using AWS pre-trained AI servicesWho this book is for This book is for data scientists, machine learning developers, deep learning researchers, and artificial intelligence enthusiasts who want to harness the power of AWS to implement powerful artificial intelligence solutions. A basic understanding of machine learning concepts is expected.

Additional Resources

AI In Identity And Access Management: Current Practices
What are the most prevalent approaches for incorporating AI in identity and access management (IAM) systems? What obstacles must be addressed in identity and access management (IAM) …

AI-driven identity and access management (IAM): The future of …
Identity and Access Management (IAM) provides improved security to organizations while improving user experiences to become a critical security

foundation of modern protection strategies. The …

AI-DRIVEN IDENTITY AND ACCESS MANAGEMENT: …
Core components, including behavioral analytics, adaptive authentication, automated access control, and intelligent threat detection, are analyzed in depth, with particular attention to their …

A Novel Zero-Trust Identity Framework for Agentic AI: …
We then propose a comprehensive frame- work built upon rich, verifiable Agent Identities (IDs), leveraging Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs), that encapsulate an …

EIC 2025 AIdentity The Intersection of AI & Identity
How do we control access to (and change/manipulation of) data that is used by AI? How do we control access to the LLMs (again: manipulation!)? How do we handle access control models for …

A literature review on the tools for Identity Access Management …
We have found a clear positive correlation between better IAM methods and decreased security risk, enhanced productivity, greater privileged activity control, and reduced financial losses, …

Enhanced Identity and Access Management with Artificial …
The article aims to impart an overview of integrating artificial intelligence (AI) with identity and access management (IAM) systems and their strategic view regarding evolution, benefits, and …

AI-Driven Identity and Access Management: Enhancing …
The integration of artificial intelligence (AI) into identity and access management (IAM) systems has garnered significant attention in recent years as organizations increasingly...

SS urnal rtiial nelligene Clu muing
With an eye towards AI’s potential uses in identity and access management - more especially in the areas of privilege monitoring, administration, and control - this research investigates the nature …

Exploring AI’s Influence on Identity and Access Management: …
Abstract: This paper explores the empirical impact of Artificial Intelligence (AI) on Identity and Access Management (IAM), with a focus on how AI and Machine Learning (ML) are …

WELCOME TO AI & ML in Identity and Access Management
Adaptive Access Adaptive access uses ML algorithms to monitor and analyze user behavior, triggering access blocking if abnormal behavior is detected.

Leveraging AI for enhanced identity and access management in …
Artificial Intelligence (AI) has emerged as a transformative tool with the potential to redefine security and IAM in the cloud. By integrating AI into IAM systems, organizations can enhance …

The Impact of AI on Identity and Access Management: An
Identity and Access Management. Artificial Intelligence (AI) and Machine Language (ML) are having a significant effect on the security sector [1]. Developers of identity access management …

A literature review on the application of AI to Identity Access …
how artificial intelligence is being used in identity and access management, as well as the challenges that have been encountered and the industry's future.

Enhanced Identity and Access Management with Artificial
The article aims to impart an overview of integrating artificial intelligence (AI) with identity and access management (IAM) systems and their strategic view regarding evolution,...

How AI can Improve Identity Verification and Access Control …
looks for the potential for advancement in AI systems with respect to IAM, focusing on identity verification and access control within IAM systems. IAM systems face really difficult problems …

Machine Identity Security in Cloud & AI: Ensuring Lifecycle …
Abstract - Machine Identity Security is critical to protecting modern digital ecosystems. The expansion of Cloud and AI technologies across organizations has dramatically expanded the …

Preventing Data Breaches in Healthcare: The Impact of AI-Driven
future implications of these technologies, this study seeks to provide insights into how AI can revolutionize identity access management and enhance overall cybersecurity in the healthcare...

AI, Machine learning and Privileged Access Management
Privileged Access Management (PAM) solutions are critical cybersecurity controls that address the security risks associated with the use of privileged access in organizations and companies. …

Identity Management Capability Powered by Artificial …
This paper provides a review of how AI powers identity management to allow easy user access privileges. Artificial Intelligence (AI) reshapes enterprises and organizes innovation...

AI In Identity And Access Management: Current Pra…
What are the most prevalent approaches for incorporating AI in identity and access management (IAM) systems? What obstacles must be …

AI-driven identity and access management (IAM)…
Identity and Access Management (IAM) provides improved security to organizations while improving user experiences to become a critical …

AI-DRIVEN IDENTITY AND ACCESS MANAGEMENT: RE…
Core components, including behavioral analytics, adaptive authentication, automated access control, and intelligent threat detection, are …

A Novel Zero-Trust Identity Framework for Agentic AI: …
We then propose a comprehensive frame- work built upon rich, verifiable Agent Identities (IDs), leveraging Decentralized Identifiers (DIDs) and …

EIC 2025 AIdentity The Intersection of AI & Identity
How do we control access to (and change/manipulation of) data that is used by AI? How do we control access to the LLMs (again: manipulation!)? …

Ai In Identity And Access Management

Ai In Identity And Access Management

Related Articles

- ai driven marketing automation
- ai in fleet management
- air brake practice test cdl

Back to Home