Telemetry And Anomaly Detection Identifying And

This book presents the characteristics and benefits industrial organizations can reap from the Industrial Internet of Things (IIoT). These characteristics and benefits include enhanced competitiveness, increased proactive decision-making, improved creativity and innovation, augmented job creation, heightened agility to respond to continuously changing challenges, and intensified data-driven decision making. In a straightforward fashion, the book also helps readers understand complex concepts that are core to IIoT enterprises, such as Big Data, analytic architecture platforms, machine learning (ML) and data science algorithms, and the power of visualization to enrich the domains experts' decision making. The book also guides the reader on how to think about ways to define new business paradigms that the IIoT facilitates, as well how to increase the probability of success in managing analytic projects that are the core engine of decision-making in the IIoT enterprise. The book starts by defining an IIoT enterprise and the framework used to efficiently operate. A description of the concepts of industrial analytics, which is a major engine for decision making in the IIoT enterprise, is provided. It then discusses how data and machine learning (ML) play an important role in increasing the competitiveness of industrial enterprises that operate using the IIoT technology and business concepts. Real world examples of data driven IIoT enterprises and various business models are presented and a discussion on how the use of ML and data science help address complex decision-making problems and generate new job opportunities. The book presents in an easy-to-understand manner how ML algorithms work and operate on data generated in the IIoT enterprise. Useful for any industry professional interested in advanced industrial software applications, including business managers and professionals interested in how data analytics can help industries and to develop innovative business solutions, as well as data and computer scientists who wish to bridge the analytics and computer science fields with the industrial world, and project managers interested in managing advanced analytic projects.

Lists citations with abstracts for aerospace related reports obtained from world wide sources and announces documents that have recently been entered into the NASA Scientific and Technical Information Database.

This proceedings book presents selected papers from the 5th Conference on Signal and Information Processing, Networking and Computers (ICSINC), held in Yuzhou, China, from November 29 to December 1, 2018. It focuses on the current research in a wide range of areas in the fields of information theory, communication systems, computer science, signal processing, aerospace technologies, and other related technologies. With contributions from experts from both academia and industry, it is a valuable resource for anyone who is interested in this field.

System Health Management: with Aerospace Applications provides the first complete reference text for System Health Management (SHM), the set of technologies and processes used to improve system dependability. Edited by a team of engineers and consultants with SHM design, development, and research experience from NASA, industry, and academia, each heading up sections in their own areas of expertise and co-coordinating contributions from leading experts, the book collates together in one text the state-of-the-art in SHM research, technology, and applications. It has been written primarily as a reference text for practitioners, for those in related disciplines, and for graduate students in aerospace or systems engineering. There are many technologies involved in SHM and no single person can be an expert in all aspects of the discipline.System Health Management: with Aerospace Applications provides an introduction to the major technologies, issues, and references in these disparate but related SHM areas. Since SHM has evolved most rapidly in aerospace, the various applications described in this book are taken primarily from the aerospace industry. However, the theories, techniques, and technologies discussed are applicable to many engineering disciplines and application areas. Readers will find sections on the basic theories and concepts of SHM, how it is applied in the system life cycle (architecture, design, verification and validation, etc.), the most important methods used (reliability, quality assurance, diagnostics, prognostics, etc.), and how SHM is applied in operations (commercial aircraft, launch operations, logistics, etc.), to subsystems (electrical power, structures, flight controls, etc.) and to system applications (robotic spacecraft, tactical missiles, rotorcraft, etc.).

The 5-volume proceedings, LNAI 12457 until 12461 constitutes the refereed proceedings of the European Conference on Machine Learning and Knowledge Discovery in Databases, ECML PKDD 2020, which was held during September 14-18, 2020. The conference was planned to take place in Ghent, Belgium, but had to change to an online format due to the COVID-19 pandemic. The 232 full papers and 10 demo papers presented in this volume were carefully reviewed and selected for inclusion in the proceedings. The volumes are organized in topical sections as follows: Part I: Pattern Mining; clustering; privacy and fairness; (social) network analysis and computational social science; dimensionality reduction and autoencoders; domain adaptation; sketching, sampling, and binary projections; graphical models and causality; (spatio-) temporal data and recurrent neural networks; collaborative filtering and matrix completion. Part II: deep learning optimization and theory; active learning; adversarial learning; federated learning; Kernel methods and online learning; partial label learning; reinforcement learning; transfer and multi-task learning; Bayesian optimization and few-shot learning. Part III: Combinatorial optimization; large-scale optimization and differential privacy; boosting and ensemble methods; Bayesian methods; architecture of neural networks; graph neural networks; Gaussian processes; computer vision and image processing; natural language processing; bioinformatics. Part IV: applied data science: recommendation; applied data science: anomaly detection; applied data science: Web mining; applied data science: transportation; applied data science: activity recognition; applied data science: hardware and manufacturing; applied data science: spatiotemporal data. Part V: applied data science: social good; applied data science: healthcare; applied data science: e-commerce and finance; applied data science: computational social science; applied data science: sports; demo track. .

This book constitutes the revised selected papers from the 22nd International Conference on Information Security Applications, WISA 2021, which took place on Jeju Island, South Korea, during August 2021. The 23 papers included in this book were carefully reviewed and selected from 66 submissions. They were organized in topical sections as follows: machine learning security; cryptography; hardware security; and application security.

This book examines the Internet of Things (IoT) and Data Analytics from a technical, application, and business point of view. Internet of Things and Data Analytics Handbook describes essential technical knowledge, building blocks, processes, design principles, implementation, and marketing for IoT projects. It provides readers with knowledge in planning, designing, and implementing IoT projects. The book is written by experts on the subject matter, including international experts from nine countries in the consumer and enterprise fields of IoT. The text starts with an overview and anatomy of IoT, ecosystem of IoT, communication protocols, networking, and available hardware, both present and future applications and transformations, and business models. The text also addresses big data analytics, machine learning, cloud computing, and consideration of sustainability that are essential to be both socially responsible and successful. Design and implementation processes are illustrated with best practices and case studies in action. In addition, the book: Examines cloud computing, data analytics, and sustainability and how they relate to IoT overs the scope of consumer, government, and enterprise applications Includes best practices, business model, and real-world case studies Hwaiyu Geng, P.E., is a consultant with Amica Research (www.AmicaResearch.org, Palo Alto, California), promoting green planning, design, and construction projects. He has had over 40 years of manufacturing and management experience, working with Westinghouse, Applied Materials, Hewlett Packard, and Intel on multi-million high-tech projects. He has written and presented numerous technical papers at international conferences. Mr. Geng, a patent holder, is also the editor/author of Data Center Handbook (Wiley, 2015).

These Proceedings are the work of researchers contributing to the 10th International Conference on Cyber Warfare and Security ICCWS 2015, co hosted this year by the University of Venda and The Council

for Scientific and Industrial Research. The conference is being held at the Kruger National Park, South Africa on the 24 25 March 2015. The Conference Chair is Dr Jannie Zaaiman from the University of Venda, South Africa, and the Programme Chair is Dr Louise Leenen from the Council for Scientific and Industrial Research, South Africa.

This book constitutes the proceedings of the 27th International Conference on Parallel and Distributed Computing, Euro-Par 2021, held in Lisbon, Portugal, in August 2021. The conference was held virtually due to the COVID-19 pandemic. The 38 full papers presented in this volume were carefully reviewed and selected from 136 submissions. They deal with parallel and distributed computing in general, focusing on compilers, tools and environments; performance and power modeling, prediction and evaluation; scheduling and load balancing; data management, analytics and machine learning; cluster, cloud and edge computing; theory and algorithms for parallel and distributed processing; parallel and distributed programming, interfaces, and languages; parallel numerical methods and applications; and high performance architecture and accelerators.

The aim of this book is to provide an overview of recent developments in Kalman filter theory and their applications in engineering and scientific fields. The book is divided into 24 chapters and organized in five blocks corresponding to recent advances in Kalman filtering theory, applications in medical and biological sciences, tracking and positioning systems, electrical engineering and, finally, industrial processes and communication networks.

Digitization and Artificial Intelligence are at the center of every board room conversation these days. Most CEOs, senior management and boards are less worried about their traditional competitors. The impact of disruption through digitization is real and quantifiable – 52% of Fortune 500 companies have been replaced since 2000. The task of enabling new digital business models gets exponentially harder as the complexity of systems are greater. Most CIOs, CTOs are struggling with when to start, what to do, and how to meet the expectations of their CEOs and Boards. Design patterns help narrow this gap by documenting a well-working solution to a problem that occurs repeatedly in a given context. “Enterprise Digitization Patterns” breaks down digital disruption enablers and delivers a cookbook across three key pillars – Digital Experience, Enterprise IoT and Autonomous Systems. The book provides reference architectures, design patterns, maturity models and practical case studies to drive new forms of customer value, business outcomes and business models. The design patterns are distinct or relevant to modern-day enterprise digital platforms that enables enterprise digital business models.

This authoritative volume presents a comprehensive guide to the evaluation and design of networked systems with improved disaster resilience. The text offers enlightening perspectives on issues relating to all major failure scenarios, including natural disasters, disruptions caused by adverse weather conditions, massive technology-related failures, and malicious human activities. Topics and features: describes methods and models for the analysis and evaluation of disaster-resilient communication networks; examines techniques for the design and enhancement of disaster-resilient systems; provides a range of schemes and algorithms for resilient systems; reviews various advanced topics relating to resilient communication systems; presents insights from an international selection of more than 100 expert researchers working across the academic, industrial, and governmental sectors. This practically-focused monograph, providing invaluable support on topics of resilient networking equipment and software, is an essential reference for network professionals including network and networked systems operators, networking equipment vendors, providers of essential services, and regulators. The work can also serve as a supplementary textbook for graduate and PhD courses on networked systems resilience.

Wireless and Satellite Systems11th EAI International Conference, WiSATS 2020, Nanjing, China, September 17-18, 2020, Proceedings, Part IISpringer Nature

Americans' safety, productivity, comfort, and convenience depend on the reliable supply of electric power. The electric power system is a complex "cyber-physical" system composed of a network of millions of components spread out across the continent. These components are owned, operated, and regulated by thousands of different entities. Power system operators work hard to assure safe and reliable service, but large outages occasionally happen. Given the nature of the system, there is simply no way that outages can be completely avoided, no matter how much time and money is devoted to such an effort. The system's reliability and resilience can be improved but never made perfect. Thus, system owners, operators, and regulators must prioritize their investments based on potential benefits. Enhancing the Resilience of the Nation's Electricity System focuses on identifying, developing, and implementing strategies to increase the power system's resilience in the face of events that can cause large-area, long-duration outages: blackouts that extend over multiple service areas and last several days or longer. Resilience is not just about lessening the likelihood that these outages will occur. It is also about limiting the scope and impact of outages when they do occur, restoring power rapidly afterwards, and learning from these experiences to better deal with events in the future.

How well does your enterprise stand up against today's sophisticated security threats? In this book, security experts from Cisco Systems demonstrate how to detect damaging security incidents on your global network--first by teaching you which assets you need to monitor closely, and then by helping you develop targeted strategies and pragmatic techniques to protect them. Security Monitoring is based on the authors' years of experience conducting incident response to keep Cisco's global network secure. It offers six steps to improve network monitoring. These steps will help you: Develop Policies: define rules, regulations, and monitoring criteria Know Your Network: build knowledge of your infrastructure with network telemetry Select Your Targets: define the subset of infrastructure to be monitored Choose Event Sources: identify event types needed to discover policy violations Feed and Tune: collect data, generate alerts, and tune systems using contextual information Maintain Dependable Event Sources: prevent critical gaps in collecting and monitoring events Security Monitoring illustrates these steps with detailed examples that will help you learn to select and deploy the best techniques for monitoring your own enterprise network.

This book focuses on the importance of human factors in the development of safe and reliable unmanned systems. It discusses current challenges such as how to improve the perceptual and cognitive abilities of robots, develop suitable synthetic vision systems, cope with degraded reliability in unmanned systems, predict robotic behavior in case of a loss of communication, the vision for future soldier-robot teams, human-agent teaming, real-world implications for human-robot interaction, and approaches to standardize both the display and control of technologies across unmanned systems. Based on the AHFE 2017 International Conference on Human Factors in Robots and Unmanned Systems, held on July 17–21 in Los Angeles, California, USA, this book is expected to foster new discussion and stimulate new advances in the development of more reliable, safer, and highly functional devices for carrying out automated and concurrent tasks.

Outlier (or anomaly) detection is a very broad field which has been studied in the context of a large number of research areas like statistics, data mining, sensor networks, environmental science, distributed systems, spatio-temporal mining, etc. Initial research in outlier detection focused on time series-based outliers (in statistics). Since then, outlier

detection has been studied on a large variety of data types including high-dimensional data, uncertain data, stream data, network data, time series data, spatial data, and spatio-temporal data. While there have been many tutorials and surveys for general outlier detection, we focus on outlier detection for temporal data in this book. A large number of applications generate temporal datasets. For example, in our everyday life, various kinds of records like credit, personnel, financial, judicial, medical, etc., are all temporal. This stresses the need for an organized and detailed study of outliers with respect to such temporal data. In the past decade, there has been a lot of research on various forms of temporal data including consecutive data snapshots, series of data snapshots and data streams. Besides the initial work on time series, researchers have focused on rich forms of data including multiple data streams, spatio-temporal data, network data, community distribution data, etc. Compared to general outlier detection, techniques for temporal outlier detection are very different. In this book, we will present an organized picture of both recent and past research in temporal outlier detection. We start with the basics and then ramp up the reader to the main ideas in state-of-the-art outlier detection techniques. We motivate the importance of temporal outlier detection and brief the challenges beyond usual outlier detection. Then, we list down a taxonomy of proposed techniques for temporal outlier detection. Such techniques broadly include statistical techniques (like AR models, Markov models, histograms, neural networks), distance- and density-based approaches, grouping-based approaches (clustering, community detection), network-based approaches, and spatio-temporal outlier detection approaches. We summarize by presenting a wide collection of applications where temporal outlier detection techniques have been applied to discover interesting outliers.

This book explores the main concepts, algorithms, and techniques of Machine Learning and data mining for aerospace technology. Satellites are the ‘eagle eyes’ that allow us to view massive areas of the Earth simultaneously, and can gather more data, more quickly, than tools on the ground. Consequently, the development of intelligent health monitoring systems for artificial satellites – which can determine satellites’ current status and predict their failure based on telemetry data – is one of the most important current issues in aerospace engineering. This book is divided into three parts, the first of which discusses central problems in the health monitoring of artificial satellites, including tensor-based anomaly detection for satellite telemetry data and machine learning in satellite monitoring, as well as the design, implementation, and validation of satellite simulators. The second part addresses telemetry data analytics and mining problems, while the last part focuses on security issues in telemetry data.

This book constitutes the refereed proceedings of the 19th EPIA Conference on Artificial Intelligence, EPIA 2019, held in Funchal, Madeira, Portugal, in September 2019. The 119 revised full papers and 6 short papers presented were carefully reviewed and selected from a total of 252 submissions. The papers are organized in 18 tracks devoted to the following topics: AIEd - Artificial Intelligence in Education, AI4G - Artificial Intelligence for Games, AIoTA - Artificial Intelligence and IoT in Agriculture, AIL - Artificial Intelligence and Law, AIM - Artificial Intelligence in Medicine, AICPDES - Artificial Intelligence in Cyber-Physical and Distributed Embedded Systems, AIPES - Artificial Intelligence in Power and Energy Systems, AITS - Artificial Intelligence in Transportation Systems, ALEA - Artificial Life and Evolutionary Algorithms, AmIA - Ambient Intelligence and Affective Environments, BAAI - Business Applications of Artificial Intelligence, GAI- General AI, IROBOT - Intelligent Robotics, KDBI - Knowledge Discovery and Business Intelligence, KRR - Knowledge Representation and Reasoning, MASTA - Multi-Agent Systems: Theory and Applications, SSM - Social Simulation and Modelling, TeMA - Text Mining and Applications.

This volume contains the proceedings of the "Third Multidisciplinary Symposium on Positive Systems: Theory and Applications (POSTA09)" held in Valencia, Spain, September 2–4, 2009. This is the only world congress whose main topic is focused on this field.

Implement a vendor-neutral and multi-cloud cybersecurity and risk mitigation framework with advice from seasoned threat hunting pros In Threat Hunting in the Cloud: Defending AWS, Azure and Other Cloud Platforms Against Cyberattacks, celebrated cybersecurity professionals and authors Chris Peiris, Binil Pillai, and Abbas Kudrati leverage their decades of experience building large scale cyber fusion centers to deliver the ideal threat hunting resource for both business and technical audiences. You'll find insightful analyses of cloud platform security tools and, using the industry leading MITRE ATT&CK framework, discussions of the most common threat vectors. You'll discover how to build a side-by-side cybersecurity fusion center on both Microsoft Azure and Amazon Web Services and deliver a multi-cloud strategy for enterprise customers. And you will find out how to create a vendor-neutral environment with rapid disaster recovery capability for maximum risk mitigation. With this book you'll learn: Key business and technical drivers of cybersecurity threat hunting frameworks in today's technological environment Metrics available to assess threat hunting effectiveness regardless of an organization's size How threat hunting works with vendor-specific single cloud security offerings and on multi-cloud implementations A detailed analysis of key threat vectors such as email phishing, ransomware and nation state attacks Comprehensive AWS and Azure "how to" solutions through the lens of MITRE Threat Hunting Framework Tactics, Techniques and Procedures (TTPs) Azure and AWS risk mitigation strategies to combat key TTPs such as privilege escalation, credential theft, lateral movement, defend against command & control systems, and prevent data exfiltration Tools available on both the Azure and AWS cloud platforms which provide automated responses to attacks, and orchestrate preventative measures and recovery strategies Many critical components for successful adoption of multi-cloud threat hunting framework such as Threat Hunting Maturity Model, Zero Trust Computing, Human Elements of Threat Hunting, Integration of Threat Hunting with Security Operation Centers (SOCs) and Cyber Fusion Centers The Future of Threat Hunting with the advances in Artificial Intelligence, Machine Learning, Quantum Computing and the proliferation of IoT devices. Perfect for technical executives (i.e., CTO, CISO), technical managers, architects, system admins and consultants with hands-on responsibility for cloud platforms, Threat Hunting in the Cloud is also an indispensable

guide for business executives (i.e., CFO, COO CEO, board members) and managers who need to understand their organization's cybersecurity risk framework and mitigation strategy.

This two-volume set LNICST 357-358 constitutes the post-conference proceedings of the 11th EAI International Conference on Wireless and Satellite Services, WiSATS 2020, held in Nanjing, China, in September 2020. The 91 full papers and workshop papers were carefully reviewed and selected from 200 submissions. Part I - LNICST 357 - details original research and results of wireless and satellite technology for a smarter global communication architecture. The theme of WISATS 2020 is “Intelligent Wireless and Satellite Communications for Beyond 5G”. Part II – LNICST 358 - presents 6 workshop papers: High Speed Space Communication and Space Information Networks (HSSCSIN); Integrated Space and Onboard Networks (ISON); Intelligent Satellite Operations, Managements, and Applications (ISOMA); Intelligent Satellites in Future Space Networked System (ISFSNS); Satellite Communications, Networking and Applications (SCNA); Satellite Internet of Things; Trusted Data Sharing, Secure Communication (SIOTTDSSC).

This book constitutes the refereed proceedings of the 36th International Conference on High Performance Computing, ISC High Performance 2021, held virtually in June/July 2021. The 24 full papers presented were carefully reviewed and selected from 74 submissions. The papers cover a broad range of topics such as architecture, networks, and storage; machine learning, AI, and emerging technologies; HPC algorithms and applications; performance modeling, evaluation, and analysis; and programming environments and systems software.

The two volume proceedings of CCIS 698 and 699 constitutes revised selected papers from the 4th International Conference on Geo-Informatics in Resource Management and Sustainable Ecosystem, GRMSE 2016, held in Hong Kong, China, in November 2016. The total of 118 papers presented in these proceedings were carefully reviewed and selected from 311 submissions. The contributions were organized in topical sections named: smart city in resource management and sustainable ecosystem; spatial data acquisition through RS and GIS in resource management and sustainable ecosystem; ecological and environmental data processing and management; advanced geospatial model and analysis for understanding ecological and environmental processes; applications of geo-informatics in resource management and sustainable ecosystem.

This new edition, an up-to-date and comprehensive title on the rapidly expanding field of satellite communication, is aimed at giving important aspects of space and satellite communication. It starts from fundamental concepts and helps reader to design satellite links. The book provides a smooth flow from satellite launch to various applications of satellite. It contains satellite systems, important parameter calculations and design concepts. The emphasis is on geostationary satellites. The text is organized in such a manner that the reader starts with orbiting parameters and ends at designing a complete multiple access links. With all of the latest information incorporated and several key pedagogical attributes included, this textbook is an invaluable learning tool for the engineering students of electronics and communication. New to This Edition • Important design equations have been listed separately. • Three new chapters—Reliability requirements in satellites, Remote sensing satellites and Error control coding—have been included. • New Sections are added in Chapters 1, 2 and 3. • A brief discussion on digitized video transmission is included in Chapter 4.

This book constitutes the thoroughly refereed post-conference proceedings of the 6th International Conference on Agents and Artificial Intelligence, ICAART 2014, held in Angers, France, in March 2014. The 21 revised full papers presented together with one invited paper were carefully reviewed and selected from 225 submissions. The papers are organized in two topical sections on agents and on artificial intelligence.

This book constitutes the refereed proceedings of the 10th International Symposium on Business Modeling and Software Design, BMSD 2020, which took place in Berlin, Germany, in July 2020. BMSD is a leading international forum that brings together researchers and practitioners interested in business modeling and its relation to software design. Particular areas of interest are: Business Processes and Enterprise Engineering; Business Models and Requirements; Business Models and Services; Business Models and Software; Information Systems Architectures and Paradigms; Data Aspects in Business Modeling and Software Development; Blockchain-Based Business Models and Information Systems; IoT and Implications for Enterprise Information Systems. The theme of BMSD 2020 was: Towards Knowledge-Driven Enterprise Information Systems.

Provides general guidance and information on systems engineering that will be useful to the NASA community. It provides a generic description of Systems Engineering (SE) as it should be applied throughout NASA. The handbook will increase awareness and consistency across the Agency and advance the practice of SE. This handbook provides perspectives relevant to NASA and data particular to NASA. Covers general concepts and generic descriptions of processes, tools, and techniques. It provides information on systems engineering best practices and pitfalls to avoid. Describes systems engineering as it should be applied to the development and implementation of large and small NASA programs and projects. Charts and tables.

Router Security Strategies: Securing IP Network Traffic Planes provides a compre-hensive approach to understand and implement IP traffic plane separation and protection on IP routers. This book details the distinct traffic planes of IP networks and the advanced techniques necessary to operationally secure them. This includes the data, control, management, and services planes that provide the infrastructure for IP networking. The first section provides a brief overview of the essential components of the Internet Protocol and IP networking. At the end of this section, you will understand the fundamental principles of defense in depth and breadth security as applied to IP traffic planes. Techniques to secure the IP data plane, IP control plane, IP management plane, and IP services plane are covered in detail in the second section. The final section provides case studies from both the enterprise network and the service provider network perspectives. In this way, the individual IP traffic plane security techniques reviewed in the second section of the book are brought together to help you create an integrated,

comprehensive defense in depth and breadth security architecture. “Understanding and securing IP traffic planes are critical to the overall security posture of the IP infrastructure. The techniques detailed in this book provide protection and instrumentation enabling operators to understand and defend against attacks. As the vulnerability economy continues to mature, it is critical for both vendors and network providers to collaboratively deliver these protections to the IP infrastructure.” –Russell Smoak, Director, Technical Services, Security Intelligence Engineering, Cisco Gregg Schudel, CCIE® No. 9591, joined Cisco in 2000 as a consulting system engineer supporting the U.S. service provider organization. Gregg focuses on IP core network security architectures and technology for interexchange carriers and web services providers. David J. Smith, CCIE No. 1986, joined Cisco in 1995 and is a consulting system engineer supporting the service provider organization. David focuses on IP core and edge architectures including IP routing, MPLS technologies, QoS, infrastructure security, and network telemetry. Understand the operation of IP networks and routers Learn about the many threat models facing IP networks, Layer 2 Ethernet switching environments, and IPsec and MPLS VPN services Learn how to segment and protect each IP traffic plane by applying defense in depth and breadth principles Use security techniques such as ACLs, rate limiting, IP Options filtering, uRPF, QoS, RTBH, QPPB, and many others to protect the data plane of IP and switched Ethernet networks Secure the IP control plane with rACL, CoPP, GTSM, MD5, BGP and ICMP techniques and Layer 2 switched Ethernet-specific techniques Protect the IP management plane with password management, SNMP, SSH, NTP, AAA, as well as other VPN management, out-of-band management, and remote access management techniques Secure the IP services plane using recoloring, IP fragmentation control, MPLS label control, and other traffic classification and process control techniques This security book is part of the Cisco Press® Networking Technology Series. Security titles from Cisco Press help networking professionals secure critical data and resources, prevent and mitigate network attacks, and build end-to-end self-defending networks.

COMMUNICATION NETWORKS AND SERVICE MANAGEMENT IN THE ERA OF ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING Discover the impact that new technologies are having on communication systems with this up-to-date and one-stop resource Communication Networks and Service Management in the Era of Artificial Intelligence and Machine Learning delivers a comprehensive overview of the impact of artificial intelligence (AI) and machine learning (ML) on service and network management. Beginning with a fulsome description of ML and AI, the book moves on to discuss management models, architectures, and frameworks. The authors also explore how AI and ML can be used in service management functions like the generation of workload profiles, service provisioning, and more. The book includes a handpicked selection of applications and case studies, as well as a treatment of emerging technologies the authors predict could have a significant impact on network and service management in the future. Statistical analysis and data mining are also discussed, particularly with respect to how they allow for an improvement of the management and security of IT systems and networks. Readers will also enjoy topics like: A thorough introduction to network and service management, machine learning, and artificial intelligence An exploration of artificial intelligence and machine learning for management models, including autonomic management, policy-based management, intent based management, and network virtualization-based management Discussions of AI and ML for architectures and frameworks, including cloud systems, software defined networks, 5G and 6G networks, and Edge/Fog networks An examination of AI and ML for service management, including the automatic generation of workload profiles using unsupervised learning Perfect for information and communications technology educators, Communication Networks and Service Management in the Era of Artificial Intelligence and Machine Learning will also earn a place in the libraries of engineers and professionals who seek a structured reference on how the emergence of artificial intelligence and machine learning techniques is affecting service and network management.

This book constitutes the proceedings of the 40th SGAI International Conference on Innovative Techniques and Applications of Artificial Intelligence, AI 2020, which was supposed to be held in Cambridge, UK, in December 2020. The conference was held virtually due to the COVID-19 pandemic. The 23 full papers and 9 short papers presented in this volume were carefully reviewed and selected from 44 submissions. The volume includes technical papers presenting new and innovative developments in the field as well as application papers presenting innovative applications of AI techniques in a number of subject domains. The papers are organized in the following topical sections: neural nets and knowledge management; machine learning; industrial applications; advances in applied AI; and medical and legal applications.

Use data analytics to drive innovation and value throughout your network infrastructure Network and IT professionals capture immense amounts of data from their networks. Buried in this data are multiple opportunities to solve and avoid problems, strengthen security, and improve network performance. To achieve these goals, IT networking experts need a solid understanding of data science, and data scientists need a firm grasp of modern networking concepts. Data Analytics for IT Networks fills these knowledge gaps, allowing both groups to drive unprecedented value from telemetry, event analytics, network infrastructure metadata, and other network data sources. Drawing on his pioneering experience applying data science to large-scale Cisco networks, John Garrett introduces the specific data science methodologies and algorithms network and IT professionals need, and helps data scientists understand contemporary network technologies, applications, and data sources. After establishing this shared understanding, Garrett shows how to uncover innovative use cases that integrate data science algorithms with network data. He concludes with several hands-on, Python-based case studies reflecting Cisco Customer Experience (CX) engineers’ supporting its largest customers. These are designed to serve as templates for developing custom solutions ranging from advanced troubleshooting to service assurance. Understand the data analytics landscape and its opportunities in Networking See how elements of an analytics solution come together in the practical use cases Explore and access network data sources, and choose the right data for your problem Innovate more successfully by understanding mental models and cognitive biases Walk through common analytics use cases from many industries, and adapt them to your environment Uncover new data science use cases for optimizing large networks Master proven algorithms, models, and methodologies for solving network problems Adapt use cases built with traditional statistical methods Use data science to improve network infrastructure analysisAnalyze control and data planes with greater sophistication Fully leverage your existing Cisco tools to collect, analyze, and visualize data

End-to-End Network Security Defense-in-Depth Best practices for assessing and improving network defenses and responding to security incidents Omar Santos Information security practices have evolved from Internet perimeter protection to an in-depth defense model in which multiple countermeasures are layered throughout the infrastructure to address vulnerabilities and

attacks. This is necessary due to increased attack frequency, diverse attack sophistication, and the rapid nature of attack velocity—all blurring the boundaries between the network and perimeter. End-to-End Network Security is designed to counter the new generation of complex threats. Adopting this robust security strategy defends against highly sophisticated attacks that can occur at multiple locations in your network. The ultimate goal is to deploy a set of security capabilities that together create an intelligent, self-defending network that identifies attacks as they occur, generates alerts as appropriate, and then automatically responds. End-to-End Network Security provides you with a comprehensive look at the mechanisms to counter threats to each part of your network. The book starts with a review of network security technologies then covers the six-step methodology for incident response and best practices from proactive security frameworks. Later chapters cover wireless network security, IP telephony security, data center security, and IPv6 security. Finally, several case studies representing small, medium, and large enterprises provide detailed example configurations and implementation strategies of best practices learned in earlier chapters. Adopting the techniques and strategies outlined in this book enables you to prevent day-zero attacks, improve your overall security posture, build strong policies, and deploy intelligent, self-defending networks. “Within these pages, you will find many practical tools, both process related and technology related, that you can draw on to improve your risk mitigation strategies.” —Bruce Murphy, Vice President, World Wide Security Practices, Cisco Omar Santos is a senior network security engineer at Cisco®. Omar has designed, implemented, and supported numerous secure networks for Fortune 500 companies and the U.S. government. Prior to his current role, he was a technical leader within the World Wide Security Practice and the Cisco Technical Assistance Center (TAC), where he taught, led, and mentored many engineers within both organizations. Guard your network with firewalls, VPNs, and intrusion prevention systems Control network access with AAA Enforce security policies with Cisco Network Admission Control (NAC) Learn how to perform risk and threat analysis Harden your network infrastructure, security policies, and procedures against security threats Identify and classify security threats Trace back attacks to their source Learn how to best react to security incidents Maintain visibility and control over your network with the SAVE framework Apply Defense-in-Depth principles to wireless networks, IP telephony networks, data centers, and IPv6 networks This security book is part of the Cisco Press® Networking Technology Series. Security titles from Cisco Press help networking professionals secure critical data and resources, prevent and mitigate network attacks, and build end-to-end self-defending networks. Category: Networking: Security Covers: Network security and incident response

This is the eBook version of the print title. Note that the eBook does not provide access to the practice test software that accompanies the print book. Learn, prepare, and practice for CCNA Cyber Ops SECFND 210-250 exam success with this Cert Guide from Pearson IT Certification, a leader in IT Certification learning. Master CCNA Cyber Ops SECFND 210-250 exam topics Assess your knowledge with chapter-ending quizzes Review key concepts with exam preparation tasks CCNA Cyber Ops SECFND 210-250 Official Cert Guide is a best-of-breed exam study guide. Cisco enterprise security experts Omar Santos, Joseph Muniz, and Stefano De Crescenzo share preparation hints and test-taking tips, helping you identify areas of weakness and improve both your conceptual knowledge and hands-on skills. Material is presented in a concise manner, focusing on increasing your understanding and retention of exam topics. The book presents you with an organized test preparation routine through the use of proven series elements and techniques. Exam topic lists make referencing easy. Chapter-ending Exam Preparation Tasks help you drill on key concepts you must know thoroughly. Review questions help you assess your knowledge, and a final preparation chapter guides you through tools and resources to help you craft your final study plan. Well-regarded for its level of detail, assessment features, and challenging review questions and exercises, this study guide helps you master the concepts and techniques that will allow you to succeed on the exam the first time. The study guide helps you master all the topics on the CCNA Cyber Ops SECFND exam, including: Fundamentals of networking protocols and networking device types Network security devices and cloud services Security principles Access control models Security management concepts and techniques Fundamentals of cryptography and PKI Essentials of Virtual Private Networks (VPNs) Windows-based Analysis Linux /MAC OS X-based Analysis Endpoint security technologies Network and host telemetry Security monitoring operations and challenges Types of attacks and vulnerabilities Security evasion techniques

Copyright: 6fc48d0502dd7496ef59403763943904