Smart Grid Security Springerbriefs In Cybersecurity

This book presents a comprehensive introduction to well logging and the inverse problem. It explores challenges such as conventional data processing methods' inability to handle local minima issues, and presents the explanations in an easy-to-follow way. The book describes statistical data interpretation by introducing the fundamentals behind the approach, as well as a range of sampling methods. In each chapter,

a specific method is comprehensively introduced, together with representative examples. The book begins with basic information on well logging and logging while drilling, as well as a definition of the inverse problem. It then moves on to discuss the fundamentals of statistical inverse methods, Bayesian inference, and a new sampling method that can be used to supplement it, the hybrid Monte Carlo method. The book then addresses a specific problem in the inversion of downhole logging data, and the interpretation of earth model complexity, before concluding with a meta-technique called the tempering method, which serves as a supplement to

statistical sampling methods. Given its scope, the book offers a valuable reference guide for drilling engineers, well logging tool physicists, and geoscientists, as well as students in the areas of petroleum engineering and electrical engineering.

This book highlights recent advances in the identification, prediction and exploitation of demand side (DS) flexibility and investigates new methods of predicting DS flexibility at various different power system (PS) levels. Renewable energy sources (RES) are characterized by volatile, partially unpredictable and mostly non-dispatchable generation. The main challenge in terms of

integrating RES into power systems is their intermittency, which negatively affects the power balance. Addressing this challenge requires an increase in the available PS flexibility, which in turn requires accurate estimation of the available flexibility on the DS and aggregation solutions at the system level. This book discusses these issues and presents solutions for effectively tackling them.

This SpringerBrief explores the opportunities and challenges posed by the smart grid. The evolution of the smart grid should allow consumers to directly communicate with their utility provider. However, complex issues such as architecture with legacy support,

varying demand response and load management, varying price of power, and so forth can lead to various decision making challenges. It is essential to identify the scope and challenges of the smart grid in a comprehensive manner so as to ensure efficient delivery of sustainable, economic, and secure electricity supplies. This book provides an overview of the smart grid and its key advances in architecture, distribution management, demand-side response and load balancing, smart automation, electric storage, power loss minimization and security. Readers interested in a basic knowledge of electric grid and communication networks will find

Evolution of Smart Grids useful. Readers who want more insight on smart grid research will also find this book a valuable resource.
This book introduces readers to the fundamentals of the IEC 62559 Use Case Methodology, explains how it is related to the Smart Grid Architecture Model (SGAM), and details how a holistic view for both architecture and requirements engineering can be achieved. It describes a standardized and holistic approach to requirements engineering for smart grid projects based on work conducted in the context of the EU M/490 standardization mandate. Over the last years, this method has been established in Europe as the basic

building block of requirements engineering in the utilities sector. The authors present a canonical, structured approach that users can apply to the Use Case Methodology and the SGAM, as well as open tools for this purpose. The application in various domains outside the smart grid is also discussed, as it can be used for critical infrastructures or system-of-systems domains like Industrie 4.0 and Ambient Assisted Living. Accordingly, the book also presents various architecture models for different fields of application, like EMAM, SCIAM, RAMI 4.0, and MAF.

Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm

Evolution of Smart Grids
Technologies, Big Data and Security
Privacy-Enhancing Fog Computing and Its Applications
The IEC 62559-2 Use Case Template and the SGAM applied in various domains

Security and smart spaces are among the most significant topics in IoT nowadays. The implementation of secured smart spaces is at the heart of this concept, and its development is a key issue in the next generation IoT. This book addresses major security aspects and challenges in realizing smart spaces and sensing platforms in critical

Cloud and IoT applications. The book focuses on both the design and implementation aspects of security models and strategies in smart that are enabled by wireless sensor networks and RFID systems. It mainly examines seamless data access approaches and encryption and decryption aspects in reliable IoT systems.

This SpringerBrief addresses the main security concerns for smart grid, e.g., the privacy of electricity consumers, the exchanged messages integrity and confidentiality, the authenticity of participated parties, and the false data

injection attacks. Moreover, the authors demonstrate in detail the various proposed techniques to secure the smart grid's different communication networks and preserve the privacy of the involved. Over many years, power grid has generated electricity from central generators and distributed it in one direction from the generation stations to end-users; also, information is one directional so that the grid's control center doesn't get enough information about customers' requirements and consequently can't prevent electricity losses. So, the electricity grid is merged with

information and communication technology to form smart grid. The main target of this incorporation is to connect different parties of power grid to exchange information about grid conditions and customers' requirements, and consequently, improve the reliability and efficiency of electricity generation and distribution. That upgrade of the power grid exposes it to the cyber security threats that the communication networks suffer from, such as malicious attacks to forge the electricity consumption readings or price, extract personal information

for residential consumers, such as daily habits and life style, or attack some grid's resources and equipment availability using denial-of-service attacks. Also, novel threats are introduced in smart grid due to the power grid nature, such as false data injection attack, in which the adversary compromises several measurement units and injects false information about the grid conditions that mislead the grid's control center to make wrong decisions for the grid and consequently impact on its stability and efficiency. This SpringerBrief presents

the concept of the smart grid architecture and investigates the security issues of the smart grid and the existing encrypted data query techniques. Unique characteristics of smart grid impose distinguished challenges on this investigation, such as multidimensional attributes in metering data and finer grained query on each dimension. Three kinds of queries are introduced, namely, equality query, conjunctive query and range query. For the equality query over encrypted metering data, an efficient searchable

encryption scheme is introduced and can be applied for auction in emerging smart grid marketing. Later chapters examine the conjunctive query and range query over encrypted data. Different techniques are used, including the Public key Encryption with Keyword Search (PEKS) and Hidden Vector Encryption (HVE), to construct the comparison predicate and range query predicate. Their correctness is demonstrated in the book. Concise and practical, Encrypted Data Querying in Smart Grids is valuable for professionals and researchers involved in data

privacy or encryption. It is also useful for graduate students interested in smart grid and related technologies.
This book brings a high level of fluidity to analytics and addresses recent trends, innovative ideas, challenges and cognitive computing solutions in big data and the Internet of Things (IoT). It explores domain knowledge, data science reasoning and cognitive methods in the context of the IoT, extending current data science approaches by incorporating insights from experts as well as a notion of artificial intelligence, and performing

inferences on the knowledge The book provides a comprehensive overview of the constituent paradigms underlying cognitive computing methods, which illustrate the increased focus on big data in IoT problems as they evolve. It includes novel, in-depth fundamental research contributions from a methodological/application in data science accomplishing sustainable solution for the future perspective. Mainly focusing on the design of the best cognitive embedded data science technologies to process and analyze the large amount of data collected

through the IoT, and aid better decision making, the book discusses adapting decision-making approaches under cognitive computing paradigms to demonstrate how the proposed procedures as well as big data and IoT problems can be handled in practice. This book is a valuable resource for scientists, professionals, researchers, and academicians dealing with the new challenges and advances in the specific areas of cognitive computing and data science approaches.

Information Security of Highly Critical Wireless Networks

Solutions for Sustainability
Communication Networks and Services
How the International Trade, Energy and Climate Change Regimes Can Help
Modeling and Evaluating Denial of Service Attacks for Wireless and Mobile Applications

This SpringerBrief covers modeling and analysis of Denial-of-Service attacks in emerging wireless and mobile applications. It uses an application-specific methodology to model and evaluate denial-of-service attacks. Three emerging applications are explored: multi-modal CSMA/CA

networks, time-critical networks for the smart grid, and smart phone applications. The authors define a new performance metric to quantify the benefits of backoff misbehavior and show the impacts of a wide range of backoff mishandling nodes on the network performance, and propose a scheme to minimize the delay of time-critical message delivery under jamming attacks in smart grid applications. An investigation on the resilience of mobile services against malware attacks is included to advance understanding of network vulnerabilities

associated with emerging wireless networks and offers instrumental guidance into the security design for future wireless and mobile applications. This book is appropriate for students, faculty, engineers, and experts in the technical area of wireless communication, mobile networks and cyber security. This SpringerBrief mainly focuses on effective big data analytics for CPS, and addresses the privacy issues that arise on various CPS applications. The authors develop a series of privacy preserving data analytic and processing methodologies through data driven

optimization based on applied cryptographic techniques and differential privacy in this brief. This brief also focuses on effectively integrating the data analysis and data privacy preservation techniques to provide the most desirable solutions for the state-of-the-art CPS with various application-specific requirements. Cyber-physical systems (CPS) are the "next generation of engineered systems," that integrate computation and networking capabilities to monitor and control entities in the physical world. Multiple domains of CPS typically collect huge

amounts of data and rely on it for decision making, where the data may include individual or sensitive information, for e.g., smart metering, intelligent transportation, healthcare, sensor/data aggregation, crowd sensing etc. This brief assists users working in these areas and contributes to the literature by addressing data privacy concerns during collection, computation or big data analysis in these large scale systems. Data breaches result in undesirable loss of privacy for the participants and for the entire system, therefore identifying the

vulnerabilities and developing tools to mitigate such concerns is crucial to build high confidence CPS. This Springerbrief targets professors, professionals and research scientists working in Wireless Communications, Networking, Cyber-Physical Systems and Data Science. Undergraduate and graduate-level students interested in Privacy Preservation of state-of-the-art Wireless Networks and Cyber-Physical Systems will use this Springerbrief as a study guide.

The brief focuses on applying sublinear algorithms to manage critical big data

challenges. The text offers an essential introduction to sublinear algorithms, explaining why they are vital to large scale data systems. It also demonstrates how to apply sublinear algorithms to three familiar big data applications: wireless sensor networks, big data processing in Map Reduce and smart grids. These applications present common experiences, bridging the theoretical advances of sublinear algorithms and the application domain. Sublinear Algorithms for Big Data Applications is suitable for researchers, engineers and graduate

students in the computer science, communications and signal processing communities.
This book mainly concentrates on protecting data security and privacy when participants communicate with each other in the Internet of Things (IoT). Technically, this book categorizes and introduces a collection of secure and privacy-preserving data communication schemes/protocols in three traditional scenarios of IoT: wireless sensor networks, smart grid and vehicular ad-hoc networks recently. This book presents

three advantages which will appeal to readers. Firstly, it broadens reader's horizon in IoT by touching on three interesting and complementary topics: data aggregation, privacy protection, and key agreement and management. Secondly, various cryptographic schemes/protocols used to protect data confidentiality and integrity is presented. Finally, this book will illustrate how to design practical systems to implement the algorithms in the context of IoT communication. In summary, readers can simply learn and directly apply the new

technologies to communicate data in IoT after reading this book.

Formal Analysis of Future Energy Systems Using Interactive Theorem Proving

Security and Privacy in Smart Grid

Smart Grid Security

Mobile Edge Computing

AI4RAILS, DREAMS, DSOGRI, SERENE 2020, Munich, Germany, September 7, 2020, Proceedings

This book provides a brief and general introduction to cybersecurity and cyber-risk assessment. Not limited to a specific approach or technique, its focus is highly pragmatic and is based on established international standards (including ISO 31000) as well as

industrial best practices. It explains how cyber-risk assessment should be conducted, which techniques should be used when, what the typical challenges and problems are, and how they should be addressed. The content is divided into three parts. First, part I provides a conceptual introduction to the topic of risk management in general and to cybersecurity and cyber-risk management in particular. Next, part II presents the main stages of cyber-risk assessment from context establishment to risk treatment and acceptance, each illustrated by a running example. Finally, part III details four important challenges and how to reasonably deal with them in practice: risk measurement, risk scales, uncertainty, and low-frequency risks with high

consequence. The target audience is mainly practitioners and students who are interested in the fundamentals and basic principles and techniques of security risk assessment, as well as lecturers seeking teaching material. The book provides an overview of the cyber-risk assessment process, the tasks involved, and how to complete them in practice.

The book deals with the conceptual and practical knowledge of the latest tools and methodologies of hardware development for Internet of Things (IoT) and variety of real-world challenges. The topics cover the state-of-the-art and future perspectives of IoT technologies, where industry experts, researchers, and academics had shared ideas and experiences

surrounding frontier technologies, breakthrough, and innovative solutions and applications. Several aspects of various hardware technologies, methodologies, and communication protocol such as formal design flow for IoT hardware, design approaches for IoT hardware, IoT solution reference architectures and Instances, simulation, modelling and programming framework, hardware basics of sensors for IoT, configurable processor and technology for IoT and real-life examples and studies are critically examined in this book. It also identifies key technological facet that supports the relevance of hardware perspective of IoT and discusses the benefits and challenges to dominate the next decades. The book serves as an

excellent reference for senior undergraduates and graduates in electrical and computer engineering, research scholars, mobile and wireless communications engineers, IT engineers, and electronics engineers who need to understand IoT at an in-depth level to build and manage IoT solutions.

This open access book presents thirteen outstanding doctoral dissertations in Information Technology from the Department of Electronics, Information and Bioengineering, Politecnico di Milano, Italy. Information Technology has always been highly interdisciplinary, as many aspects have to be considered in IT systems. The doctoral studies program in IT at Politecnico di Milano

emphasizes this interdisciplinary nature, which is becoming more and more important in recent technological advances, in collaborative projects, and in the education of young researchers. Accordingly, the focus of advanced research is on pursuing a rigorous approach to specific research topics starting from a broad background in various areas of Information Technology, especially Computer Science and Engineering, Electronics, Systems and Control, and Telecommunications. Each year, more than 50 PhDs graduate from the program. This book gathers the outcomes of the thirteen best theses defended in 2019-20 and selected for the IT PhD Award. Each of the authors provides a chapter

summarizing his/her findings, including an introduction, description of methods, main achievements and future work on the topic. Hence, the book provides a cutting-edge overview of the latest research trends in Information Technology at Politecnico di Milano, presented in an easy-to-read format that will also appeal to non-specialists.

This SpringerBrief explores features of digital protocol wireless communications systems, and features of the emerging electrical smart grid. Both low power and high power wireless systems are described. The work also examines the cybersecurity vulnerabilities, threats and current levels of risks to critical infrastructures that rely on digital wireless

technologies. Specific topics include areas of application for high criticality wireless networks (HCWN), modeling risks and vulnerabilities, governance and management frameworks, systemic mitigation, reliable operation, assessing effectiveness and efficiency, resilience testing, and accountability of HCWN. Designed for researchers and professionals, this SpringerBrief provides essential information for avoiding malevolent uses of wireless networks. The content is also valuable for advanced-level students interested in security studies or wireless networks.

Sublinear Algorithms for Big Data Applications

Graph Theory Applications to Deregulated Power Systems

Demand-side Flexibility in Smart Grid

The Use Case and Smart Grid Architecture Model Approach
A Game- and Decision-Theoretic Approach to Resilient Interdependent Network Analysis and Design

This book explores links and synergies between international trade and two of the most urgent challenges of the 21st century: achieving sustainable energy (i.e., energy that is affordable, secure, and clean) and mitigating climate change. It takes the unique approach of not only examining how international trade can help achieve energy and climate goals, but also the impact of emerging tools and technologies such as smart grids and demand response, and the potential role and impact of citizens and prosumers. The book analyzes energy- and trade-related regulations in a range of jurisdictions to assess how conducive the regulation is

towards achieving sustainable energy, and identifies gaps and overlaps in the existing legal framework.

The Industry 4.0 revolution is changing the world around us. Artificial intelligence and machine learning, automation and robotics, big data, Internet of Things, augmented reality, virtual reality, and creativity are the tools of Industry 4.0. Improved collaboration is seen between smart systems and humans, which merges humans' critical and cognitive thinking abilities with highly accurate and fast industrial automation. Securing IoT in Industry 4.0 Applications with Blockchain examines the role of IoT in Industry 4.0 and how it can be made secure through various technologies including blockchain. The book begins with an in-depth look at IoT and discusses applications, architecture, technologies, tools, and programming languages. It then examines

blockchain and cybersecurity, as well as how blockchain achieves cybersecurity. It also looks at cybercrimes and their preventive measures and issues related to IoT security and trust. Features An overview of how IoT is used to improve the performance of Industry 4.0 systems The evolution of the Industrial Internet of Things (IIoT), its proliferation and market share, and some examples across major industries An exploration of how smart farming is helping farmers prevent plant disease The concepts behind the Internet of Nano Things (IoNT), including the nanomachine and nanonetwork architecture and nano-communication paradigms A look at how blockchains can enhance cybersecurity in a variety of applications, including smart contracts, transferring financial instruments, and Public Key Infrastructure An overview of the structure and working of a blockchain,

including the types, evolution, benefits, and applications of blockchain to industries A framework of technologies designed to shield networks, computers, and data from malware, vulnerabilities, and unauthorized activities An explanation of the automation system employed in industries along with its classification, functionality, flexibility, limitations, and applications

Power systems are increasingly collecting large amounts of data due to the expansion of the Internet of Things into power grids. In a smart grids scenario, a huge number of intelligent devices will be connected with almost no human intervention characterizing a machine-to-machine scenario, which is one of the pillars of the Internet of Things. The book characterizes and evaluates how the emerging growth of data in communications networks applied to smart

grids will impact the grid efficiency and reliability. Additionally, this book discusses the various security concerns that become manifest with Big Data and expanded communications in power grids. Provide a general description and definition of big data, which has been gaining significant attention in the research community. Introduces a comprehensive overview of big data optimization methods in power system. Reviews the communication devices used in critical infrastructure, especially power systems; security methods available to vet the identity of devices; and general security threats in CI networks. Presents applications in power systems, such as power flow and protection. Reviews electricity theft concerns and the wide variety of data-driven techniques and applications developed for electricity theft detection.

In lively and engaging language, this book describes our dependence on freight transport and its vulnerability to diminishing supplies and high prices of oil. Ships, trucks, and trains are the backbone of civilization, hauling the goods that fulfill our every need and desire. Their powerful, highly-efficient diesel combustion engines are exquisitely fine-tuned to burn petroleum-based diesel fuel. These engines and the fuels that fire them have been among the most transformative yet disruptive technologies on the planet. Although this transportation revolution has allowed many of us to fill our homes with global goods even a past emperor would envy, our era of abundance, and the freight transport system in particular, is predicated on the affordability and high energy density of a single fuel, oil. This book explores alternatives to this finite resource including other liquid fuels, truck

and locomotive batteries and utility-scale energy storage technology, and various forms of renewable electricity to support electrified transport. Transportation also must adapt to other challenges: Threats from climate change, financial busts, supply-chain failure, and transportation infrastructure decay. Robert Hirsch, who wrote the "Peaking of World Oil Production" report for the U.S. Department of Energy in 2005, said that planning for peak world production must start at least 10, if not 20 years ahead of time. What little planning exists focuses mainly on how to accommodate 30 percent more economic growth while averting climate change, ignoring the possibility that we are at, or near, the end of growth. Taken for granted, the modern transportation system will not endure forever. The time is now to take a realistic and critical look at the choices ahead, and

how the future of transportation may unfold.
Security in IoT-Enabled Spaces
Cognitive Computing for Big Data Systems Over IoT
Special Topics in Information Technology
Cyber-Risk Management

This book highlights recent advances in smart cities technologies, with a focus on new technologies such as biometrics, blockchains, data encryption, data mining, machine learning, deep learning, cloud security, and mobile security. During the past five years, digital cities have been emerging as a technology reality that will come to dominate the usual life of people, in either developed or developing countries. Particularly, with big data issues from smart cities, privacy and security have been a widely concerned matter due to its relevance and sensitivity

extensively present in cybersecurity, healthcare, medical service, e-commercial, e-governance, mobile banking, e-finance, digital twins, and so on. These new topics rises up with the era of smart cities and mostly associate with public sectors, which are vital to the modern life of people. This volume summarizes the recent advances in addressing the challenges on big data privacy and security in smart cities and points out the future research direction around this new challenging topic.

This is an open access book. It offers comprehensive, self-contained knowledge on Mobile Edge Computing (MEC), which is a very promising technology for achieving intelligence in the next-generation wireless communications and computing networks.The book starts with the basic concepts, key techniques and network architectures of MEC. Then, we

present the wide applications of MEC, including edge caching, 6G networks, Internet of Vehicles, and UAVs. In the last part, we present new opportunities when MEC meets blockchain, Artificial Intelligence, and distributed machine learning (e.g., federated learning). We also identify the emerging applications of MEC in pandemic, industrial Internet of Things and disaster management.The book allows an easy cross-reference owing to the broad coverage on both the principle and applications of MEC. The book is written for people interested in communications and computer networks at all levels. The primary audience includes senior undergraduates, postgraduates, educators, scientists, researchers, developers, engineers, innovators and research strategists.
This brief introduces game- and decision-theoretical techniques for the analysis

and design of resilient interdependent networks. It unites game and decision theory with network science to lay a system-theoretical foundation for understanding the resiliency of interdependent and heterogeneous network systems. The authors pay particular attention to critical infrastructure systems, such as electric power, water, transportation, and communications. They discuss how infrastructure networks are becoming increasingly interconnected as the integration of Internet of Things devices, and how a single-point failure in one network can propagate to other infrastructures, creating an enormous social and economic impact. The specific topics in the book include: · static and dynamic meta-network resilience game analysis and design; · optimal control of interdependent epidemics spreading over

complex networks; and · applications to secure and resilient design of critical infrastructures. These topics are supported by up-to-date summaries of the authors' recent research findings. The authors then discuss the future challenges and directions in the analysis and design of interdependent networks and explain the role of multi-disciplinary research has in computer science, engineering, public policy, and social sciences fields of study. The brief introduces new application areas in mathematics, economics, and system and control theory, and will be of interest to researchers and practitioners looking for new approaches to assess and mitigate risks in their systems and enhance their network resilience. A Game- and Decision-Theoretic Approach to Resilient Interdependent Network Analysis and Design also has self-contained chapters, which allows for

multiple levels of reading by anyone with an interest in game and decision theory and network science.

This book provides a detailed description of network science concepts applied to power systems and electricity markets, offering an appropriate blend of theoretical background and practical applications for operation and power system planning. It discusses an approach to understanding power systems from a network science perspective using the direct recognition of the interconnectivity provided by the transmission system. Further, it explores the network properties in detail and characterizes them as a tool for online and offline applications for power system operation. The book includes an in-depth explanation of electricity markets problems that can be addressed from a graph theory perspective. It is intended for advanced undergraduate

and graduate students in the fields of electric energy systems, operations research, management science and economics. Practitioners in the electric energy sector also benefit from the concepts and techniques presented here.

Transportation and Power Grid in Smart Cities

Energy and the Future of Transportation

When Trucks Stop Running

Internet of Things for Smart Cities

Securing IoT in Industry 4.0 Applications with Blockchain

This book describes an accurate analysis technique for energy systems based on formal methods—computer-based mathematical logic techniques for the specification, validation, and verification of the systems. Correctness and accuracy of the financial, operational, and implementation analysis are of the paramount importance for the

materialization of the future energy systems, such as smart grids, to achieve the objectives of cost-effectiveness, efficiency, and quality-of-service. In this regard, the book develops formal theories of microeconomics, asymptotic, and stability to support the formal analysis of generation and distribution cost, smart operations, and processing of energy in a smart grid. These formal theories are also employed to formally verify the cost and utility modeling for: Energy generation and distribution; Asymptotic bounds for online scheduling algorithms for plug-in electric vehicles; and Stability of the power converters for wind turbines. The proposed approach results in mechanized proofs for the specification, validation, and verification of corresponding smart grid problems. The formal mathematical theories developed can be applied to the formal analysis of several other hardware

and software systems as well, making this book of interest to researchers and practicing engineers in a variety of power electronic fields.

This book discusses the evolution of future-generation technologies through the Internet of things, bringing together all the related technologies on a single platform to offer valuable insights for undergraduate and postgraduate students, researchers, academics and industry practitioners. The book uses data, network engineering and intelligent decision-support system-by-design principles to design a reliable IoT-enabled ecosystem and to implement cyber-physical pervasive infrastructure solutions. It takes readers on a journey that begins with understanding the insight paradigm of IoT-enabled technologies and how it can be applied. It walks readers through engaging with real-time challenges and building a safe

infrastructure for IoT-based, future-generation technologies. The book helps researchers and practitioners to understand the design architecture through IoT and the state of the art in IoT countermeasures. It also highlights the differences between heterogeneous platforms in IoT-enabled infrastructure and traditional ad hoc or infrastructural networks, and provides a comprehensive discussion on functional frameworks for IoT, object identification, IoT domain model, RFID technology, wearable sensors, WBAN, IoT semantics, knowledge extraction, and security and privacy issues in IoT-based ecosystems. Written by leading international experts, it explores IoT-enabled insight paradigms, which are utilized for the future benefit of humans. It also includes references to numerous works. Divided into stand-alone chapters, this highly readable book is intended for specialists, researchers,

graduate students, designers, experts, and engineers involved in research on healthcare-related issues.

This book on smart grid security is meant for a broad audience from managers to technical experts. It highlights security challenges that are faced in the smart grid as we widely deploy it across the landscape. It starts with a brief overview of the smart grid and then discusses some of the reported attacks on the grid. It covers network threats, cyber physical threats, smart metering threats, as well as privacy issues in the smart grid. Along with the threats the book discusses the means to improve smart grid security and the standards that are emerging in the field. The second part of the book discusses the legal issues in smart grid implementations, particularly from a privacy (EU data protection) point of view.

This book introduces the concept of smart city as the potential solution to the challenges created by urbanization. The Internet of Things (IoT) offers novel features with minimum human intervention in smart cities. This book describes different components of Internet of Things (IoT) for smart cities including sensor technologies, communication technologies, big data analytics and security.

Social Network Forensics, Cyber Security, and Machine Learning

A Hardware Development Perspective

Wireless Communications Networks for the Smart Grid

Dependable Computing - EDCC 2020 Workshops

Statistical Inversion of Electromagnetic Logging Data

This brief focuses on the current research on security

and privacy preservation in smart grids. Along with a review of the existing works, this brief includes fundamental system models, possible frameworks, useful performance, and future research directions. It explores privacy preservation demand response with adaptive key evolution, secure and efficient Merkle tree based authentication, and fine-grained keywords comparison in the smart grid auction market. By examining the current and potential security and privacy threats, the author equips readers to understand the developing issues in smart grids. The brief is designed for

researchers and professionals working with computer communication networks and smart grids. Graduate students interested in networks and communication engineering will also find the brief an essential resource. This SpringerBrief presents adaptive resource allocation schemes for secondary users for dynamic spectrum access (DSA) in cognitive radio networks (CRNs) by considering Quality-of-Service requirements, admission control, power/rate control, interference constraints, and the impact of spectrum sensing or primary user interruptions. It presents the challenges, motivations, and

applications of the different schemes. The authors discuss cloud-assisted geolocation-aware adaptive resource allocation in CRNs by outsourcing computationally intensive processing to the cloud. Game theoretic approaches are presented to solve resource allocation problems in CRNs. Numerical results are presented to evaluate the performance of the proposed methods. Adaptive Resource Allocation in Cognitive Radio Networks is designed for professionals and researchers working in the area of wireless networks. Advanced-level students in electrical engineering and computer science, especially

those focused on wireless networks, will find this information helpful.
This book discusses the issues and challenges in Online Social Networks (OSNs). It highlights various aspects of OSNs consisting of novel social network strategies and the development of services using different computing models. Moreover, the book investigates how OSNs are impacted by cutting-edge innovations.
Smart Grid SecuritySpringer
Querying over Encrypted Data in Smart Grids
Frameworks, Tools and Applications
Internet of Things
Online Algorithms for Optimal

Energy Distribution in Microgrids
Dynamic Spectrum Access for Wireless Networks

This brief presents a comprehensive review of the network architecture and communication technologies of the smart grid communication network (SGCN). It then studies the strengths, weaknesses and applications of two promising wireless mesh routing protocols that could be used to implement the SGCN. Packet transmission reliability, latency and robustness of these two protocols are evaluated and compared by simulations in various practical SGCN scenarios. Finally, technical challenges and open research opportunities of the SGCN are

addressed. Wireless Communications Networks for Smart Grid provides communication network architects and engineers with valuable proven suggestions to successfully implement the SGCN. Advanced-level students studying computer science or electrical engineering will also find the content helpful.

With the increasing worldwide trend in population migration into urban centers, we are beginning to see the emergence of the kinds of mega-cities which were once the stuff of science fiction. It is clear to most urban planners and developers that accommodating the needs of the tens of millions of inhabitants of those megalopolises in an orderly and uninterrupted manner will require the

seamless integration of and real-time monitoring and response services for public utilities and transportation systems. Part speculative look into the future of the world's urban centers, part technical blueprint, this visionary book helps lay the groundwork for the communication networks and services on which tomorrow's "smart cities" will run. Written by a uniquely well-qualified author team, this book provides detailed insights into the technical requirements for the wireless sensor and actuator networks required to make smart cities a reality. Presenting an optimal energy distribution strategy for microgrids in a smart grid environment, and featuring a detailed analysis of the mathematical techniques of convex

optimization and online algorithms, this book provides readers with essential content on how to achieve multi-objective optimization that takes into consideration power subscribers, energy providers and grid smoothing in microgrids. Featuring detailed theoretical proofs and simulation results that demonstrate and evaluate the correctness and effectiveness of the algorithm, this text explains step-by-step how the problem can be reformulated and solved, and how to achieve the distributed online algorithm on the basis of a centralized offline algorithm. Special attention is paid to how to apply this algorithm in practical cases and the possible future trends of the microgrid and smart grid research and applications. Offering a

valuable guide to help researchers and students better understand the new smart grid, this book will also familiarize readers with the concept of the microgrid and its relationship with renewable energy.

Cloud computing is the latest market-oriented computing paradigm which brings software design and development into a new era characterized by “XaaS”, i.e. everything as a service. Cloud workflows, as typical software applications in the cloud, are composed of a set of partially ordered cloud software services to achieve specific goals. However, due to the low QoS (quality of service) nature of the cloud environment, the design of workflow systems in the cloud

becomes a challenging issue for the delivery of high quality cloud workflow applications. To address such an issue, this book presents a systematic investigation to the three critical aspects for the design of a cloud workflow system, viz. system architecture, system functionality and quality of service. Specifically, the system architecture for a cloud workflow system is designed based on the general four-layer cloud architecture, viz. application layer, platform layer, unified resources layer and fabric layer. The system functionality for a cloud workflow system is designed based on the general workflow reference model but with significant extensions to accommodate software services in the

cloud. The support of QoS is critical for the quality of cloud workflow applications. This book presents a generic framework to facilitate a unified design and development process for software components that deliver lifecycle support for different QoS requirements. While the general QoS requirements for cloud workflow applications can have many dimensions, this book mainly focuses on three of the most important ones, viz. performance, reliability and security. In this book, the architecture, functionality and QoS management of our SwinDeW-C prototype cloud workflow system are demonstrated in detail as a case study to evaluate our generic design for cloud workflow systems. To conclude,

this book offers a general overview of cloud workflow systems and provides comprehensive introductions to the design of the system architecture, system functionality and QoS management.

Big Data Privacy Preservation for Cyber-Physical Systems

Enabling Secure and Privacy Preserving Communications in Smart Grids

Secure and Privacy-Preserving Data Communication in Internet of Things

Big Data Privacy and Security in Smart Cities

The Design of Cloud Workflow Systems

This book constitutes refereed proceedings of the Workshops of the

16th European Dependable Computing Conference, EDCC: Workshop on Articial Intelligence for Railways, AI4RAILS 2020, Worskhop on Dynamic Risk Management for Autonomous Systems, DREAMS 2020, Workshop on Dependable Solutions for Intelligent Electricity Distribution Grids, DSOGRI 2020, Workshop on Software Engineering for Resilient Systems, SERENE 2020, held in September 2020. Due to the COVID-19 pandemic the workshops were held

virtually. The 12 full papers and 4 short papers were thoroughly reviewed and selected from 35 submissions. The workshop papers complement the main conference topics by addressing dependability or security issues in specic application domains or by focussing in specialized topics, such as system resilience.

This SpringerBrief covers the security and privacy challenges in fog computing, and

proposes a new secure and privacy-preserving mechanisms to resolve these challenges for securing fog-assisted IoT applications. Chapter 1 introduces the architecture of fog-assisted IoT applications and the security and privacy challenges in fog computing. Chapter 2 reviews several promising privacy-enhancing techniques and illustrates examples on how to leverage these techniques to enhance

the privacy of users in fog computing. Specifically, the authors divide the existing privacy-enhancing techniques into three categories: identity-hidden techniques, location privacy protection and data privacy enhancing techniques. The research is of great importance since security and privacy problems faced by fog computing impede the healthy development of its enabled IoT applications. With the

advanced privacy-enhancing techniques, the authors propose three secure and privacy-preserving protocols for fog computing applications, including smart parking navigation, mobile crowdsensing and smart grid. Chapter 3 introduces identity privacy leakage in smart parking navigation systems, and proposes a privacy-preserving smart parking navigation system to prevent identity privacy

exposure and support efficient parking guidance retrieval through road-side units (fogs) with high retrieving probability and security guarantees. Chapter 4 presents the location privacy leakage, during task allocation in mobile crowdsensing, and propose a strong privacy-preserving task allocation scheme that enables location-based task allocation and reputation-based report selection without

exposing knowledge about the location and reputation for participators in mobile crowdsensing. Chapter 5 introduces the data privacy leakage in smart grid, and proposes an efficient and privacy-preserving smart metering protocol to allow collectors (fogs) to achieve real-time measurement collection with privacy-enhanced data aggregation. Finally, conclusions and future research directions are given in

Chapter 6. This brief validates the significant feature extension and efficiency improvement of IoT devices without sacrificing the security and privacy of users against dishonest fog nodes. It also provides valuable insights on the security and privacy protection for fog-enabled IoT applications. Researchers and professionals who carry out research on security and privacy in wireless

communication will want to purchase this SpringerBrief. Also, advanced level students, whose main research area is mobile network security will also be interested in this SpringerBrief.

Big Data Analytics in Future Power Systems