Access Free Pdf Devices Iot For Certificates Other And Root Create To How

This is likewise one of the factors by obtaining the soft documents of this **Pdf Devices Iot For Certificates Other And Root Create To How** by online. You might not require more become old to spend to go to the book instigation as competently as search for them. In some cases, you likewise realize not discover the message Pdf Devices Iot For Certificates Other And Root Create To How that you are looking for. It will very squander the time.

However below, bearing in mind you visit this web page, it will be for that reason unquestionably simple to get as without difficulty as download guide Pdf Devices Iot For Certificates Other And Root Create To How

It will not tolerate many era as we accustom before. You can reach it even if act out something else at house and even in your workplace. so easy! So, are you question? Just exercise just what we present below as capably as review **Pdf Devices Iot For Certificates Other And Root Create To How** what you later than to read!

KEY=AND - SHERLYN LUCA

Technology for Smart Futures

Springer This book explores the nexus of Sustainability and Information Communication Technologies that are rapidly changing the way we live, learn, and do business. The monumental amount of energy required to power the Zeta byte of data traveling across the globe’s billions of computers and mobile phones daily cannot be overstated. This ground-breaking reference examines the possibility that our evolving technologies may enable us to mitigate our global energy crisis, rather than adding to it. By connecting concepts and trends such as smart homes, big data, and the internet of things with their applications to sustainability, the authors suggest that emerging and ubiquitous technologies embedded in our daily lives may rightfully be considered as enabling solutions for our future sustainable

development.

Practical IoT Hacking

The Definitive Guide to Attacking the Internet of Things

No Starch Press Written by all-star security experts, Practical IoT Hacking is a quick-start conceptual guide to testing and exploiting IoT systems and devices. Drawing from the real-life exploits of five highly regarded IoT security researchers, Practical IoT Hacking teaches you how to test IoT systems, devices, and protocols to mitigate risk. The book begins by walking you through common threats and a threat modeling framework. You'll develop a security testing methodology, discover the art of passive reconnaissance, and assess security on all layers of an IoT system. Next, you'll perform VLAN hopping, crack MQTT authentication, abuse UPnP, develop an mDNS poisoner, and craft WS-Discovery attacks. You'll tackle both hardware hacking and radio hacking, with in-depth coverage of attacks against embedded IoT devices and RFID systems. You'll also learn how to: Write a DICOM service scanner as an NSE module Hack a microcontroller through the UART and SWD interfaces Reverse engineer firmware and analyze mobile companion apps Develop an NFC fuzzer using Proxmark3 Hack a smart home by jamming wireless alarms, playing back IP camera feeds, and controlling a smart treadmill The tools and devices you'll use are affordable and readily available, so you can easily practice what you learn. Whether you're a security researcher, IT team member, or hacking hobbyist, you'll find Practical IoT Hacking indispensable in your efforts to hack all the things REQUIREMENTS: Basic knowledge of Linux command line, TCP/IP, and programming

Cybersecurity Management

An Organizational and Strategic Approach

University of Toronto Press Cybersecurity Management looks at the current state of cybercrime and explores how organizations can develop resources and capabilities to prepare themselves for the changing cybersecurity environment.

IoT Security

Advances in Authentication

John Wiley & Sons An up-to-date guide to an overview of authentication in the Internet of Things (IoT) The Internet of things (IoT) is the network of the countless physical devices that have the possibility to connect and exchange data. Among the various security requirements, authentication to the IoT is the first step to prevent the impact of attackers. IoT Security offers an important guide into the development of the many authentication mechanisms that provide IoT authentication at various levels such as user level, device level and network level. The book covers a wide range of topics including an overview of IoT and addresses in detail the security challenges at every layer by considering both the technologies and the architecture used. The authors—noted experts on the topic—provide solutions for remediation of compromised security, as well as methods for risk mitigation, and offer suggestions for prevention and improvement. In addition, IoT Security offers a variety of illustrative use cases. This important book: Offers an authoritative reference designed for use by all IoT stakeholders Includes information for securing devices at the user, device, and network levels Contains a classification of existing vulnerabilities Written by an international group of experts on the topic Provides a guide to the most current information available on IoT security Written for network operators, cloud operators, IoT device manufacturers, IoT device users, wireless users, IoT standardization organizations, and security solution developers, IoT Security is an essential guide that contains information on security features, including underlying networks, architectures, and security requirements.

Connectivity Frameworks for Smart Devices

The Internet of Things from a Distributed Computing

Perspective

Springer This timely volume provides a review of the state-of-the-art frameworks and methodologies for connecting diverse objects and devices according to the vision for an Internet of Things (IoT). A specific focus is placed on the communication, security, and privacy aspects of device connectivity in distributed environments. Insights and case studies are provided by an authoritative selection of contributors of international repute into the latest research advances and practical approaches with respect to the connectivity of heterogeneous smart and sensory devices. Topics and features: Examines aspects of device connectivity within the IoT Presents a resource-based architecture for IoT, and proposes a resource management framework for corporate device clouds Reviews integration approaches for the IoT environment, and discusses performance optimization of intelligent home networks Introduces a novel solution for interoperable data management in multi-clouds, and suggests an approach that addresses the debate over network neutrality in the IoT Describes issues of data security, privacy, access control, and authentication in the distributed IoT environment Reviews the evolution of VANETs in relation to the Internet of Vehicles, and provides a perspective on developing smart sustainable cities This invaluable text/reference will be of great benefit to a broad audience, from students and researchers interested in the IoT vision, to practicing communication engineers and network security specialists.

Internet of Things: Concepts and System Design

Springer Nature This comprehensive overview of IoT systems architecture includes in-depth treatment of all key components: edge, communications, cloud, data processing, security, management, and uses. Internet of Things: Concepts and System Design provides a reference and foundation for students and practitioners that they can build upon to design IoT systems and to understand how the specific parts they are working on fit into and interact with the rest of the system. This is especially important since IoT is a multidisciplinary area that requires diverse skills and knowledge including: sensors, embedded systems, real-time systems, control systems, communications, protocols, Internet, cloud computing, large-scale distributed processing and storage systems, AI and ML, (preferably) coupled with domain experience in the area where it is to be applied, such as building or manufacturing automation. Written in a reader-minded approach that starts by describing the problem (why should I care?), placing it in context (what does

this do and where/how does it fit in the great scheme of things?) and then describing salient features of solutions (how does it work?), this book covers the existing body of knowledge and design practices, but also offers the author's insights and articulation of common attributes and salient features of solutions such as IoT information modeling and platform characteristics.

Practical Internet of Things Security

Design a security framework for an Internet connected ecosystem, 2nd Edition

Packt Publishing Ltd A practical, indispensable security guide that will navigate you through the complex realm of securely building and deploying systems in our IoT-connected world Key Features Learn best practices to secure your data from the device to the cloud Use systems security engineering and privacy-by-design principles to design a secure IoT ecosystem A practical guide that will help you design and implement cyber security strategies for your organization Book Description With the advent of the Internet of Things (IoT), businesses have to defend against new types of threat. The business ecosystem now includes the cloud computing infrastructure, mobile and fixed endpoints that open up new attack surfaces. It therefore becomes critical to ensure that cybersecurity threats are contained to a minimum when implementing new IoT services and solutions. This book shows you how to implement cybersecurity solutions, IoT design best practices, and risk mitigation methodologies to address device and infrastructure threats to IoT solutions. In this second edition, you will go through some typical and unique vulnerabilities seen within various layers of the IoT technology stack and also learn new ways in which IT and physical threats interact. You will then explore the different engineering approaches a developer/manufacturer might take to securely design and deploy IoT devices. Furthermore, you will securely develop your own custom additions for an enterprise IoT implementation. You will also be provided with actionable guidance through setting up a cryptographic infrastructure for your IoT implementations. You will then be guided on the selection and configuration of Identity and Access Management solutions for an IoT implementation. In conclusion, you will explore cloud security architectures and security best practices for operating and managing cross-organizational, multi-domain IoT deployments. What you will learn Discuss the need for separate security

requirements and apply security engineering principles on IoT devices Master the operational aspects of planning, deploying, managing, monitoring, and detecting the remediation and disposal of IoT systems Use Blockchain solutions for IoT authenticity and integrity Explore additional privacy features emerging in the IoT industry, such as anonymity, tracking issues, and countermeasures Design a fog computing architecture to support IoT edge analytics Detect and respond to IoT security incidents and compromises Who this book is for This book targets IT Security Professionals and Security Engineers (including pentesters, security architects and ethical hackers) who would like to ensure the security of their organization's data when connected through the IoT. Business analysts and managers will also find this book useful.

Dependable IoT for Human and Industry

Modeling, Architecting, Implementation

CRC Press There are numerous publications which introduce and discuss the Internet of Things (IoT). In the midst of these, this work has several unique characteristics which should change the reader’s perspective, and in particular, provide a more profound understanding of the impact of the IoT on society. Dependable IoT for Human and Industry covers the main aspects of Internet of Things and IoT based systems such as global issues of applications, modeling, development and implementation of dependable IoT for different human and industry domains. Technical topics discussed in the book include: Introduction in Internet of vital and trust Things Modelling and assessment techniques for dependable and secure IoT systems Architecting and development of IoT systems Implementation of IoT for smart cities and drone fleets; business and blockchain, transport and industry Training courses and education experience on Internet and Web of ThingThe book contains chapters which have their roots in the International Conference IDAACS 2017, and Workshop on Cyber Physical Systems and IoT Dependability CyberIoT-DESSERT 2017.

Decision Support Systems VIII: Sustainable Data-Driven

and Evidence-Based Decision Support

4th International Conference, ICDSST 2018, Heraklion, Greece, May 22–25, 2018, Proceedings

Springer This book constitutes the proceedings of the 4th International Conference on Decision Support Systems, ICDSST 2018, held in Heraklion, Greece, in May 2018. The main topic of this year's conference was "Sustainable Data-Driven and Evidence Based Decision Support". The 15 papers presented in this volume were carefully reviewed and selected from 71 submissions. They were organized in topical sections named: decision support systems for a sustainable society; decision support systems serving the public; decision support systems in management and organization; and advances in decision support systems' technologies and methods. The EWG-DSS series of International Conference on Decision Support System Technology (ICDSST), starting with ICDSST 2015 in Belgrade, were planned to consolidate the tradition of annual events organized by the EWG-DSS in offering a platform for European and international DSS communities, comprising the academic and industrial sectors, to present state-of-the-art DSS research and developments, to discuss current challenges that surround decision-making processes, to exchange ideas about realistic and innovative solutions, and to co-develop potential business opportunities.

Intelligent Workloads at the Edge

Deliver cyber-physical outcomes with data and machine learning using AWS IoT Greengrass

Packt Publishing Ltd Explore IoT, data analytics, and machine learning to solve cyber-physical problems using the latest capabilities of managed services such as AWS IoT Greengrass and Amazon SageMaker Key FeaturesAccelerate

your next edge-focused product development with the power of AWS IoT GreengrassDevelop proficiency in architecting resilient solutions for the edge with proven best practicesHarness the power of analytics and machine learning for solving cyber-physical problemsBook Description The Internet of Things (IoT) has transformed how people think about and interact with the world. The ubiquitous deployment of sensors around us makes it possible to study the world at any level of accuracy and enable data-driven decision-making anywhere. Data analytics and machine learning (ML) powered by elastic cloud computing have accelerated our ability to understand and analyze the huge amount of data generated by IoT. Now, edge computing has brought information technologies closer to the data source to lower latency and reduce costs. This book will teach you how to combine the technologies of edge computing, data analytics, and ML to deliver next-generation cyber-physical outcomes. You'll begin by discovering how to create software applications that run on edge devices with AWS IoT Greengrass. As you advance, you'll learn how to process and stream IoT data from the edge to the cloud and use it to train ML models using Amazon SageMaker. The book also shows you how to train these models and run them at the edge for optimized performance, cost savings, and data compliance. By the end of this IoT book, you'll be able to scope your own IoT workloads, bring the power of ML to the edge, and operate those workloads in a production setting. What you will learnBuild an end-to-end IoT solution from the edge to the cloudDesign and deploy multi-faceted intelligent solutions on the edgeProcess data at the edge through analytics and MLPackage and optimize models for the edge using Amazon SageMakerImplement MLOps and DevOps for operating an edge-based solutionOnboard and manage fleets of edge devices at scaleReview edge-based workloads against industry best practicesWho this book is for This book is for IoT architects and software engineers responsible for delivering analytical and machine learning–backed software solutions to the edge. AWS customers who want to learn and build IoT solutions will find this book useful. Intermediate-level experience with running Python software on Linux is required to make the most of this book.

The Internet in Everything

Freedom and Security in a World with No Off Switch

Yale University Press A compelling argument that the Internet of things threatens human rights and security and that suggests policy prescriptions to protect our future The Internet has leapt from human-facing display screens into the

material objects all around us. In this so-called Internet of Things—connecting everything from cars to cardiac monitors to home appliances—there is no longer a meaningful distinction between physical and virtual worlds. Everything is connected. The social and economic benefits are tremendous, but there is a downside: an outage in cyberspace can result not only in a loss of communication but also potentially a loss of life. Control of this infrastructure has become a proxy for political power, since countries can easily reach across borders to disrupt real-world systems. Laura DeNardis argues that this diffusion of the Internet into the physical world radically escalates governance concerns around privacy, discrimination, human safety, democracy, and national security, and she offers new cyber-policy solutions. In her discussion, she makes visible the sinews of power already embedded in our technology and explores how hidden technical governance arrangements will become the constitution of our future.

Intelligent, Secure, and Dependable Systems in Distributed and Cloud Environments

First International Conference, ISDDC 2017, Vancouver, BC, Canada, October 26-28, 2017, Proceedings

Springer This book constitutes the refereed proceedings of the First International Conference on Intelligent, Secure, and Dependable Systems in Distributed and Cloud Environments, ISDDC 2017, held in Vancouver, BC, Canada, in October 2017.The 12 full papers presented together with 1 short paper were carefully reviewed and selected from 43 submissions. This book also contains 3 keynote talks and 2 tutorials. The contributions included in this proceedings cover many aspects of theory and application of effective and efficient paradigms, approaches, and tools for building, maintaining, and managing secure and dependable systems and infrastructures, such as botnet detection, secure cloud computing and cryptosystems, IoT security, sensor and social network security, behavioral systems and data science, and mobile computing.

Advancing Research in Information and Communication Technology

IFIP's Exciting First 60+ Years, Views from the Technical Committees and Working Groups

Springer Nature For 60 years the International Federation for Information Processing (IFIP) has been advancing research in Information and Communication Technology (ICT). This book looks into both past experiences and future perspectives using the core of IFIP's competence, its Technical Committees (TCs) and Working Groups (WGs). Soon after IFIP was founded, it established TCs and related WGs to foster the exchange and development of the scientific and technical aspects of information processing. IFIP TCs are as diverse as the different aspects of information processing, but they share the following aims: To establish and maintain liaison with national and international organizations with allied interests and to foster cooperative action, collaborative research, and information exchange. To identify subjects and priorities for research, to stimulate theoretical work on fundamental issues, and to foster fundamental research which will underpin future development. To provide a forum for professionals with a view to promoting the study, collection, exchange, and dissemination of ideas, information, and research findings and thereby to promote the state of the art. To seek and use the most effective ways of disseminating information about IFIP's work including the organization of conferences, workshops and symposia and the timely production of relevant publications. To have special regard for the needs of developing countries and to seek practicable ways of working with them. To encourage communication and to promote interaction between users, practitioners, and researchers. To foster interdisciplinary work and – in particular – to collaborate with other Technical Committees and Working Groups. The 17 contributions in this book describe the scientific, technical, and further work in TCs and WGs and in many cases also assess the future consequences of the work's results. These contributions explore the developments of IFIP and the ICT profession now and over the next 60 years. The contributions are arranged per TC and conclude with the

chapter on the IFIP code of ethics and conduct.

The Internet of Things

From Data to Insight

John Wiley & Sons Provides comprehensive coverage of the current state of IoT, focusing on data processing infrastructure and techniques Written by experts in the field, this book addresses the IoT technology stack, from connectivity through data platforms to end-user case studies, and considers the tradeoffs between business needs and data security and privacy throughout. There is a particular emphasis on data processing technologies that enable the extraction of actionable insights from data to inform improved decision making. These include artificial intelligence techniques such as stream processing, deep learning and knowledge graphs, as well as data interoperability and the key aspects of privacy, security and trust. Additional aspects covered include: creating and supporting IoT ecosystems; edge computing; data mining of sensor datasets; and crowd-sourcing, amongst others. The book also presents several sections featuring use cases across a range of application areas such as smart energy, transportation, smart factories, and more. The book concludes with a chapter on key considerations when deploying IoT technologies in the enterprise, followed by a brief review of future research directions and challenges. The Internet of Things: From Data to Insight Provides a comprehensive overview of the Internet of Things technology stack with focus on data driven aspects from data modelling and processing to presentation for decision making Explains how IoT technology is applied in practice and the benefits being delivered. Acquaints readers that are new to the area with concepts, components, technologies, and verticals related to and enabled by IoT Gives IoT specialists a deeper insight into data and decision-making aspects as well as novel technologies and application areas Analyzes and presents important emerging technologies for the IoT arena Shows how different objects and devices can be connected to decision making processes at various levels of abstraction The Internet of Things: From Data to Insight will appeal to a wide audience, including IT and network specialists seeking a broad and complete understanding of IoT, CIOs and CIO teams, researchers in IoT and related fields, final year undergraduates, graduate students, post-graduates, and IT and science media professionals.

Internet of Things and the Law

Legal Strategies for Consumer-Centric Smart Technologies

Taylor & Francis Internet of Things and the Law: Legal Strategies for Consumer-Centric Smart Technologies is the most comprehensive and up-to-date analysis of the legal issues in the Internet of Things (IoT). For decades, the decreasing importance of tangible wealth and power – and the increasing significance of their disembodied counterparts – has been the subject of much legal research. For some time now, legal scholars have grappled with how laws drafted for tangible property and predigital 'offline' technologies can cope with dematerialisation, digitalisation, and the internet. As dematerialisation continues, this book aims to illuminate the opposite movement: rematerialisation, namely, the return of data, knowledge, and power within a physical 'smart' world. This development frames the book's central question: can the law steer rematerialisation in a human-centric and socially just direction? To answer it, the book focuses on the IoT, the sociotechnological phenomenon that is primarily responsible for this shift. After a thorough analysis of how existing laws can be interpreted to empower IoT end users, Noto La Diega leaves us with the fundamental question of what happens when the law fails us and concludes with a call for collective resistance against 'smart' capitalism.

The Official CompTIA Security+ Self-Paced Study Guide (Exam SY0-601)

CompTIA Security+ Study Guide (Exam SY0-601)

IoT Security

Advances in Authentication

John Wiley & Sons An up-to-date guide to an overview of authentication in the Internet of Things (IoT) The Internet of things (IoT) is the network of the countless physical devices that have the possibility to connect and exchange data. Among the various security requirements, authentication to the IoT is the first step to prevent the impact of attackers. IoT Security offers an important guide into the development of the many authentication mechanisms that provide IoT authentication at various levels such as user level, device level and network level. The book covers a wide range of topics including an overview of IoT and addresses in detail the security challenges at every layer by considering both the technologies and the architecture used. The authors—noted experts on the topic—provide solutions for remediation of compromised security, as well as methods for risk mitigation, and offer suggestions for prevention and improvement. In addition, IoT Security offers a variety of illustrative use cases. This important book: Offers an authoritative reference designed for use by all IoT stakeholders Includes information for securing devices at the user, device, and network levels Contains a classification of existing vulnerabilities Written by an international group of experts on the topic Provides a guide to the most current information available on IoT security Written for network operators, cloud operators, IoT device manufacturers, IoT device users, wireless users, IoT standardization organizations, and security solution developers, IoT Security is an essential guide that contains information on security features, including underlying networks, architectures, and security requirements.

Real-Time Sensor Networks and Systems for the Industrial IoT

MDPI The Industrial Internet of Things (Industrial IoT—IIoT) has emerged as the core construct behind the various cyber-physical systems constituting a principal dimension of the fourth Industrial Revolution. While initially born as the concept behind specific industrial applications of generic IoT technologies, for the optimization of operational

efficiency in automation and control, it quickly enabled the achievement of the total convergence of Operational (OT) and Information Technologies (IT). The IIoT has now surpassed the traditional borders of automation and control functions in the process and manufacturing industry, shifting towards a wider domain of functions and industries, embraced under the dominant global initiatives and architectural frameworks of Industry 4.0 (or Industrie 4.0) in Germany, Industrial Internet in the US, Society 5.0 in Japan, and Made-in-China 2025 in China. As real-time embedded systems are quickly achieving ubiquity in everyday life and in industrial environments, and many processes already depend on real-time cyber-physical systems and embedded sensors, the integration of IoT with cognitive computing and real-time data exchange is essential for real-time analytics and realization of digital twins in smart environments and services under the various frameworks' provisions. In this context, real-time sensor networks and systems for the Industrial IoT encompass multiple technologies and raise significant design, optimization, integration and exploitation challenges. The ten articles in this Special Issue describe advances in real-time sensor networks and systems that are significant enablers of the Industrial IoT paradigm. In the relevant landscape, the domain of wireless networking technologies is centrally positioned, as expected.

Practical Internet of Things Security

Packt Publishing Ltd A practical, indispensable security guide that will navigate you through the complex realm of securely building and deploying systems in our IoT-connected world About This Book Learn to design and implement cyber security strategies for your organization Learn to protect cyber-physical systems and utilize forensic data analysis to beat vulnerabilities in your IoT ecosystem Learn best practices to secure your data from device to the cloud Gain insight into privacy-enhancing techniques and technologies Who This Book Is For This book targets IT Security Professionals and Security Engineers (including pentesters, security architects and ethical hackers) who would like to ensure security of their organization's data when connected through the IoT. Business analysts and managers will also find it useful. What You Will Learn Learn how to break down cross-industry barriers by adopting the best practices for IoT deployments Build a rock-solid security program for IoT that is cost-effective and easy to maintain Demystify complex topics such as cryptography, privacy, and penetration testing to improve your security posture See how the selection of individual components can affect the security posture of the entire system Use Systems Security Engineering and Privacy-by-design principles to design a secure IoT ecosystem Get to know how to leverage the burdgening cloud-based systems that will support the IoT into the future. In Detail With the advent of Intenret of

Things (IoT), businesses will be faced with defending against new types of threats. The business ecosystem now includes cloud computing infrastructure, mobile and fixed endpoints that open up new attack surfaces, a desire to share information with many stakeholders and a need to take action quickly based on large quantities of collected data. . It therefore becomes critical to ensure that cyber security threats are contained to a minimum when implementing new IoT services and solutions. . The interconnectivity of people, devices, and companies raises stakes to a new level as computing and action become even more mobile, everything becomes connected to the cloud, and infrastructure is strained to securely manage the billions of devices that will connect us all to the IoT. This book shows you how to implement cyber-security solutions, IoT design best practices and risk mitigation methodologies to address device and infrastructure threats to IoT solutions. This book will take readers on a journey that begins with understanding the IoT and how it can be applied in various industries, goes on to describe the security challenges associated with the IoT, and then provides a set of guidelines to architect and deploy a secure IoT in your Enterprise. The book will showcase how the IoT is implemented in early-adopting industries and describe how lessons can be learned and shared across diverse industries to support a secure IoT. Style and approach This book aims to educate readers on key areas in IoT security. It walks readers through engaging with security challenges and then provides answers on how to successfully manage IoT security and build a safe infrastructure for smart devices. After reading this book, you will understand the true potential of tools and solutions in order to build real-time security intelligence on IoT networks.

GB/T-2021, GB-2021 -- Chinese National Standard PDF-English, Catalog (year 2021)

Chinese National Standard: GB Series of year 2021

https://www.chinesestandard.net This document provides the comprehensive list of Chinese National Standards - Category: GB, GB/T Series of year 2021.

From Machine-to-Machine to the Internet of Things: Introduction to a New Age of Intelligence

Academic Press This book outlines the background and overall vision for the Internet of Things (IoT) and Machine-to-Machine (M2M) communications and services, including major standards. Key technologies are described, and include everything from physical instrumentation of devices to the cloud infrastructures used to collect data. Also included is how to derive information and knowledge, and how to integrate it into enterprise processes, as well as system architectures and regulatory requirements. Real-world service use case studies provide the hands-on knowledge needed to successfully develop and implement M2M and IoT technologies sustainably and profitably. Finally, the future vision for M2M technologies is described, including prospective changes in relevant standards. This book is written by experts in the technology and business aspects of Machine-to-Machine and Internet of Things, and who have experience in implementing solutions. Standards included: ETSI M2M, IEEE 802.15.4, 3GPP (GPRS, 3G, 4G), Bluetooth Low Energy/Smart, IETF 6LoWPAN, IETF CoAP, IETF RPL, Power Line Communication, Open Geospatial Consortium (OGC) Sensor Web Enablement (SWE), ZigBee, 802.11, Broadband Forum TR-069, Open Mobile Alliance (OMA) Device Management (DM), ISA100.11a, WirelessHART, M-BUS, Wireless M-BUS, KNX, RFID, Object Management Group (OMG) Business Process Modelling Notation (BPMN) Key technologies for M2M and IoT covered: Embedded systems hardware and software, devices and gateways, capillary and M2M area networks, local and wide area networking, M2M Service Enablement, IoT data management and data warehousing, data analytics and big data, complex event processing and stream analytics, knowledge discovery and management, business process and enterprise integration, Software as a Service and cloud computing Combines both technical explanations together with design features of M2M/IoT and use cases. Together, these descriptions will assist you to develop solutions that will work in the real world Detailed description of the network architectures and technologies that form the basis of M2M and IoT Clear guidelines and examples of M2M and IoT use cases from real-world implementations such as Smart Grid, Smart Buildings, Smart Cities, Participatory Sensing, and Industrial Automation A description of the vision for M2M and its evolution towards IoT

Cognitive Hyperconnected Digital Transformation Internet of Things Intelligence Evolution

CRC Press Cognitive Hyperconnected Digital Transformation provides an overview of the current Internet of Things (IoT) landscape, ranging from research, innovation and development priorities to enabling technologies in a global context. It is intended as a standalone book in a series that covers the Internet of Things activities of the IERC-Internet of Things European Research Cluster, including both research and technological innovation, validation and deployment. The book builds on the ideas put forward by the European Research Cluster, the IoT European Platform Initiative (IoT-EPI) and the IoT European Large-Scale Pilots Programme, presenting global views and state-of-the-art results regarding the challenges facing IoT research, innovation, development and deployment in the next years. Hyperconnected environments integrating industrial/business/consumer IoT technologies and applications require new IoT open systems architectures integrated with network architecture (a knowledge-centric network for IoT), IoT system design and open, horizontal and interoperable platforms managing things that are digital, automated and connected and that function in real-time with remote access and control based on Internet-enabled tools. The IoT is bridging the physical world with the virtual world by combining augmented reality (AR), virtual reality (VR), machine learning and artificial intelligence (AI) to support the physical-digital integrations in the Internet of mobile things based on sensors/actuators, communication, analytics technologies, cyber-physical systems, software, cognitive systems and IoT platforms with multiple functionalities. These IoT systems have the potential to understand, learn, predict, adapt and operate autonomously. They can change future behaviour, while the combination of extensive parallel processing power, advanced algorithms and data sets feed the cognitive algorithms that allow the IoT systems to develop new services and propose new solutions. IoT technologies are moving into the industrial space and enhancing traditional industrial platforms with solutions that break free of device-, operating system- and protocol-dependency. Secure edge computing solutions replace local networks, web services replace software, and devices with networked programmable logic controllers (NPLCs) based on Internet protocols replace devices that use proprietary protocols. Information captured by edge devices on the factory floor is secure and accessible from any location in real time, opening the communication gateway both vertically (connecting machines across the factory and enabling the instant availability

of data to stakeholders within operational silos) and horizontally (with one framework for the entire supply chain, across departments, business units, global factory locations and other markets). End-to-end security and privacy solutions in IoT space require agile, context-aware and scalable components with mechanisms that are both fluid and adaptive. The convergence of IT (information technology) and OT (operational technology) makes security and privacy by default a new important element where security is addressed at the architecture level, across applications and domains, using multi-layered distributed security measures. Blockchain is transforming industry operating models by adding trust to untrusted environments, providing distributed security mechanisms and transparent access to the information in the chain. Digital technology platforms are evolving, with IoT platforms integrating complex information systems, customer experience, analytics and intelligence to enable new capabilities and business models for digital business.

IoT Security

Advances in Authentication

John Wiley & Sons An up-to-date guide to an overview of authentication in the Internet of Things (IoT) The Internet of things (IoT) is the network of the countless physical devices that have the possibility to connect and exchange data. Among the various security requirements, authentication to the IoT is the first step to prevent the impact of attackers. IoT Security offers an important guide into the development of the many authentication mechanisms that provide IoT authentication at various levels such as user level, device level and network level. The book covers a wide range of topics including an overview of IoT and addresses in detail the security challenges at every layer by considering both the technologies and the architecture used. The authors—noted experts on the topic—provide solutions for remediation of compromised security, as well as methods for risk mitigation, and offer suggestions for prevention and improvement. In addition, IoT Security offers a variety of illustrative use cases. This important book: Offers an authoritative reference designed for use by all IoT stakeholders Includes information for securing devices at the user, device, and network levels Contains a classification of existing vulnerabilities Written by an international group of experts on the topic Provides a guide to the most current information available on IoT security Written for network operators, cloud operators, IoT device manufacturers, IoT device users, wireless users, IoT standardization

organizations, and security solution developers, IoT Security is an essential guide that contains information on security features, including underlying networks, architectures, and security requirements.

GB/T-2019, GB-2019 -- Chinese National Standard PDF-English, Catalog (year 2019)

Chinese National Standard: GB Series of year 2019

https://www.chinesestandard.net This document provides the comprehensive list of Chinese National Standards - Category: GB, GB/T Series of year 2019.

GB/T-2018, GB-2018 -- Chinese National Standard PDF-English, Catalog (year 2018)

Chinese National Standard: GB Series of year 2018

https://www.chinesestandard.net This document provides the comprehensive list of Chinese National Standards - Category: GB, GB/T Series of year 2018.

Internet of Things From Hype to Reality

The Road to Digitization

Springer This book comprehensively describes an end-to-end Internet of Things (IoT) architecture that is comprised of devices, network, compute, storage, platform, applications along with management and security components. It is organized into five main parts, comprising of a total of 11 chapters. Part I presents a generic IoT reference model to establish a common vocabulary for IoT solutions. This includes a detailed description of the Internet protocol layers and the Things (sensors and actuators) as well as the key business drivers to realize the IoT vision. Part II focuses on the IoT requirements that impact networking protocols and provides a layer-by-layer walkthrough of the protocol stack with emphasis on industry progress and key gaps. Part III introduces the concept of Fog computing and describes the drivers for the technology, its constituent elements, and how it relates and differs from Cloud computing. Part IV discusses the IoT services platform, the cornerstone of the solution followed by the Security functions and requirements. Finally, Part V provides a treatment of the topic of connected ecosystems in IoT along with practical applications. It then surveys the latest IoT standards and discusses the pivotal role of open source in IoT. “Faculty will find well-crafted questions and answers at the end of each chapter, suitable for review and in classroom discussion topics. In addition, the material in the book can be used by engineers and technical leaders looking to gain a deep technical understanding of IoT, as well as by managers and business leaders looking to gain a competitive edge and understand innovation opportunities for the future.” Dr. Jim Spohrer, IBM “This text provides a very compelling study of the IoT space and achieves a very good balance between engineering/technology focus and business context. As such, it is highly-recommended for anyone interested in this rapidly-expanding field and will have broad appeal to a wide cross-section of readers, i.e., including engineering professionals, business analysts, university students, and professors.” Professor Nasir Ghani, University of South Florida

International Conference on Computer Networks and

Communication Technologies

ICCNCT 2018

Springer The book features research papers presented at the International Conference on Computer Networks and Inventive Communication Technologies (ICCNCT 2018), offering significant contributions from researchers and practitioners in academia and industry. The topics covered include computer networks, network protocols and wireless networks, data communication technologies, and network security. Covering the main core and specialized issues in the areas of next-generation wireless network design, control, and management, as well as in the areas of protection, assurance, and trust in information security practices, these proceedings are a valuable resource, for researchers, instructors, students, scientists, engineers, managers, and industry practitioners.

Smart Systems and IoT: Innovations in Computing

Proceeding of SSIC 2019

Springer Nature The book features original papers from the 2nd International Conference on Smart IoT Systems: Innovations and Computing (SSIC 2019), presenting scientific work related to smart solution concepts. It discusses computational collective intelligence, which includes interactions between smart devices, smart environments and smart interactions, as well as information technology support for such areas. It also describes how to successfully approach various government organizations for funding for business and the humanitarian technology development projects. Thanks to the high-quality content and the broad range of the topics covered, the book appeals to researchers pursuing advanced studies.

Proceedings of International Conference on IoT Inclusive Life (ICIIL 2019), NITTTR Chandigarh, India

Springer Nature This book gathers selected research papers presented at the AICTE-sponsored International Conference on IoT Inclusive Life (ICIIL 2019), which was organized by the Department of Computer Science and Engineering, National Institute of Technical Teachers Training and Research, Chandigarh, India, on December 19–20, 2019. In contributions by active researchers, the book presents innovative findings and important developments in IoT-related studies, making it a valuable resource for researchers, engineers, and industrial professionals around the globe.

Drone Law and Policy

Global Development, Risks, Regulation and Insurance

Routledge Drone Law and Policy describes the drone industry and its evolution, describing the benefits and risks of its exponential growth. It outlines the current and proposed regulatory framework in Australia, the United States, the United Kingdom and Europe, taking into consideration the current and evolving technological and insurance landscape. This book makes recommendations as to additional regulatory and insurance initiatives which the authors believe are necessary to achieve an effective balance between the various competing interests. The 23 chapters are written by global specialists on crucial topics, such as terrorism and security, airport and aircraft safety, maritime deployment, cyber-risks, regulatory oversight, licensing, standards and insurance. This book will provide authoritative reference and expert guidance for regulators and government agencies, legal practitioners, insurance companies and brokers globally, as well as for major organisations utilising drones in industrial applications.

ECCWS 2021 20th European Conference on Cyber Warfare and Security

Academic Conferences Inter Ltd Conferences Proceedings of 20th European Conference on Cyber Warfare and Security

Data Science in Cybersecurity and Cyberthreat Intelligence

Springer Nature This book presents a collection of state-of-the-art approaches to utilizing machine learning, formal knowledge bases and rule sets, and semantic reasoning to detect attacks on communication networks, including IoT infrastructures, to automate malicious code detection, to efficiently predict cyberattacks in enterprises, to identify malicious URLs and DGA-generated domain names, and to improve the security of mHealth wearables. This book details how analyzing the likelihood of vulnerability exploitation using machine learning classifiers can offer an alternative to traditional penetration testing solutions. In addition, the book describes a range of techniques that support data aggregation and data fusion to automate data-driven analytics in cyberthreat intelligence, allowing complex and previously unknown cyberthreats to be identified and classified, and countermeasures to be incorporated in novel incident response and intrusion detection mechanisms.

Advances in Smart System Technologies

Select Proceedings of ICFSST 2019

Springer Nature This book presents select peer-reviewed proceedings of the International Conference on Frontiers in Smart Systems Technologies (ICFSST 2019). It focuses on latest research and cutting-edge technologies in smart systems and intelligent autonomous systems with advanced functionality. Comprising topics related to diverse aspects

of smart technologies such as high security, reliability, miniaturization, energy consumption, and intelligent data processing, the book contains contributions from academics as well as industry. Given the range of the topics covered, this book will prove useful for students, researchers, and professionals alike.

Green Internet of Things Sensor Networks

Applications, Communication Technologies, and Security Challenges

Springer Nature This book presents methods for advancing green IoT sensor networks and IoT devices. Three main methods presented are: a standalone system to support IoT devices that is informed by the amount of energy the solar array system can produce; a model of securing a building's main power supply against unauthorized use; and security of the IoT devices and their networks. For each, the authors outline the methods, presents security and privacy issues, and their solutions. The work suggests a layered approach to expose security issues and challenges at each layer of the IoT architecture and proposes techniques used to mitigate these challenges. Finally, perspectives are drawn and discussed for future directions in securing IoT sensor networks, covering evolving areas such as artificial intelligence, blockchain technology, sensor Internet of People, context-aware sensing, cloud infrastructure, security and privacy, and the Internet of Everything.

Role of IoT in Green Energy Systems

IGI Global In the era of Industry 4.0, the world is increasingly becoming smarter as everything from mobile phones to cars to TVs connects with unique addresses and communication mechanisms. However, in order to enable the smart world to be sustainable, ICT must embark into energy efficient paradigms. Green ICT is a moving factor contributing towards energy efficiency by reducing energy utilization through software or hardware procedures. Role of IoT in Green Energy Systems presents updated research trends in green technology and the latest product and application developments towards green energy. Covering topics that include energy conservation and harvesting, renewable

energy, and green and underwater internet of things, this essential reference book creates further awareness of smart energy and critically examines the contributions of ICT towards green technologies. IT specialists, researchers, academicians, and students in the area of energy harvesting and energy management, and/or those working towards green energy technologies, wireless sensor networks, and smart applications will find this monograph beneficial in their studies.

Volume 6 Winter 2018 Issue 2

Lulu.com

Smart IoT for Research and Industry

Springer Nature This book covers a variety of smart IoT applications for industry and research. For industry, the book is a guide for considering the real-time aspects of automation of application domains. The main topics covered in the industry section include real-time tracking and navigation, smart transport systems and application for GPS domains, modern electric grid control for electricity industry, IoT prospectives for modern society, IoT for modern medical science, and IoT automation for Industry 4.0. The book then provides a summary of existing IoT research that underlines enabling technologies, such as fog computing, wireless sensor networks, data mining, context awareness, real-time analytics, virtual reality, and cellular communications. The book pertains to researchers, outcome-based academic leaders, as well as industry leaders.

Internet of Things

Challenges, Advances, and Applications

CRC Press Internet of Things: Challenges, Advances, and Applications provides a comprehensive introduction to IoT, related technologies, and common issues in the adoption of IoT on a large scale. It surveys recent technological advances and novel solutions for challenges in the IoT environment. Moreover, it provides detailed discussion of the utilization of IoT and its underlying technologies in critical application areas, such as smart grids, healthcare,

insurance, and the automotive industry. The chapters of this book are authored by several international researchers and industry experts. This book is composed of 18 self-contained chapters that can be read, based on interest. Features: Introduces IoT, including its history, common definitions, underlying technologies, and challenges Discusses technological advances in IoT and implementation considerations Proposes novel solutions for common implementation issues Explores critical application domains, including large-scale electric power distribution networks, smart water and gas grids, healthcare and e-Health applications, and the insurance and automotive industries The book is an excellent reference for researchers and post-graduate students working in the area of IoT, or related areas. It also targets IT professionals interested in gaining deeper knowledge of IoT, its challenges, and application areas.

Cyber Security

Critical Infrastructure Protection

Springer Nature This book focus on critical infrastructure protection. The chapters present detailed analysis of the issues and challenges in cyberspace and provide novel solutions in various aspects. The first part of the book focus on digital society, addressing critical infrastructure and different forms of the digitalization, strategic focus on cyber security, legal aspects on cyber security, citizen in digital society, and cyber security training. The second part focus on the critical infrastructure protection in different areas of the critical infrastructure. The chapters cover the cybersecurity situation awareness, aviation and air traffic control, cyber security in smart societies and cities, cyber security in smart buildings, maritime cyber security, cyber security in energy systems, and cyber security in healthcare. The third part presents the impact of new technologies upon cyber capability building as well as new challenges brought about by new technologies. These new technologies are among others are quantum technology, firmware and wireless technologies, malware analysis, virtualization.

The Internet of Things

What Everyone Needs to Know®

Oxford University Press The Internet of Things (IoT) is the notion that nearly everything we use, from gym shorts to streetlights, will soon be connected to the Internet; the Internet of Everything (IoE) encompasses not just objects, but the social connections, data, and processes that the IoT makes possible. Industry and financial analysts have predicted that the number of Internet-enabled devices will increase from 11 billion to upwards of 75 billion by 2020. Regardless of the number, the end result looks to be a mind-boggling explosion in Internet connected stuff. Yet, there has been relatively little attention paid to how we should go about regulating smart devices, and still less about how cybersecurity should be enhanced. Similarly, now that everything from refrigerators to stock exchanges can be connected to a ubiquitous Internet, how can we better safeguard privacy across networks and borders? Will security scale along with this increasingly crowded field? Or, will a combination of perverse incentives, increasing complexity, and new problems derail progress and exacerbate cyber insecurity? For all the press that such questions have received, the Internet of Everything remains a topic little understood or appreciated by the public. This volume demystifies our increasingly "smart" world, and unpacks many of the outstanding security, privacy, ethical, and policy challenges and opportunities represented by the IoE. Scott J. Shackelford provides real-world examples and straightforward discussion about how the IoE is impacting our lives, companies, and nations, and explain how it is increasingly shaping the international community in the twenty-first century. Are there any downsides of your phone being able to unlock your front door, start your car, and control your thermostat? Is your smart speaker always listening? How are other countries dealing with these issues? This book answers these questions, and more, along with offering practical guidance for how you can join the effort to help build an Internet of Everything that is as secure, private, efficient, and fun as possible.