The Hunt For Iot

This contributed volume provides the state-of-the-art development on security and privacy for cyber-physical systems (CPS) and industrial Internet of Things (IIoT). More specifically, this book discusses the security challenges in CPS and IIoT systems as well as how Artificial Intelligence (AI) and Machine Learning (ML) can be used to address these challenges. Furthermore, this book proposes various defence strategies, including intelligent cyber-attack and anomaly detection algorithms for different IIoT applications. Each chapter corresponds to an important snapshot including an overview of the opportunities and challenges of realizing the AI in IIoT environments, issues related to data security, privacy and application of blockchain technology in the IIoT environment. This book also examines more advanced and specific topics in AI-based solutions developed for efficient anomaly detection in IIoT environments. Different AI/ML techniques including deep representation learning, Snapshot Ensemble Deep Neural Network (SEDNN), federated learning and multi-stage learning are discussed and analysed as well. Researchers and professionals working in computer security with an emphasis on the scientific foundations and engineering techniques for securing IIoT systems and their underlying computing and communicating systems will find this book useful as a reference. The content of this book will be particularly useful for advanced-level students studying computer science, computer technology, cyber security, and information systems. It also applies to advanced-level students studying electrical engineering and system engineering, who would benefit from the case studies.

The convenience of online shopping has driven consumers to turn to the internet to purchase everything from clothing to housewares and even groceries. The ubiquity of online retail stores and availability of hard-to-find products in the digital marketplace has been a catalyst for a heighted interest in research on the best methods, techniques, and strategies for remaining competitive in the era of e-commerce. The Encyclopedia of E-Commerce Development, Implementation, and Management is an authoritative reference source highlighting crucial topics relating to effective business models, managerial strategies, promotional initiatives, development methodologies, and end-user considerations in the online commerce sphere. Emphasizing emerging research on up-and-coming topics such as social commerce, the Internet of Things, online gaming, digital products, and mobile services, this multi-volume encyclopedia is an essential addition to the reference collection of both academic and corporate libraries and caters to the research needs of graduate-level students, researchers, IT developers, and business professionals. .

A comprehensive discussion of the findings of the PICASSO initiative on ICT policy ICT Policy, Research, and Innovation: Perspectives and Prospects for EU-US Collaboration provides a clearly readable overview of selected information and communication technology (ICT) and policy topics. Rather than deluge the reader with technical details, the distinguished authors provide just enough technical background to make sense of the underlying policy discussions. The book covers policy, research, and innovation topics on technologies as wide-ranging as: Internet of Things Cyber physical systems 5G Big data ICT Policy, Research, and Innovation compares and contrasts the policy approaches taken by the EU and the US in a variety of areas. The potential for future cooperation is outlined as well. Later chapters provide policy perspectives about some major issues affecting EU/US development cooperation, while the book closes with a discussion of how the development of these new technologies is changing our conceptions of fundamental aspects of society.

This book focuses on the Internet of Everything and related fields. The Internet of Everything adds connectivity and intelligence to just about

every device, giving it special functions. The book provides a common platform for integrating information from heterogeneous sources. However, this can be quite reductive, as the Internet of Everything provides links not only among things, but also data, people, and business processes. The evolution of current sensor and device networks, with strong interactions between people and social environments, will have a dramatic impact on everything from city planning, first responders, the military and health. Such a shared ecosystem will allow for the interaction between data, sensor inputs and heterogeneous systems. Semantics is a fundamental component of this since semantic technologies are able to provide the necessary bridge between different data representations, and to solve terminology incongruence. Integrating data from distributed devices, sensor networks, social networks and biomedical instruments requires, first of all, the systematization of the current state of the art in such fields. Then, it is necessary to identify a common action thread to actually merge and homogenize standards and techniques applied in such a heterogeneous field. The exact requirements of an Internet of Everything environment need to be precisely identified and formally expressed, and finally, the role of modern computing paradigms, such as Cloud and Fog Computing, needs to be assessed with respect to the requirements expressed by an Internet of Everything ecosystem.

A comprehensive guide to Fog and Edge applications, architectures, and technologies Recent years have seen the explosive growth of the Internet of Things (IoT): the internet-connected network of devices that includes everything from personal electronics and home appliances to automobiles and industrial machinery. Responding to the ever-increasing bandwidth demands of the IoT, Fog and Edge computing concepts have developed to collect, analyze, and process data more efficiently than traditional cloud architecture. Fog and Edge Computing: Principles and Paradigms provides a comprehensive overview of the state-of-the-art applications and architectures driving this dynamic field of computing while highlighting potential research directions and emerging technologies. Exploring topics such as developing scalable architectures, moving from closed systems to open systems, and ethical issues rising from data sensing, this timely book addresses both the challenges and opportunities that Fog and Edge computing presents. Contributions from leading IoT experts discuss federating Edge resources, middleware design issues, data management and predictive analysis, smart transportation and surveillance applications, and more. A coordinated and integrated presentation of topics helps readers gain thorough knowledge of the foundations, applications, and issues that are central to Fog and Edge computing. This valuable resource: Provides insights on transitioning from current Cloud-centric and 4G/5G wireless environments to Fog Computing Examines methods to optimize virtualized, pooled, and shared resources Identifies potential technical challenges and offers suggestions for possible solutions Discusses major components of Fog and Edge computing architectures such as middleware, interaction protocols, and autonomic management Includes access to a website portal for advanced online resources Fog and Edge Computing: Principles and Paradigms is an essential source of up-to-date information for systems architects, developers, researchers, and advanced undergraduate and graduate students in fields of computer science and engineering.

The rate of cybercrimes is increasing because of the fast-paced advancements in computer and internet technology. Crimes employing mobile devices, data embedding/mining systems, computers, network communications, or any malware impose a huge threat to data security. Countering Cyber Attacks and Preserving the Integrity and Availability of Critical Systems addresses current problems and issues emerging in cyber forensics and investigations and proposes new solutions that can be adopted and implemented to counter security breaches within various organizations. The publication examines a variety of topics such as advanced techniques for forensic developments in computer and communication-link environments and legal perspectives including procedures for cyber investigations, standards, and policies. It is designed for policymakers, forensic analysts, technology developers, security administrators, academicians, researchers, and

students.

The Internet of Things (IoT) can be defined as any network of things capable of generating, storing and exchanging data, and in some cases acting on it. This new form of seamless connectivity has many applications: smart cities, smart grids for energy management, intelligent transport, environmental monitoring, healthcare systems, etc. and EU policymakers were quick to realize that machine-to-machine communication and the IoT were going to be vital to economic development. It was also clear that the security of such systems would be of paramount importance and, following the European Commission's Cybersecurity Strategy of the European Union in 2013, the EU's Horizon 2020 programme was set up to explore available options and possible approaches to addressing the security and privacy issues of the IoT. This book presents 10 papers which have emerged from the research of the Horizon 2020 and CHIST-ERA programmes, and which address a wide cross-section of projects ranging from the secure management of personal data and the specific challenges of the IoT with respect to the GDPR, through access control within a highly dynamic IoT environment and increasing trust with distributed ledger technologies, to new cryptographic approaches as a counter-measure for side-channel attacks and the vulnerabilities of IoT-based ambient assisted living systems. The security and safety of the Internet of Things will remain high on the agenda of policymakers for the foreseeable future, and this book provides an overview for all those with an interest in the field.

This book constitutes the proceedings of the 21st International Conference on Information Security, ISC 2018, held in Guildford, UK, in September 2018. The 26 full papers presented in this volume were carefully reviewed and selected from 59 submissions. The book also includes one invited talk in full-paper length. The papers were organized in topical sections named: software security; symmetric ciphers and cryptanalysis; data privacy and anonymization; outsourcing and assisted computing; advanced encryption; privacy-preserving applications; advanced signatures; and network security.

Cultural heritage is perceived as the glue that keeps individuals together and makes them feel a part of something larger. It is the past that allows individuals to understand their present and move towards the future. In networked society, it is impossible to think about cultural heritage and its preservation and maintenance without including the digital processes and ICT systems, as well as its impact on territorial innovation. The Handbook of Research on Cultural Heritage and Its Impact on Territory Innovation and Development is a critical and comprehensive reference book that analyzes how preservation and sustainability of cultural heritage occurs in countries, as well as how it contributes to territorial innovation. Moreover, the book examines how technological tools contribute to its preservation and sustainability, as well as its dissemination. Highlighting topics that include public policies, spatial development, and architectural heritage, this book is ideal for cultural heritage professionals, government officials, policymakers, academicians, researchers, and students.

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.

The complexity and severity of the Distributed Denial of Service (DDoS) attacks are increasing day-by-day. The Internet has a highly inconsistent structure in terms of resource distribution. Numerous technical solutions are available, but those involving economic aspects have not been given much consideration. The book, DDoS Attacks – Classification, Attacks, Challenges, and Countermeasures, provides an overview of both types of defensive solutions proposed so far, exploring different dimensions that would mitigate the DDoS effectively and show the implications associated with them. Features: Covers topics that describe taxonomies of the DDoS attacks in detail, recent trends and classification of defensive mechanisms on the basis of deployment location, the types of defensive action, and the solutions offering economic incentives. Introduces chapters discussing the various types of DDoS attack associated with different layers of security, an attacker’s motivations, and the importance of incentives and liabilities in any defensive solution. Illustrates the role of fair resource-allocation schemes, separate payment mechanisms for attackers and legitimate users, negotiation models on cost and types of resources, and risk assessments and transfer mechanisms. DDoS Attacks – Classification, Attacks, Challenges, and Countermeasures is designed for the readers who have an interest in the cybersecurity domain, including students and researchers who are exploring different dimensions associated with the DDoS attack, developers and security professionals who are focusing on developing defensive schemes and applications for detecting or mitigating the DDoS attacks, and faculty members across different universities.

Implement a vendor-neutral and multi-cloud cybersecurity and risk mitigation framework with advice from seasoned threat hunting pros In Threat Hunting in the Cloud: Defending AWS, Azure and Other Cloud Platforms Against Cyberattacks, celebrated cybersecurity professionals and authors Chris Peiris, Binil Pillai, and Abbas Kudrati leverage their decades of experience building large scale cyber fusion centers to deliver the ideal threat hunting resource for both business and technical audiences. You'll find insightful analyses of cloud platform security tools and, using the industry leading MITRE ATT&CK framework, discussions of the

most common threat vectors. You'll discover how to build a side-by-side cybersecurity fusion center on both Microsoft Azure and Amazon Web Services and deliver a multi-cloud strategy for enterprise customers. And you will find out how to create a vendor-neutral environment with rapid disaster recovery capability for maximum risk mitigation. With this book you'll learn: Key business and technical drivers of cybersecurity threat hunting frameworks in today's technological environment Metrics available to assess threat hunting effectiveness regardless of an organization's size How threat hunting works with vendor-specific single cloud security offerings and on multi-cloud implementations A detailed analysis of key threat vectors such as email phishing, ransomware and nation state attacks Comprehensive AWS and Azure "how to" solutions through the lens of MITRE Threat Hunting Framework Tactics, Techniques and Procedures (TTPs) Azure and AWS risk mitigation strategies to combat key TTPs such as privilege escalation, credential theft, lateral movement, defend against command & control systems, and prevent data exfiltration Tools available on both the Azure and AWS cloud platforms which provide automated responses to attacks, and orchestrate preventative measures and recovery strategies Many critical components for successful adoption of multi-cloud threat hunting framework such as Threat Hunting Maturity Model, Zero Trust Computing, Human Elements of Threat Hunting, Integration of Threat Hunting with Security Operation Centers (SOCs) and Cyber Fusion Centers The Future of Threat Hunting with the advances in Artificial Intelligence, Machine Learning, Quantum Computing and the proliferation of IoT devices. Perfect for technical executives (i.e., CTO, CISO), technical managers, architects, system admins and consultants with hands-on responsibility for cloud platforms, Threat Hunting in the Cloud is also an indispensable guide for business executives (i.e., CFO, COO CEO, board members) and managers who need to understand their organization's cybersecurity risk framework and mitigation strategy.

This book defines what IoT Systems manageability looks like and what the associated resources and costs are of that manageability. It identifies IoT Systems performance expectations and addresses the difficult challenges of determining actual costs of IoT Systems implementation, operation, and management across multiple institutional organizations. It details the unique challenges that cities and institutions have in implementing and operating IoT Systems.

Managing IoT Systems for Institutions and CitiesCRC Press

Big Data Analytics for Intelligent Healthcare Management covers both the theory and application of hardware platforms and architectures, the development of software methods, techniques and tools, applications and governance, and adoption strategies for the use of big data in healthcare and clinical research. The book provides the latest research findings on the use of big data analytics with statistical and machine learning techniques that analyze huge amounts of real-time healthcare data. Examines the methodology and requirements for development of big data architecture, big data modeling, big data as a service, big data analytics, and more Discusses big data applications for intelligent healthcare management, such as revenue management and pricing, predictive analytics/forecasting, big data integration for medical data, algorithms and techniques, etc. Covers the development of big data tools, such as data, web and text mining, data mining, optimization, machine learning, cloud in big data with Hadoop, big data in IoT, and more

This book explores the emergence of the modern higher education sector in the independent Irish state. The author traces its origins from the traditional universities, technical schools and teacher training colleges at the start of the twentieth century, cataloguing its development into the complex, multi-layered and diverse system of the early twenty-first century. Focusing on the socio-political and cultural contexts which shaped the evolution of higher education, the author analyses the interplay between the state, academic institutions and other key institutional actors – notably churches, cultural organizations, employers, trade unions and supranational bodies. This study explores policy, structural and institutional change in Irish higher education, suggesting that the emergence of the modern higher education system in Ireland was influenced by ideologies and trends which owed much to a wider European and international context. The book considers how the exercise of power at local, national and international level impinged on the mission, purpose and values of higher education and on the creation and expansion of a distinctive higher education system. The author also explores a transformation in public and political understandings of the role of higher education, charting the gradual evolution from traditionalist conceptions of the academy as a repository for cultural and religious value formation, to the re-positioning of higher education as a vital factor in the knowledge based economy. This comprehensive volume will appeal to students and scholars of the Irish education system, educators and practitioners in the field, and those interested in higher education in Ireland more generally.

Crime science is precisely what it says it is: the application of science to the phenomenon of crime. This handbook, intended as a crime science manifesto, showcases the scope of the crime science field and provides the reader with an understanding of the assumptions, aspirations and methods of crime science, as well as the variety of topics that fall within its purview. Crime science provides a distinctive approach to understanding and dealing with crime: one that is outcome-oriented, evidence-based and that crosses boundaries between disciplines. The central mission of crime science is to find new ways to cut crime and increase security. Beginning by setting out the case for crime science, the editors examine the roots of crime science in environmental criminology and describe its key features. The book is then divided into two sections. The first section comprises chapters by disciplinary specialists about the contributions their sciences can make or have already made to crime science. Chapter 12 of this book is freely available as a downloadable Open Access PDF under a Creative Commons Attribution-Non Commercial-No Derivatives 3.0 license. https://s3-us-west-2.amazonaws.com/tandfbis/rt-files/docs/Open+Access+Chapters/9780415826266_oachapter12.pdf

This book constitutes the proceedings of the 7th International Conference on Internet of Things (IoT) Technologies for HealthCare, HealthyIoT 2020, held in Viana do Castello, Portugal, in December 2020. Due to Covid-19 pandemic the conference was held virtually. The IoT as a set of existing and emerging technologies, notions and services can provide many solutions to delivery of electronic healthcare, patient care, and medical data management. The 12 revised full papers presented were carefully reviewed and selected from 27 submissions. The papers are grouped in topics on physical data tracking wearables, applications and systems; psychological data tracking wearables, applications and systems; scenarios and security.

Provides the authoritative and up-to-date information required for securing IoT architecture and applications The vast amount of data generated by the Internet of Things (IoT) has made information security vital for not only personal privacy, but also for the sustainability of the IoT itself. Security and Privacy in the Internet of Things brings together high-quality research on IoT information security models, architectures, techniques, and application domains. This concise yet comprehensive volume explores state-of-the-art mitigations in IoT security while addressing important privacy challenges across different IoT layers. Divided into three parts, the book provides timely coverage of IoT architecture, security technologies and mechanisms, and applications. The authors outline emerging trends in IoT security and privacy with a focus on areas such as smart homes and cities, e-health, critical infrastructure, and industrial applications. Topics include authentication and access control, the use of blockchains for IoT transactions, attack detection and prevention, energy-efficient management of IoT objects, and secure integration of IoT and Cloud computing. Presenting the current body of knowledge in a single volume, Security and Privacy in the Internet of Things: Discusses a broad range of IoT architectures and applications Covers both the logical and physical security of IoT devices Examines IoT security and privacy standards, protocols, and approaches Addresses the secure integration of IoT and social networks Describes privacy preserving techniques, intrusion detection systems, and threat and vulnerability analyses Security and Privacy in the Internet of Things: Architectures, Techniques, and Applications is essential reading for researchers, industry practitioners, and students involved in IoT development and deployment.

This book provides an insight on the importance that Internet of Things (IoT) and Information and Communication Technology (ICT) solutions can have in taking care of people's health. Key features of this book present the recent and emerging developments in various specializations in curing health problems and finding their solutions by incorporating IoT and ICT. This book presents useful IoT and ICT applications and architectures that cater to their improved healthcare requirements. Topics include in-home healthcare services based on the Internet-of-Things; RFID technology for IoT based personal healthcare; Real-time reporting and monitoring; Interfacing devices to IoT; Smart medical services; Embedded gateway configuration (EGC); Health monitoring infrastructure; and more. Features a number of practical solutions and applications of IoT and ICT on healthcare; Includes application domains such as communication technology and electronic materials and devices; Applies to researchers, academics, students, and practitioners around the world.

Look Inside the Trillion Dollar Club of Frontier Investors "State-owned investment funds are the new frontier investors, larger in size, influence, and power than the traditional Wall Street of investment banks, asset managers, and hedge funds. They are the 'unicorn-makers' behind the scene. Offering a series of in-depth case studies that combine broad perspectives on the tech investment world with specific national examples, this highly original book examines a vital and increasingly important relationship between governments and globalizing VC tech markets." —Anthony Scaramucci, Founder & Managing Partner of SkyBridge "The private sector doesn't have the answers to a growing list of the world's problems. It is the State, working through powerful institutions such as sovereign wealth funds, that has taken a key economic and investment role. Investors need to understand

these state-controlled wealth funds – what they do and how they do it – and this book provides a timely update that fills a gap in the literature on global finance." —Dato' Seri Cheah Cheng Hye, Co-Founder and Co-Chairman, Value Partners; Non-executive Director, Hong Kong Exchanges and Clearing Ltd "Sovereign Wealth Funds (SWFs) lie at the intersection of finance, politics, macroeconomics, and international relations. This book not only constitutes perhaps the most in-depth and insightful investigation of sovereign investors to date, but it starts a broader debate over globalization and state economic intervention in the context of world digital revolution. Invaluable to European governments and businesses, in particular, as the EU strives to become the third tech pillar of the world next to the US and China." —Pierre-Yves Lucas, Head of Cooperation Mongolia, European Union; former Adviser to the CEO of the SWF of Kazakhstan "This is a story about Time Machines." —Ajay Royan, Co-founder with Peter Thiel of Mithril VC Funds

This book presents the combined proceedings of the 10th International Conference on Computer Science and its Applications (CSA 2018) and the 13th KIPS International Conference on Ubiquitous Information Technologies and Applications (CUTE 2018), both held in Kuala Lumpur, Malaysia, Dec 17 - 19, 2018. The aim of these two meetings was to promote discussion and interaction among academics, researchers and professionals in the field of ubiquitous computing technologies. These proceedings reflect the state of the art in the development of computational methods, involving theory, algorithms, numerical simulation, error and uncertainty analysis and novel applications of new processing techniques in engineering, science, and other disciplines related to ubiquitous computing.

A collection of 220 folk songs representing different parts of the United States, some with foreign roots. The songs are based on pentatonic scales making it easy for children to learn the melodies. All of the songs are playable on Orff instruments. These songs can be used as a springboard for discussing other states and cultures.

Resource optimization has always been a thrust area of research, and as the Internet of Things (IoT) is the most talked about topic of the current era of technology, it has become the need of the hour. Therefore, the idea behind this book was to simplify the journey of those who aspire to understand resource optimization in the IoT. To this end, included in this book are various real-time/offline applications and algorithms/case studies in the fields of engineering, computer science, information security, and cloud computing, along with the modern tools and various technologies used in systems, leaving the reader with a high level of understanding of various techniques and algorithms used in resource optimization.

The ubiquity of modern technologies has allowed for increased connectivity between people and devices across the globe. This connected infrastructure of networks creates numerous opportunities for applications and uses. The Internet of Things: Breakthroughs in Research and Practice is an authoritative reference source for the latest academic material on the interconnectivity of networks and devices in the digital era and examines best practices for integrating this

advanced connectivity across multiple fields. Featuring extensive coverage on innovative perspectives, such as secure computing, regulatory standards, and trust management, this book is ideally designed for engineers, researchers, professionals, graduate students, and practitioners seeking scholarly insights on the Internet of Things.

This volume casts light on mergers and alliances in higher education by examining developments of this type in different countries. It combines the direct experiences of those at the heart of such transformations, university leaders and senior officials responsible for higher education policy, with expert analysts of the systems concerned. Higher education in Europe faces a series of major challenges. The economic crisis has accelerated expectations of an increased role in addressing economic and societal challenges while at the same time putting pressure on available finances. Broader trends such as shifting student demographics and expectations, globalisation and mobility and new ways of working with business have contributed to these increased pressures. In the light of these trends there have been moves, both from national or regional agencies and from individual institutions to respond by combining resources, either through collaborative arrangements or more fundamentally through mergers between two or more universities. After an introductory chapter by the editors which establishes the context for mergers and alliances, the book falls into two main parts. Part 1 takes a national or regional perspective to give some sense of the historical context, the wider drivers and the importance of these developments in these cases. Included are both systemic accounts (for countries as France, Sweden, Romania, Russia, Wales and England), and specific cross-cutting in itiatives including a major facility at Magurele in Romania and a Spanish programme for promoting international campuses of excellence. Part 2 is built from specific cases of universities, either in mergers or alliances, with examples from different countries (such as France, UK, Romania, Spain, Germany, Denmark, Finland, Switzerland). A concluding chapter by the editors assesses these experiences and indicates the implications and future needs for understanding in this domain.

This book presents refereed proceedings of the First International Conference on Advances in Cyber Security, ACeS 2019, held in Penang, Malaysia, in July-August 2019. The 25 full papers and 1 short paper were carefully reviewed and selected from 87 submissions. The papers are organized in topical sections on internet of things, industry and blockchain, and cryptology; digital forensics and surveillance, botnet and malware, and DDoS and intrusion detection/prevention; ambient cloud and edge computing, wireless and cellular communication.

Internet of Things (IoT) is a new platform of various physical objects or “things equipped with sensors, electronics, smart devices, software, and network connections. IoT represents a new revolution of the Internet network which is driven by the recent advances of technologies such as sensor networks (wearable and implantable), mobile devices, networking, and cloud computing technologies. IoT permits these the smart devices to collect, store and analyze the collected data

with limited storage and processing capacities. Swarm Intelligence for Resource Management in the Internet of Things presents a new approach in Artificial Intelligence that can be used for resources management in IoT, which is considered a critical issue for this network. The authors demonstrate these resource management applications using swarm intelligence techniques. Currently, IoT can be used in many important applications which include healthcare, smart cities, smart homes, smart hospitals, environment monitoring, and video surveillance. IoT devices cannot perform complex on-site data processing due to their limited battery and processing. However, the major processing unit of an application can be transmitted to other nodes, which are more powerful in terms of storage and processing. By applying swarm intelligence algorithms for IoT devices, we can provide major advantages for energy saving in IoT devices. Swarm Intelligence for Resource Management in the Internet of Things shows the reader how to overcome the problems and challenges of creating and implementing swarm intelligence algorithms for each application Examines the development and application of swarm intelligence systems in artificial intelligence as applied to the Internet of Things Discusses intelligent techniques for the implementation of swarm intelligence in IoT Prepared for researchers and specialists who are interested in the use and integration of IoT and cloud computing technologies

Vivimos inmersos en un proceso de transformación que nos lleva hacia una sociedad digital conectada. España está experimentando cambios trascendentales derivados de una revolución tecnológica sin precedentes que se extiende por todo el mundo. Un año más, Fundación Telefónica ha llevado a cabo un riguroso estudio sobre el avance de la transición digital en nuestro país. El informe Sociedad Digital en España, además de reflejar los indicadores que ponen en relieve el estado de desarrollo de las infraestructuras y de los servicios de telecomunicaciones, se adentra en el análisis sobre cómo esta gran ola de innovación está remodelando el tejido socioeconómico nacional. Al igual que en las ediciones precedentes, este estudio parte de tres fuentes de información: la ofrecida por los principales indicadores nacionales e internacionales sobre el ecosistema digital, aquella que surge de las encuestas a clientes de las unidades de negocio de Telefónica y, por último, la visión regional que han aportado directamente las comunidades autónomas. En la edición 2019 del informe se tratan temas como los desafíos y oportunidades que nos plantea la inteligencia artificial, la tecnología blockchain como garante de las relaciones entre distintas partes dentro de un mundo virtual, las ventajas en términos de productividad que consiguen las nuevas fábricas inteligentes de la industria 4.0, o sobre cómo cada vez más aspectos de nuestras vidas transcurren en la esfera ciberespacio. Sociedad Digital en España persigue establecer una imagen fiel sobre cómo se va convirtiendo nuestro país en una sociedad en red, señalando los logros alcanzados, pero, igualmente, poniendo en relieve los retos que enfrentamos para no dejar a nadie en el camino, garantizando una transición inclusiva que, más allá de la tecnología, esté centrada en las personas.

Eros: The Myth of Ancient Greek Sexuality is a controversial book that lays bare the meanings Greeks gave to sex. Contrary to the romantic idealization of sex dominating our culture, the Greeks saw eros as a powerful force of nature, potentially dangerous, and

in need of control by society: Eros the Destroyer, not Cupid the Insipid, fired the Greek imagination.The destructiveness of eros can be seen in Greek imagery and metaphor, and in the Greeks' attitudes toward women and homosexuals. Images of love as fire, disease, storms, insanity, and violence?Top 40 song clichfor us?locate eros among the unpredictable and deadly forces of nature. The beautiful Aphrodite embodies the alluring danger of sex, while femmes fatales like Pandora and Helen represent the risky charms of female sexuality. And homosexuality typifies for the Greeks the frightening power of an indiscriminate appetite that threatens the stability of culture itself.In Eros: The Myth of Ancient Greek Sexuality, Bruce Thornton offers a uniquely sweeping and comprehensive account of ancient sexuality free of currently fashionable theoretical jargon and pretentions. In its conclusions the book challenges the distortions of much recent scholarship on Greek sexuality. And throughout it links the wary attitudes of the Greeks to our present-day concerns about love, sex, and family. What we see, finally, are the origins of some of our own views as well as a vision of sexuality that is perhaps more honest and mature than our own dangerous illusions.

In 2017, researchers discovered a vulnerability in microprocessors used in computers and devices all over the world. The vulnerability, named Spectre, combines side effects from caching and speculative execution, which are techniques that have been used for many years to increase the speed at which computers operate. The discovery upends a number of common assumptions about cybersecurity and draws attention to the complexities of the global supply chain and global customer base for the vast range of devices and cloud capabilities that all computer users rely on. In October 2018, the Forum on Cyber Resilience hosted a workshop to explore the implications of this development. This publication summarizes the presentations and discussions from the workshop.

This book offers the first comprehensive view on integrated circuit and system design for the Internet of Things (IoT), and in particular for the tiny nodes at its edge. The authors provide a fresh perspective on how the IoT will evolve based on recent and foreseeable trends in the semiconductor industry, highlighting the key challenges, as well as the opportunities for circuit and system innovation to address them. This book describes what the IoT really means from the design point of view, and how the constraints imposed by applications translate into integrated circuit requirements and design guidelines. Chapter contributions equally come from industry and academia. After providing a system perspective on IoT nodes, this book focuses on state-of-the-art design techniques for IoT applications, encompassing the fundamental sub-systems encountered in Systems on Chip for IoT: ultra-low power digital architectures and circuits low- and zero-leakage memories (including emerging technologies) circuits for hardware security and authentication System on Chip design methodologies on-chip power management and energy harvesting ultra-low power analog interfaces and analog-digital conversion short-range radios miniaturized battery technologies packaging and assembly of IoT integrated systems (on silicon and non-silicon substrates). As a common thread, all chapters conclude with a prospective view on the foreseeable evolution of the related technologies for IoT. The concepts developed throughout the book are exemplified by two IoT node system demonstrations from industry. The unique balance between breadth and depth of this book: enables expert readers quickly to develop an understanding of the specific challenges and state-of-the-art solutions for IoT, as well

as their evolution in the foreseeable future provides non-experts with a comprehensive introduction to integrated circuit design for IoT, and serves as an excellent starting point for further learning, thanks to the broad coverage of topics and selected references makes it very well suited for practicing engineers and scientists working in the hardware and chip design for IoT, and as textbook for senior undergraduate, graduate and postgraduate students (familiar with analog and digital circuits).

RIoT Control: Understanding and Managing Risks and the Internet of Things explains IoT risk in terms of project requirements, business needs, and system designs. Learn how the Internet of Things (IoT) is different from “Regular Enterprise security, more intricate and more complex to understand and manage. Billions of internet-connected devices make for a chaotic system, prone to unexpected behaviors. Industries considering IoT technologies need guidance on IoT-ready security and risk management practices to ensure key management objectives like Financial and Market success, and Regulatory compliance. Understand the threats and vulnerabilities of the IoT, including endpoints, newly emerged forms of gateway, network connectivity, and cloud-based data centers. Gain insights as to which emerging techniques are best according to your specific IoT system, its risks, and organizational needs. After a thorough introduction to the Iot, Riot Control explores dozens of IoT-specific risk management requirements, examines IoT-specific threats and finally provides risk management recommendations which are intended as applicable to a wide range of use-cases. Explains sources of risk across IoT architectures and performance metrics at the enterprise level Understands risk and security concerns in the next-generation of connected devices beyond computers and mobile consumer devices to everyday objects, tools, and devices Offers insight from industry insiders about emerging tools and techniques for real-world IoT systems